Le Préposé fédéral suppléant

Eidgenössischer Datenschutzbeauftragter
Préposé fédéral à la protection des données
Incaricato federale per la protezione dei dati
Swiss Federal Data Protection Commissioner

A2004.08.24-0004 / 2004-00092

25.08.2004/WJ

26e Conférence internationale des Commissaires à la protection des données et à la vie privée

Wroclaw, 14 – 16 septembre 2004

Quelques aspects de protection des données lors de l'utilisation de données biométriques dans le secteur privé

Jean-Philippe Walter
Dr. en droit
Préposé fédéral suppléant à la protection des données,
Berne (Suisse)

L'utilisation de la biométrie n'est plus essentiellement réservée à des secteurs particuliers comme la poursuite ou la répression pénale. Elle se généralise et s'étend à de nombreuses applications dans le secteur public et le secteur privé. La biométrie n'est pas seulement une technique, mais d'abord une caractéristique propre de tout être vivant. Il y a une tendance à la banalisation de données personnelles provenant de la personne. La biométrie présente des risques quant au respect des droits et des libertés fondamentales et par conséquent est un enjeu de taille pour la protection des données. Elle peut également être un instrument de protection de la vie privée (PET). La collecte et le traitement de données biométriques doivent intervenir dans le respect des exigences de protection des données et en particulier des principes de base (notamment licéité, bonne foi, finalité, proportionnalité, sécurité et droits de personnes concernées). La biométrie n'est pas la solution à tous nos problèmes de sécurisation des systèmes d'informations ou d'installations sensibles. Il faut rester prudent quant aux utilisations qui peuvent en être faites. Dans le secteur privé, l'utilisation de la biométrie comme moyen d'authentification est le plus souvent suffisant. On ne recourra à la biométrie que s'il n'y a pas d'autres moyens moins intrusifs d'atteindre l'objectif visé ou si elle est un élément de protection des données. En cas de recours à la biométrie, on privilégiera des éléments biométriques qui limitent le risque d'abus, tel que ceux qui ne laissent pas de trace. Les systèmes d'informations biométriques doivent faire l'objet de procédures de certification et d'audit de protection des données.

The use of biometrics is not primarily limited to special branches like criminal prosecution anymore. More and more, its scope in the public as well as the private sector is expanding. However, biometrics is not only a technology, but first and foremost a characteristic of every living creature. There is a tendency to trivialize human personal data. As a threat to fundamental rights and freedoms, biometrics constitutes an important challenge with regard to data protection. At the same time, biometrics can serve as an instrument for the protection of privacy (PET). The collection and processing of biometric data must be conducted only in accordance with the requirements of data protection regulations and especially with the basic principles (lawfulness, good faith, purpose-link, data security, proportionality and rights of the persons concerned).

Jean-Philippe Walter
Tel +41 (0) 31 322 41 31

Feldeggweg 1
CH-3003 Berne
Fax +41 (0) 31 325 99 96
www.edsb.ch

Biometrics is not the solution to all our problems in the area of safeguarding information systems or sensitive installations – on the contrary, the technology has to be applied cautiously. In the private sector, it is in most cases sufficient to use biometrics as a means of authentication – and even then, only if there are no measures with a less drastic impact on privacy, or if the use of biometric means serves data protection purposes. If biometrics has to be used, priority will be on those biometric elements that are the least likely to be abused, e.g. those that leave no traces. Biometric information-systems must be submitted to data protection certification and audit procedures.

1. Généralisation et banalisation de la biométrie

Longtemps la biométrie était réservée à des secteurs particuliers et a été utilisée presque essentiellement dans le domaine de la justice et notamment de la poursuite et de la répression pénale aux fins d'identification. Pour le commun des mortels, la prise d'empreinte digitale avait – et a encore - une connotation policière et pénale. Pour beaucoup d'entre-nous, la biométrie appartenait, il y a peu encore, aux romans d'espionnage ou de science-fiction. Aujourd'hui, l'utilisation de la biométrie a tendance – et ce pas seulement à cause des événements du 11 septembre 2001 – à se généraliser, voire même à se banaliser. Les méthodes d'examen de l'identité d'une personne ayant accès à des domaines sensibles en terme de sécurité et de confidentialité sont aujourd'hui essentielles, notamment dans un environnement ouvert tel que l'internet[1]. Les applications biométriques ne se limitent plus au domaine de la lutte contre le crime et le terrorisme ou la garantie de la sécurité publique[2]. L'utilisation de la biométrie est de plus en plus répandue dans le secteur de l'immigration et du contrôle aux frontières. Elle s'étend également à toute la société civile, dans des procédures automatisées d'authentification et d'identification allant de l'accès à une cantine scolaire, en passant par le paiement d'un titre de transