Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Préposé fédéral à la protection des données et à la transparence
PFPDT

Guide relatif aux systèmes de reconnaissance biométrique

Version 1.0
Septembre 2009

Le présent document est destiné aux **développeurs** et aux **exploitants** de systèmes de reconnaissance biométrique. Il a pour objectif de mettre en lumière les enjeux et les modalités d'évaluation des systèmes de reconnaissance biométrique en matière de protection des données personnelles au regard de la loi fédérale sur la protection des données, aussi bien pour un système existant que pour un nouveau système.

Ce document est subdivisé en trois parties. La partie introductive est consacrée en particulier à la **terminologie et aux définitions** nécessaires à une bonne compréhension de cette matière complexe qu'est la biométrie. La deuxième partie liste les **principes directeurs** applicables lors de la conception et l'utilisation de systèmes de reconnaissance biométrique. Et enfin la troisième partie est construite sous forme d'un **guide d'évaluation**. Ce dernier constitue la partie pratique du document et comprend lui-même quatre séries de questions, pour lesquelles nous fournissons les éléments-clés permettant de mettre en lumière les exigences à respecter en matière de protection des données. En répondant à toutes ces questions au regard de votre cas d'espèce, vous serez ainsi à même d'évaluer globalement le système de reconnaissance existant ou envisagé et de pouvoir prendre en compte les aspects de protection des données.

Feldeggweg 1, 3003 Berne
Tél. 058 463 74 84, Fax 058 465 99 96
www.edoeb.admin.ch

Table des matières

1. Introduction

1.1 Préambule

Les systèmes de reconnaissance biométriques, utilisés de plus en plus largement tant dans le domaine privé que public, comportent de nombreux avantages pour les personnes qui les introduisent et les personnes concernées. Toutefois, l'utilisation de données biométriques pour l'identification ou la vérification d'une identité prétendue comporte également des risques quant au respect des droits et des libertés fondamentales.

Ces systèmes de reconnaissance reposent sur l'analyse de caractéristiques physiologiques ou comportementales du corps humain. L'utilisation de données biométriques pour la reconnaissance comporte des risques pour les personnes concernées: en particulier le non respect du droit à l'autodétermination informationnelle, l'usurpation d'identité, la création d'un identifiant unique global, l'exploitation d'informations complémentaires sur la personne concernée (par exemple des maladies) contenues dans les données biométriques. Cette thématique est d'autant plus importante au regard des risques liés aux perspectives d'utilisation future de caractéristiques biométriques comme identifiant unique global; à savoir pour apparier des données provenant de diverses sources afin de réaliser un profil de personnalité à l'insu des personnes concernées.

Les caractéristiques biométriques sont en principe permanentes (chaque individu les conserve tout au long de son existence), uniques (propres à chaque individu) et universelles (présentes chez tous les individus). Notons toutefois que la permanence, l'unicité et l'universalité ne sont pas absolues, étant donné resp. l'altération naturelle, accidentelle ou volontaire de certaines caractéristiques au cours du temps, l'existence de jumeaux biométriques et la survenance d'échecs à l'enrôlement.

Le présent document a pour objectif de mettre en lumière les enjeux et les modalités d'évaluation des systèmes de reconnaissance biométrique, en matière de protection des données personnelles.

L'architecture des systèmes influence grandement les risques et l'intensité d'atteinte(s) à la personnalité, à l'intégrité physique ou à la dignité humaine. Afin de limiter les risques d'atteinte, il convient d'observer les principes de la protection des données, tout particulièrement les principes de licéité, de transparence (bonne foi, reconnaissabilité et obligation d'informer), de finalité, de proportionnalité et de sécurité des données. Conformément au principe de proportionnalité, les traitements de données personnelles doivent être réalisés à l'aide de moyens adéquats, nécessaires et non excessifs au regard des finalités du traitement. Ainsi, le recours à des systèmes de reconnaissance biométrique devrait être envisagé uniquement s'il n'existe pas de moyen moins intrusif pour atteindre l'objectif visé. Si l'introduction d'un système de reconnaissance biométrique est justifiée au vu des circonstances, il convient de définir l'architecture du système (en particulier le processus de reconnaissance, les modalités de stockage des données, les caractéristique(s) biométrique(s) et les données biométriques) de manière à limiter autant que possible le risque d'atteinte pour les personnes concernées. De plus, des mesures techniques et organisationnelles appropriées doivent être mises en place afin de garantir la fiabilité des systèmes et la sécurité des données, en particulier lors du stockage et de la transmission de celles-ci. En outre, les personnes concernées doivent être dûment informées de leurs droits.

Le présent document comporte trois parties. Cette première partie apporte des précisions terminologiques et détaille les principales technologies biométriques. La deuxième partie comprend une liste des principes directeurs spécifiques aux systèmes de reconnaissance biométrique. Finalement, la troisième partie comporte un guide d'évaluation utilisable aussi bien pour les nouveaux systèmes que pour les systèmes existants. Dans la mesure où les orientations choisies s'écartent de celles conseillées dans ce document, il conviendra d'exposer les motifs justifiant tout recours à une solution plus intrusive.

Enfin, le présent document tient compte de l'état actuel de la technologie. Si nécessaire, le PFPDT procédera ultérieurement à des adaptations, compte tenu de l'évolution de la technologie et de l'expérience acquise.

1.2 Terminologie et définitions

1.2.1 Terminologie

La notion de biométrie et les processus de fonctionnement des systèmes de reconnaissance biométrique sont complexes.

Au sens premier, le terme biométrie[1] (*Biometrik – biometry*), fait référence à l'analyse des caractéristiques physiques d'une personne (voix, contour du visage, empreintes digitales, …).

Depuis peu, le terme biométrie, est également utilisé dans un sens plus restrictif, en référence aux *systèmes de reconnaissance biométrique* (*Biometrie – biometrics*). Il n'existe pas de définition unanimement ou généralement reconnue pour la notion de *système de reconnaissance biométrique automatisée* (*Biometrie – biometrics*).

L'adoption d'une terminologie et de définitions harmonisées en la matière est essentielle à la compréhension du fonctionnement, des avantages des systèmes de reconnaissance biométrique et des enjeux qui s'y rapportent.

Plusieurs projets ont vu le jour, notamment au niveau de l'ISO, toutefois les divergences demeurent; aucun consensus concernant l'harmonisation de la terminologie et de définitions dans le domaine des systèmes de reconnaissance biométrique n'a pu être atteint à ce jour.

La section suivante contient une liste choisie de définitions retenues par le préposé fédéral à la protection des données et à la transparence (PFPDT).

[1] Composé de bio- (du grec bios - «la vie») et de - métrie (du grec metron - «mesure»)

1.2.2 Définitions

On entend par:

Caractéristiques biométriques, les caractéristiques physiologiques[2] ou comportementales[3] mesurables d'un individu.

Système de reconnaissance biométrique, système qui permet de procéder à la reconnaissance automatisée ou humaine (vérification ou identification) des individus sur la base de leurs caractéristiques biométriques.

Donnée biométrique brute, une représentation physique ou numérique d'une caractéristique biométrique, utilisable par un système de reconnaissance biométrique.

Donnée biométrique dérivée ou gabarit biométrique (biometric template), une réduction numérisée d'une donnée biométrique brute, utilisable par un système de reconnaissance biométrique automatisée.

Données biométriques, données biométriques brutes ou dérivées.

Enrôlement biométrique, processus initial de collecte d'une donnée biométrique d'un individu et la sauvegarde de celle-ci en tant que donnée biométrique de référence.

Echec à l'enrôlement (failure to enrol «*FTE*»), la proportion des utilisateurs pour qui le système de reconnaissance biométrique n'est pas en mesure de capturer une donnée biométrique de référence de qualité suffisante.

Vérification biométrique, le processus de comparaison (1:1) d'une donnée biométrique d'épreuve avec une donnée biométrique de référence dans le but de vérifier si la personne concernée est bien celle qu'elle prétend être.

Identification biométrique, le processus de comparaison (1:n) d'une donnée biométrique d'épreuve avec un ensemble de données biométrique de référence stockées dans une base de données, dans le but de déterminer qui est la personne concernée.

Echec à l'acquisition (failure to acquire «*FTA*»), la proportion de tentatives pour lesquelles le système de reconnaissance biométrique n'est pas en mesure de capturer une image de qualité suffisante.

Seuil d'acceptation (threshold), valeur minimale qu'une comparaison biométrique doit atteindre pour être considérée comme réussie. Lorsque cette valeur est choisie de manière à ce que le taux de fausses acceptations soit égal au taux de faux rejets, le seuil est appelé taux d'erreurs égales (equal error rate «EER»).

Taux de fausses acceptations (false acceptance rate «FAR»), la probabilité qu'un système de reconnaissance biométrique identifie un individu ou authentifie un imposteur par erreur.

[2] Notamment les empreintes digitales, l'image de l'iris ou du visage, la géométrie ou le réseau veineux de la main
[3] Notamment la signature, la voix ou la démarche

Taux de faux rejets (false rejection rate «FRR»), la probabilité qu'un système de reconnaissance biométrique échoue lors de l'identification ou la vérification d'une personne enrôlée *[pour plus de détails sur les taux d'erreur, notamment «FMR» et «FMNR», voir FIDIS D 3.10: Biometrics in identity management[4]].*

Gabarit biométrique sur carte (template on card), un support mémoire sur lequel les gabarits biométriques de référence peuvent être enregistrés.

Comparaison biométrique sur carte (match on card), une smartcard à processeur, sur laquelle les gabarits biométriques de référence peuvent être enregistrés et comparés à des données d'épreuve collectées.

Système biométrique sur carte (system on card / encapsulated biometrics), une smartcard à processeur équipée d'un lecteur biométrique (en l'état actuel de la technique, uniquement d'empreintes digitales), sur laquelle des données biométriques peuvent être collectées, enregistrées et comparées.

1.3 Principales technologies biométriques

La reconnaissance biométrique est un domaine de recherche en constante évolution. Les différentes technologies de reconnaissance biométrique, utilisées pour identifier ou vérifier une identité prétendue, reposent sur l'analyse de **caractéristiques physiologiques** (*something you are; passive biometrics*) ou **caractéristiques comportementales** (*something you do; active biometrics*) d'un individu.

Caractéristiques physiologiques:	**Caractéristiques comportementales:**
- contour du visage	- signature autographe
- empreintes digitales	- empreinte vocale
- contour de la main	- démarche
- scan de l'iris	- dactylographie (keystroke)
- réseau veineux de la main ou du doigt	- …
- …	

Une caractéristique biométrique devrait être pour le moins:

- distinctive (distinctiveness), différent d'un individu à l'autre;
- universelle (*universality*), dont dispose tout individu;
- permanente (*permanence*), qui reste inchangée dans le temps – pour chaque individu;
- accessible (*collectability*), dont l'image est facilement capturable.

Idéalement, une caractéristique biométrique devrait être en outre:

- performante (*performance*), robuste, précise, efficace et rapidement analysable;
- acceptée (*acceptance*), dont la collecte ne soulève pas d'opposition;
- fiable (*reliability*), dont la contrefaçon et le contournement de sa délivrance sont peu aisés.

[4] http://www.fidis.net/resources/deliverables/hightechid/#c2057

2. Principes directeurs pour les systèmes de reconnaissance biométrique

Cette partie contient une liste de principes directeurs applicables lors de la conception et de l'utilisation des systèmes de reconnaissance biométriques.

- Les **traitements** de données personnelles doivent être **licites** (art. 4 al.1 LPD) et **transparents** (art. 4 al. 2 & 4 LPD).

- Les **finalités** du traitement (art. 4 al. 3 LPD) doivent être strictement respectées. Par conséquent, des données biométriques collectées dans le but de procéder à une reconnaissance biométrique ne doivent, sauf justification légale (notamment à des fins de poursuite pénale), pas être traitées de manière incompatible avec les finalités originelles.

- Des **alternatives** doivent être prévues pour les personnes qui ne sont pas en mesure d'utiliser un système de reconnaissance biométrique afin d'éviter toute discrimination injustifiée. Ces alternatives doivent en outre être proposées à toutes les personnes qui ne souhaitent pas que leurs données biométriques soient utilisées à des fins de reconnaissance, à condition que les finalités visées ne s'en trouvent pas remises en cause.

- L'**architecture des systèmes de reconnaissance biométrique** influence grandement les risques et l'intensité d'atteinte(s) à la personnalité, à l'intégrité physique ou à la dignité humaine. Les exigences en matière de protection des données personnelles doivent être prises en compte et intégrées dès la phase de conception et lors de la maintenance de ces systèmes.

- Il convient de ne **pas** exploiter des **informations personnelles complémentaires** (notamment une maladie, la race) contenues dans les données biométriques.

- Le principe de **proportionnalité** (art. 4 al. 2 LPD) doit être strictement observé. On recourra en particulier à la biométrie, **que s'il n'y a pas de moyens moins intrusifs** d'atteindre l'objectif visé ou si celle-ci est un élément de protection et/ou sécurité des données. Il convient ainsi d'**adopter des moyens adéquats, pertinents et non excessifs** au regard des finalités du traitement, lors du choix **des systèmes de reconnaissance** (moyens traditionnels et/ou reconnaissance biométrique), **des processus de reconnaissance** (vérification biométriques vs. identification), **des modalités de stockage des données** (décentralisation vs. centralisation), **des caractéristiques biométriques** (sans trace ni capture imperceptible vs. laissant des traces et/ou dont la capture est imperceptible) et **des données biométriques** (données biométriques dérivées vs. données biométriques brutes).

- La **journalisation des processus biométriques** (enrôlement et/ou reconnaissance) doit en particulier répondre aux principes de finalité et de proportionnalité. La création des fichiers journaux, leur durée de conservation, leur anonymisation ou leur destruction doivent être fixées à la mesure de ces deux principes.

- Pour les processus de **vérification biométrique**, les **technologies n'impliquant pas le stockage central des données biométriques** et permettant aux personnes concernées de contrôler en partie (gabarit ou comparaison sur carte) ou en totalité (système sur carte) l'usage qui est fait de leurs données biométriques doivent être privilégiées. Toutefois, la création d'une base

de données centralisée est admissible si celle-ci répond à un intérêt prépondérant qualifié de sécurité.

- Si les données biométriques sont stockées de manière centralisée, une procédure d'**effacement des données** doit être prévue lorsque celles-ci ne sont plus nécessaires pour atteindre le(s) but(s) indiqué(s) lors de la collecte, dans la loi ou qui ressort(ent) des circonstances.

- Les systèmes de reconnaissance biométrique doivent être conçus et adaptés de manière à garantir **l'exactitude, la qualité des données biométriques** (art. 5 al. 1 LPD). Pour ce faire, il convient tout d'abord de définir le nombre minimum de traits biométriques distinctifs permettant de garantir un niveau de reconnaissance (vérification/identification) adapté à la finalité. D'autre part, il s'agit ensuite de choisir en particulier un seuil d'acceptation en fonction du taux admissible de fausses acceptations (FAR). Il faut en outre prendre en compte les conséquences négatives que les faux rejets (FRR) peuvent occasionner aux personnes concernées. Ces choix visent globalement à assurer la fiabilité et l'efficacité du système de reconnaissance au regard des finalités.

- Des mesures techniques et organisationnelles (adaptées à la sensibilité de données biométriques traitées) doivent être mises en place afin de garantir la **sécurité des données** (art. 7 al. 1 LPD), en particulier lors du stockage et de la communication de celles-ci.

- Les **droits des personnes concernées** (art. 8 LPD) doivent être garantis. Aussi les personnes concernées doivent avoir la possibilité de contrôler l'usage qui est fait de leurs données biométriques; être dûment informées et associées au processus de traitement (collecte auprès de la personne concernée ou du moins à sa connaissance) sauf si la loi prévoit expressément que la réalisation du traitement se fasse de manière secrète; de pouvoir avoir accès à leurs données biométriques et obtenir la rectification ou la destruction de celles-ci le cas échéant.

- Le maître de fichier doit le cas échéant **déclarer les fichiers biométriques** (art. 11*a* al. 2 & 3 LPD) au PFPDT.

3. Guide d'évaluation

3.1 Introduction

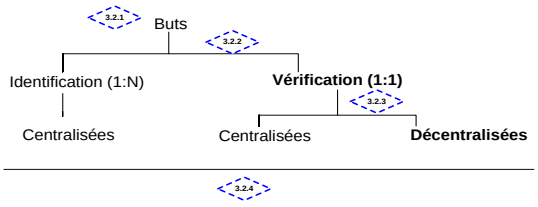
Les systèmes de reconnaissance biométrique présentent des risques quant au respect des droits et libertés fondamentales. De ce fait, le respect du principe de proportionnalité est essentiel, lors du choix du système de reconnaissance (moyens traditionnels et/ou biométriques), des processus de reconnaissance (vérification ou identification), des modalités de stockage (décentralisation ou centralisation), des caractéristiques biométriques, des données biométriques (brutes ou dérivées) et des mesures pour assurer la sécurité des données ainsi que la fiabilité du système. Les traitements de données personnelles doivent ainsi être réalisés à l'aide de moyens adéquats, nécessaires et non excessifs au regard des finalités du traitement.

Le guide d'évaluation est divisé en quatre sections: finalités, licéité et transparence (3.2); moyens de reconnaissance (3.3); sécurité des données et fiabilité du système (3.4); droits des personnes concernées (3.5). Il comprend les questions à prendre en compte pour l'analyse des systèmes de reconnaissance biométrique au regard du droit à la protection des données ainsi qu'un commentaire pour chaque question. Un schéma synthétique des questions précède les trois premières sections.

3.2 Finalités, licéité et transparence

Les données personnelles doivent être traitées pour des finalités clairement définies, licites et reconnaissables pour les personnes concernées. En outre, les traitements subséquents doivent être compatibles avec les finalités originelles.

Finalités, licéité et transparence (les solutions recommandées figurent **en gras)**



3.2.1 Quels sont les buts de l'introduction du système de reconnaissance biométrique?

3.2.2 Quel est le processus de reconnaissance, s'agit-il d'identification ou de vérification biométrique?

3.2.3 Les données biométriques sont-elles stockées de manière centralisée ou décentralisée (modalités de stockage)?

3.2.4 Quels sont les motifs justificatifs du traitement?

3.2.1 Quels sont les buts de l'introduction du système de reconnaissance biométrique?

Les buts du traitement des données biométriques doivent être clairement définis et reconnaissables pour les personnes concernées.

3.2.2 Quel est le processus de reconnaissance, s'agit-il d'identification ou de vérification biométrique?

Si le but recherché est de vérifier l'identité prétendue (claimed identity), il convient de mettre en place un processus de vérification biométrique. La vérification biométrique répond aux besoins «d'authentification forte» qui ne peuvent être atteints à l'aide de moyens traditionnels d'authentification, tels les mots de passe ou les jetons d'accès (tokens).

L'identification biométrique comporte des risques d'atteinte plus importants, par conséquent, la mise en place d'un tel processus est envisageable uniquement si celui-ci est indispensable pour atteindre le but recherché, en l'occurrence *savoir qui est la personne concernée*. Il convient à cet égard de préciser si le processus d'identification visé doit être entièrement automatisée ou non (cf.3.4.5).

3.2.3 Les données biométriques sont-elles stockées de manière centralisée ou décentralisée (modalités de stockage)?

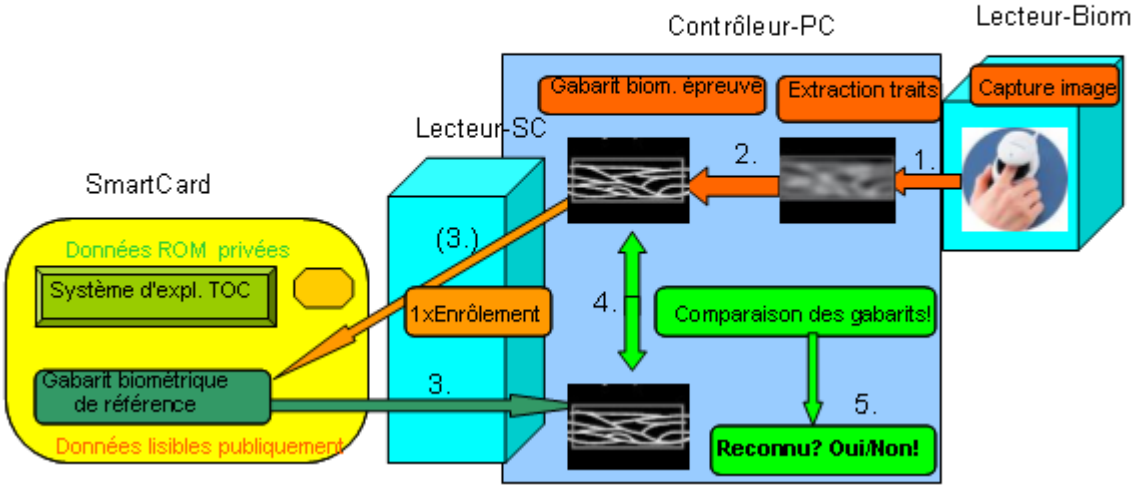
Si les données biométriques sont stockées de manière centralisée, ce qui est évidemment nécessaire pour tout processus d'identification biométrique, les exigences en matière de protection des données sont plus contraignantes. Le maître du fichier doit en particulier veiller à respecter les finalités du traitement, ne pas utiliser les données biométriques comme identifiant unique, assurer l'exactitude des données, garantir le droit d'accès aux données pour les personnes concernées, sécuriser les données par des mesures techniques et organisationnelles appropriées (chiffrement, backups, etc.).

Si le traitement des données biométriques a pour but de vérifier l'identité prétendue de la personne concernée, chaque donnée biométrique de référence doit être stockée intégralement (voire partiellement[5]) de manière décentralisée sur un support personnel. Il existe différents types de supports, permettant aux personnes concernées de contrôler en partie (gabarit biométrique sur carte - *template on card* ou comparaison biométrique sur carte - *match on card*) ou en totalité (système biométrique sur carte - *system on card*) l'usage qui est fait de leurs données biométriques. Une complète autodétermination informationnelle implique que les données biométriques ne se trouvent jamais hors du contrôle des personnes concernées; actuellement ceci n'est assuré que par la solution la plus avancée (système biométrique sur carte - *system on card / encapsulated biometrics*).

Les solutions de base (gabarit biométrique sur carte - *template on card*) permettent uniquement de stocker les données biométriques de références sur un support personnel. Les solutions intermédiaires (comparaison biométrique sur carte - *match on card*) permettent de surcroît la réalisation du processus de comparaison sur la carte. Enfin, les solutions avancées (système biométrique sur carte - *system on card / encapsulated biometrics*), en pratique basées que sur des empreintes digitales, permettent de stocker les données biométriques de référence, de réaliser le processus de comparaison et de prendre une décision sur la carte (réussite ou échec de la vérification biométrique).

[5] Certains développements récents visent un *partitionnement de la référence biométrique* en deux éléments, l'un décentralisé et l'autre centralisé, avec la particularité que la comparaison n'est possible qu'en présence de ces deux éléments!

Gabarit biométrique sur carte



A) Enrôlement:

1) Capture des données biométriques de référence (données brutes) à l'aide du contrôleur (PC)
2) Extraction des traits distinctifs de référence à l'aide du contrôleur (PC) et envoi du gabarit biométrique de référence à la carte.
3) Stockage du gabarit biométrique de référence sur la carte.

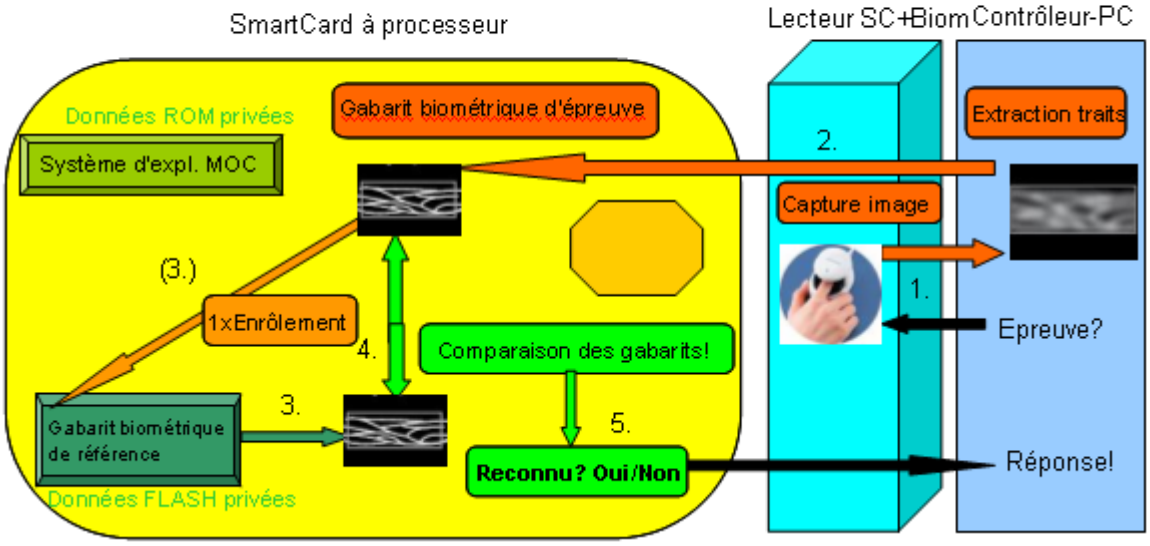
B) Vérification:

1) Capture de la donnée de biométrique (donnée brute) d'épreuve à l'aide du contrôleur (PC)
2) Extraction des traits distinctifs d'épreuve (=> gabarit biométrique d'épreuve)
3) Envoi du gabarit biométrique de référence au contrôleur (PC)
4) Comparaison sur le contrôleur des échantillons de référence et d'épreuve.
5) Reconnaissance: Oui/non sur le contrôleur (PC).

Dans ce cas, les personnes concernées ont un contrôle partiel de l'usage de leurs données biométriques de référence stockées sur la carte.

Lors de la vérification, les données biométriques nécessaires sont lues par le lecteur de smartcards et transmises au système de reconnaissance. A cette occasion, une copie non autorisée des données biométriques n'est pas exclue.

Comparaison biométrique sur carte



A) Enrôlement:

1) Capture des données biométriques de référence (données brutes) à l'aide du contrôleur (PC)
2) Extraction des traits distinctifs de référence à l'aide du contrôleur (PC) et envoi du gabarit biométrique de référence à la carte.
3) Stockage du gabarit biométrique de référence sur la carte.

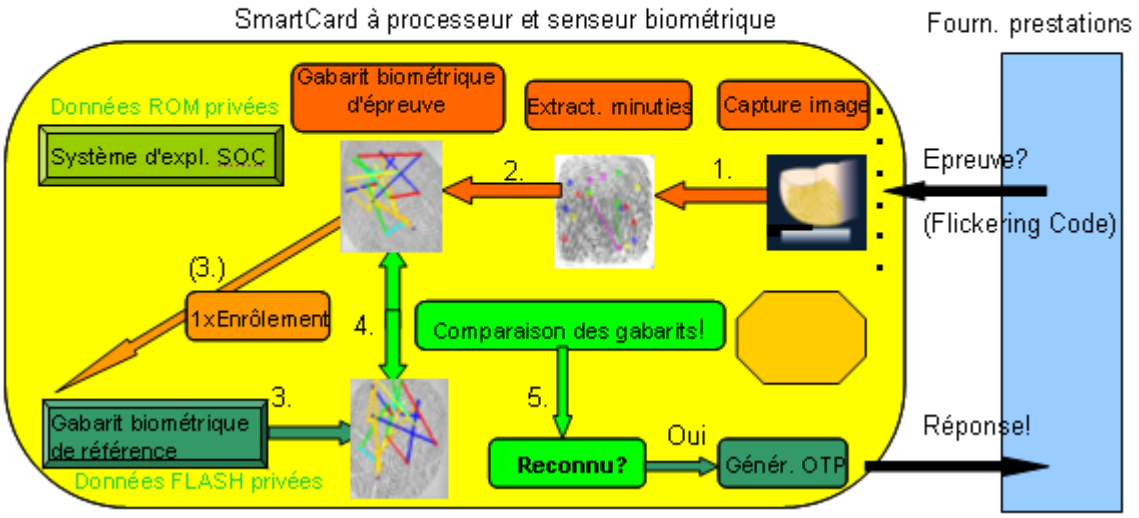
B) Vérification:

1) Capture de la donnée de biométrique (donnée brute) d'épreuve à l'aide du contrôleur (PC)
2) Extraction des traits distinctifs d'épreuve (=> gabarit biométrique d'épreuve)
3) Envoi du gabarit biométrique de référence à la carte
4) Comparaison sur la carte des données de référence et d'épreuve
5) Reconnaissance: Oui/non transmis au contrôleur (PC).

Une smartcard avec comparaison biométrique sur carte dispose d'une unité de calcul autonome, de sorte que la comparaison entre les caractéristiques biométriques (gabarit biométrique d'épreuve) et les données biométriques stockées localement (gabarit biométrique de référence) est réalisée sur la carte. Le système de contrôle d'accès reçoit uniquement une acceptation ou un rejet de la carte, aucune donnée biométrique ne lui est transmise. Ainsi, les personnes concernées ont le contrôle sur leurs données biométriques, ainsi que les données de transactions relatives au processus de comparaison. Par contre, elles ne sont pas en mesure de contrôler l'utilisation qui est faite des données de transaction échangées entre le lecteur et la carte.

Système biométrique sur carte

(System on card – encapsulated biometrics)



A) Enrôlement:

1) Capture des empreintes digitales de référence sur la carte
2) Extraction des minuties de référence sur la carte
3) Stockage du gabarit biométrique de référence sur la carte.

B) Vérification:

1) Capture des empreintes digitales d'épreuve sur la carte
2) Extraction des minuties d'épreuve et création du gabarit biométrique d'épreuve
3) Lecture des données de référence sur la carte
4) Comparaison sur la carte des gabarits de référence et d'épreuve
5) Reconnaissance: si réussie, génération d'un «mot de passe à usage unique» (One Time Password) pour le fournisseur de prestations.

Les personnes concernées ont le contrôle complet de l'utilisation de leurs données biométriques stockées sur la carte, car cette dernière dispose d'une unité de calcul et d'un lecteur biométrique. Il n'y a ainsi aucun échange de données biométriques de référence ou de données de transaction entre la carte et le système de contrôle d'accès. En l'occurrence, le fournisseur de prestations ne reçoit du système biométrique sur carte qu'un «mot de passe à usage unique», qui ne peut être généré puis utilisé que par une personne authentifiée.

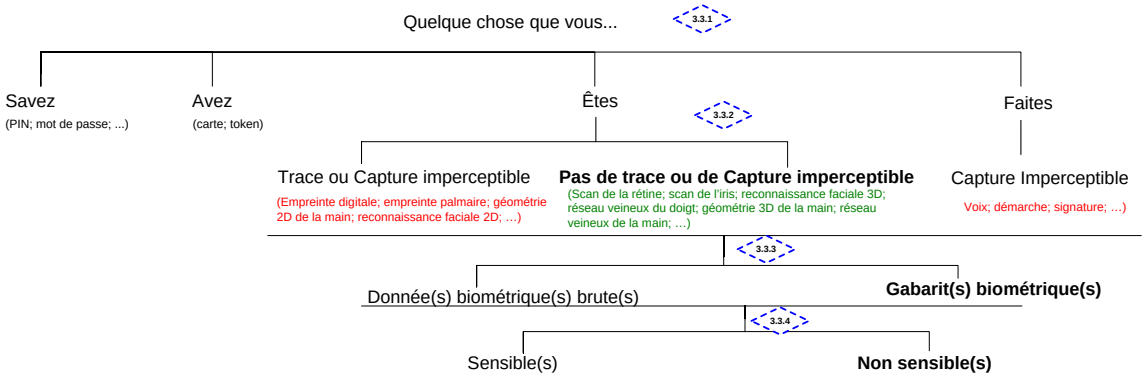
3.2.4 Quels sont les motifs justificatifs du traitement?

Tout traitement de données personnelles par les organes fédéraux doit reposer sur une base légale. De plus, des données sensibles ou des profils de personnalité ne peuvent être traités que si une loi au sens formel le prévoit expressément. En revanche, les motifs justifiant le traitement de données personnelles par des personnes privées sont: soit le consentement de la personne concernée, soit un intérêt public ou privé prépondérant, soit la loi. Le consentement doit être libre, spécifique et informé. Cela suppose que les personnes concernées soient dûment informées et qu'une alternative à la reconnaissance biométrique soit mise à leur disposition pour autant que les finalités ne s'en trouvent pas mises en cause.

3.3 Moyens de reconnaissance

Le respect du principe de proportionnalité lors du choix des moyens de reconnaissance est essentiel. Aussi, lors du choix des modalités de reconnaissance biométrique (vérification ou identification), des caractéristiques biométriques, des données biométriques stockées et du type de donnée (à caractère sensible ou non); il convient de choisir les moyens adéquats, nécessaires et non excessifs au regard des finalités du traitement; c'est-à-dire les technologies biométriques les moins intrusives parmi celles aptes à atteindre les finalités recherchées.

Moyens de reconnaissance (les solutions recommandées figurent **en gras**)



3.3.1 Quelles modalités sont utilisées pour procéder à la reconnaissance ?

3.3.2 S'agit-il de caractéristiques biométriques pour lesquelles des traces sont laissées dans la vie quotidienne ou est-il possible de capturer ces caractéristiques biométriques à l'insu de la personnes concernées (i.e. de manière imperceptible)

3.3.3 Des données biométriques biométriques brutes et/ou dérivées sont-elles stockées ?

3.3.4 S'agit-il de données sensibles au sens de l'art. 3 lit. c LPD ?

3.3.1 Quelles modalités sont utilisées pour procéder à la reconnaissance?

Outre les modalités biométriques, quelques chose que vous êtes – *something you are* (physiologique) ou quelque chose que vous faites – *something you do* (comportementale), il y a les moyens traditionnels d'authentification, à savoir quelque chose que vous savez – *something you know* (NIP, mot de passe, …) ou quelques chose que vous avez – *something you have* (les cartes, jetons, clés, badges, …) avec ou sans contact.

Le processus de vérification biométrique, devra dans la mesure du possible avoir lieu sur la base d'une donnée biométrique (voire plusieurs, si cela est justifié au regard des circonstances); éventuellement complété par des moyens traditionnels d'authentification.

Pour les processus d'identification biométrique, un seul échantillon conduit de manière générale à un groupe de personnes plus ou moins large. De ce fait, l'identification individuelle n'est possible qu'à l'aide d'indices complémentaires; notamment des échantillons biométriques supplémentaires et/ou tout indice pertinent.

La question de la compatibilité des finalités pose également le problème de l'interopérabilité de différents systèmes reposant sur la biométrie. La standardisation qu'exige l'interopérabilité a pour conséquence une augmentation de l'éventail des possibilités d'interconnexion entre des bases de données.

3.3.2 S'agit-il de caractéristiques biométriques pour lesquelles des traces sont laissées dans la vie quotidienne ou est-il possible de capturer ces caractéristiques biométriques à l'insu de la personne concernée (de manière imperceptible)?

Certaines caractéristiques biométriques sont susceptibles d'être capturées et utilisées à l'insu des personnes concernées. Dans la vie courante, chacun laisse des traces, plus ou moins facilement exploitables, de différentes caractéristiques biométriques. De plus, certaines données biométriques sont susceptibles d'être capturées à l'insu des personnes concernées.

Les technologies reposant sur des données biométriques ne laissant pas ou peu de traces et ne permettant pas une capture à l'insu des personnes concernées doivent être privilégiées[6].

[6] Comme le groupe de l'art. 29 l'a précisé dans le document de travail sur la biométrie, n° 80 du 1er août 2003, «L'utilisation, à des fins de contrôle d'accès (authentification/vérification), de systèmes biométriques se référant à des caractéristiques physiques qui ne laissent pas de traces (par exemple la forme de la main, mais non les empreintes digitales) ou de systèmes biométriques se référant à des caractéristiques physiques qui laissent des traces, mais dont les données ne sont pas enregistrées dans une mémoire détenue par une personne autre que la personne concernée (autrement dit, les données ne sont pas mises en mémoire dans le dispositif de contrôle d'accès ou dans une base de données centrale), crée moins de risques pour la protection des libertés et des droits fondamentaux de la personne».

3.3.3 Des données biométriques brutes et/ou dérivées (gabarits biométriques - *templates*) sont-elles stockées?

Les données dérivées contiennent moins d'informations sur les personnes concernées, leur utilisation doit être privilégiée. L'objectif est d'extraire un nombre suffisant de traits distinctifs pour les finalités recherchées.

En outre, si des données brutes sont stockées, il convient d'énoncer les motifs justificatifs de ce traitement.

3.3.4 S'agit-il de données sensibles au sens de l'art. 3 lit. c LPD?

Les données biométriques sont des données personnelles. Selon les caractéristiques biométriques traitées, les données biométriques sont susceptibles de contenir des informations complémentaires relatives à la race ou à la santé; dans ce cas il s'agit de données sensibles au sens de l'art. 3 lit. c LPD. A la lumière des recherches scientifiques menées à ce jour, l'empreinte digitale, la géométrie de la main et du visage, la numérisation de l'iris et la reconnaissance vocale entre autres contiennent des informations complémentaires relatives à la race ou la santé.

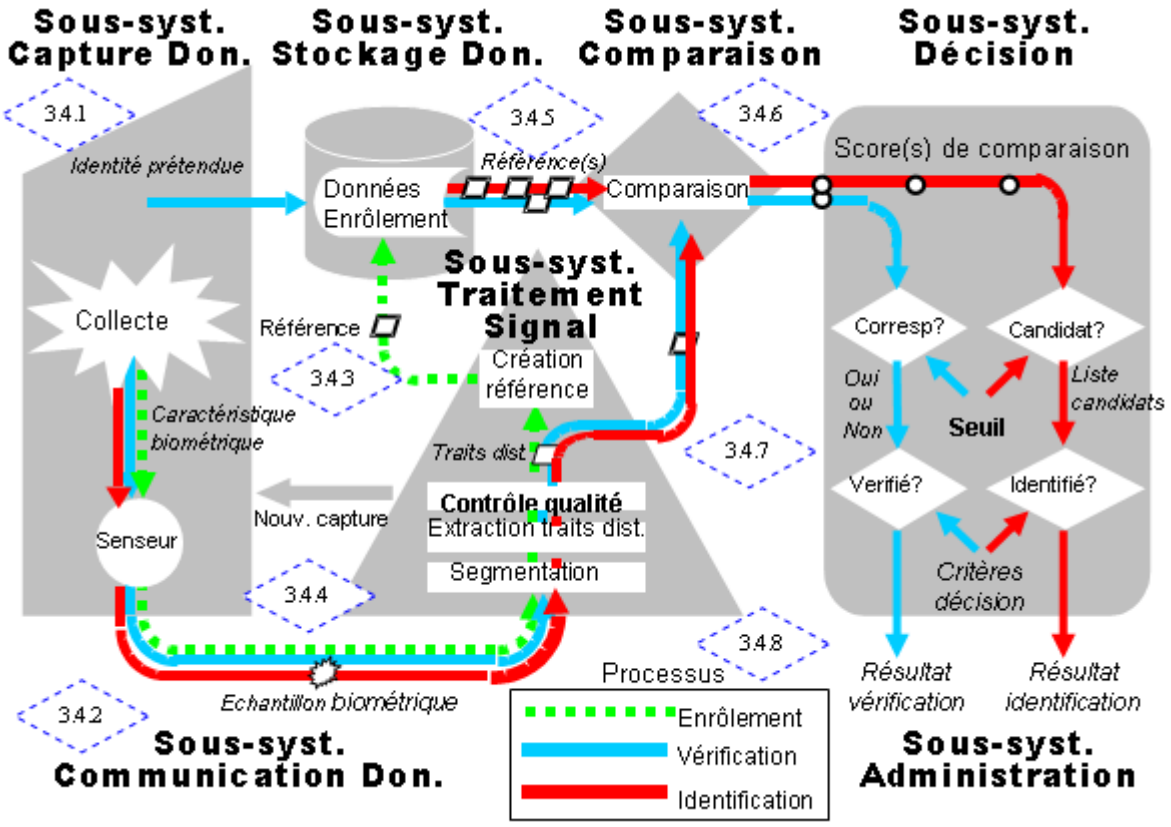
3.4 Sécurité des données et fiabilité du système

3.4.1 Quelle est l'architecture du système de reconnaissance biométrique?

Les systèmes de reconnaissance comportent trois phases essentielles: l'enregistrement préalable, les vérifications ou identifications subséquentes, suivies des autorisations d'accès accordées à la personne reconnue (authentifiée). Dans notre contexte, la phase d'enregistrement comprend en premier lieu l'identification formelle de la personne concernée, suivie de l'enrôlement biométrique. Malgré la grande diversité de finalité(s) et de mise en œuvre des systèmes de reconnaissance biométrique, ces derniers ont néanmoins bon nombre d'éléments en commun, qui permettent d'esquisser une description générale.

En principe, un système de reconnaissance biométrique comprend les sous-systèmes de capture des données, de communication des données, de traitement du signal, de stockage des données, de comparaison, de décision et d'administration.

Représentation conceptuelle d'un système de reconnaissance biométrique:



3.4.1 Quelle est l'architecture du système de reconnaissance biométrique ?

3.4.2 Quelles sont les mesures de sécurité mises en place ?

3.4.3 Quel est le fonctionnement du processus d'enrôlement biométrique ?

3.4.4 Quelle est la proportion d'échecs à l'enrôlement (FTE) ?

3.4.5 Quel est le nombre prévu de personnes enrôlées ?

3.4.6 Quel est le fonctionnement du processus de reconnaissance biométrique ?

3.4.7 Quel est le seuil d'acceptation choisi, en fonction du taux tolérable de fausses acceptations ? Quel est en conséquence le taux de faux rejets?

3.4.8 Y a-t-il une journalisation des processus biométriques (enrôlement et reconnaissance), dans l'affirmative lesquels ?

Les échantillons biométriques capturés sont prélevés sur une personne à l'aide d'un senseur. Les données issues du senseur sont transmises à un processeur, qui en extrait de manière reproductible des mesures distinctives (traits), en éliminant tous les autres composants. Les traits résultants peuvent être stockés dans une base de données comme une référence, parfois appelée référence ou gabarit biométrique. Dans certains cas, l'échantillon brut (sans extraction de traits) peut être stocké comme référence biométrique. Un nouvel échantillon peut être comparé à une référence spécifique, à plusieurs références ou à toutes les références présentes dans la base de données, afin d'établir s'il y a correspondance ou pas. Une décision au sujet de l'identité prétendue ou recherchée est rendue sur la base de la similarité entre les traits de l'échantillon et ceux de la (ou des) référence(s) comparées.

Les **sous-systèmes** d'un système de reconnaissance biométrique fonctionnent comme suit:

- capture des données: collecte d'une image ou d'un signal tiré de la caractéristique biométrique présentée par un sujet au senseur biométrique, lequel restitue cette image ou ce signal sous la forme d'un échantillon biométrique capturé. Il est important que le senseur détecte le caractère vivant de la caractéristique présentée (fiabilité) et préférable qu'il ne requiert pas de contact physique avec celle-ci (acceptation, sécurité).

- communication des données: assure la transmission des échantillons, traits, références, résultats et décisions entre les différents sous-systèmes, éventuellement à l'aide de formats standards d'échange de données biométriques. L'échantillon biométrique capturé peut être compressé et/ou chiffré avant la transmission et décompressé et/ou déchiffré avant utilisation, le chiffrement étant en particulier recommandé pour assurer la confidentialité et l'intégrité des données transmises.

- traitement du signal: comprend en principe un processus de **segmentation** visant à localiser le signal de la caractéristique du sujet dans l'échantillon biométrique capturé, un processus **d'extraction de traits** permettant d'extraire de manière reproductible les traits distinctifs de l'échantillon biométrique capturé, et un processus de **contrôle de qualité** évaluant la validité des échantillons, traits, références, etc, avec la possibilité de retourner le contrôle au sous-système de capture pour collecter d'autres échantillons ou de modifier les paramètres de segmentation ou d'extraction.

- stockage des données: l'ensemble des références stockées constituent une «**base de données d'enrôlement»**, comprenant éventuellement d'autres détails sur le sujet enrôlé ou sur le processus d'enrôlement. Les références peuvent être stockées dans l'appareil de capture, sur un média portable (smartcard), sur un PC ou serveur local ou encore dans une base de données centrale.

- comparaison: les traits sont comparés à une (vérification) ou plusieurs (identification) référence(s) et les **résultats de comparaison** (degré de correspondance) sont transmis au sous-système de décision.

- décision: la comparaison est considérée comme **réussie** lorsque le résultat de comparaison est supérieur ou égal à un **seuil d'acceptation** (threshold) prédéfini, comme **échouée** sinon. Dans le cadre d'une identification, la réussite conduit à une **liste de candidats** potentiels.

- administration: pilote l'ensemble du système biométrique, en permettant par exemple de renseigner le sujet pendant ou après la capture, de définir le seuil d'acceptation ou tout autre paramètre influençant le comportement global du système, de journaliser ou non (logfiles) les événements survenus dans le système ou encore d'interfacer l'application principale exploitant le système biométrique.

Vu la complexité d'un tel système, il est clair que sa sécurité est tributaire de chacun des sous-systèmes impliqués, de sorte que la disponibilité de solutions ou *produits au bénéfice d'une certification en matière de protection des données* (art. 5 OCPD dès le 01.01.2010) pourrait être un avantage. Il n'en reste pas moins que la mise en œuvre d'un tel système, même basé sur des produits certifiés, reste une tâche compliquée, qui requiert une attention soutenue et permanente (lors de la création et de la maintenance des systèmes de reconnaissance) pour respecter au mieux les exigences de protection des données.

3.4.2 Quelles sont les mesures de sécurité mises en place?

Des mesures techniques et organisationnelles adaptées à la sensibilité des données biométriques traitées et permettant d'empêcher les accès indus doivent être mises en places. Les contrôles d'accès peuvent être physiques ou logiques (relatifs aux systèmes ou aux données).

Ceci concerne tout particulièrement les sous-systèmes de stockage et de communication des données.

3.4.3 Quel est le fonctionnement du processus d'enrôlement biométrique?

Lors de l'enrôlement, une donnée biométrique brute est dans un premier temps saisie à l'aide d'un capteur, puis l'image est analysée et un gabarit biométrique en est extrait. Dans cette optique, comment sont extraits les points caractéristiques (*features*) et combien sont retenus pour constituer le gabarit biométrique (est-il possible de moduler, réduire le nombre de points caractéristiques)?

3.4.4 Quelle est la proportion d'échec à l'enrôlement (FTE)?

Le taux d'erreurs à l'enrôlement rend explicites les difficultés que les personnes concernées peuvent rencontrer durant ce processus; ce facteur est fortement dépendant de la caractéristique biométrique utilisée. Il est par conséquent nécessaire de prévoir une voie alternative à la reconnaissance biométrique (principe de non-discrimination).

3.4.5 Quel est le nombre prévu de personnes enrôlées?

Le nombre de personnes enrôlées est particulièrement important dans le cadre d'un processus d'identification, étant donné qu'il conditionne la dimension de la base de données centralisée et de facto la taille de la liste de candidats produite par la comparaison 1-N. À cet égard, il faut relever qu'une identification entièrement automatisée n'est réalisable en pratique que si cette liste ne comprend jamais plus d'un seul candidat. En revanche, dès que la liste contient plus d'un candidat, l'identification doit être achevée, en règle générale «manuellement», sur la base de critères additionnels.

3.4.6 Quel est le fonctionnement du processus de reconnaissance biométrique?

Le processus de reconnaissance biométrique consiste à vérifier l'identité prétendue ou identifier un individu en comparant une donnée biométrique de référence (collectée lors de l'*enrôlement biométrique)* avec la donnée biométrique d'épreuve (collectée lors de la procédure de reconnaissance). Il est important de souligner le caractère probabiliste de la reconnaissance

biométrique. En effet, suite à la comparaison des données biométriques, un taux de similitude est obtenu. Le système biométrique ne «reconnaîtra» la personne que si ce taux atteint ou dépasse le seuil d'acceptation préalablement fixé.

3.4.7 Quel est le seuil d'acceptation choisi, en fonction du taux tolérable de fausses acceptations? Quel est en conséquence le taux de faux rejets?

Plus le seuil d'acceptation est placé haut, plus le taux de faux rejets (*FRR*) augmente, ce qui signifie que des personnes enrôlées ne seront parfois pas reconnues. Un abaissement du seuil d'acceptation permet d'abaisser ce taux de faux rejets, mais avec la conséquence fâcheuse d'une hausse proportionnelle du taux de fausses acceptations (*FAR*), ce qui implique une augmentation du risque non bénin d'usurpation d'identités.

3.4.8 Y a-t-il une journalisation des processus biométriques (enrôlement et reconnaissance), dans l'affirmative lesquelles?

Ce traitement de données (création, conservation, destruction ou anonymisation de fichiers journaux) doit répondre aux principes de finalité et de proportionnalité.

3.5 Droits des personnes concernées

3.5.1 Quelles sont les mesures mises en places afin de garantir les droits des personnes concernées?

Les personnes concernées doivent pouvoir faire valoir leur droit d'accès et le cas échéant demander que leurs données personnelles soient rectifiées, détruites ou signalées comme litigieuses s'il n'est pas possible d'établir l'inexactitude de celles-ci.

De plus, si des données personnelles sensibles sont traitées ou des profils de personnalité réalisés, les personnes concernées doivent être dûment informées. Les personnes concernées doivent au minimum être informées de l'identité du maître de fichier, des finalités du traitement pour lequel les données sont collectées et des catégories de destinataires des données si la communication des données est envisagée.

Enfin, une alternative à la reconnaissance biométrique doit être mise en place afin d'éviter toute discrimination des personnes qui ne seraient pas en mesure d'utiliser un système de reconnaissance biométrique (ne possédant pas les données biométriques requises ou si la qualité de ces données n'est pas suffisante). De plus, une alternative doit également être mise à disposition de toute personne qui ne souhaite pas que ses données biométriques soient utilisées à des fins de reconnaissance, pour autant que la finalité visée ne s'en trouve pas mise en cause.

3.5.2 Le fichier a-t-il été déclaré au PFPDT?

La déclaration des fichiers et la tenue par le Préposé fédéral à la protection des données et à la transparence (PFPDT) d'un registre des fichiers accessible en ligne a pour objectif d'assurer d'une part la transparence et de facilité l'exercice de leurs droits aux personnes concernées ainsi que l'activité de surveillance du PFPDT.

Les organes fédéraux et les personnes privées qui traitent régulièrement des données sensibles, des profils de personnalité ou qui communiquent régulièrement des données personnelles à des tiers sont tenus de déclarer leurs fichiers au PFPDT sous réserve des exceptions prévues à l'art. 11a al. 5 LPD. Pour plus d'informations concernant les modalités d'annonce des fichiers, veuillez consulter le site internet du PFPDT (www.edoeb.admin.ch).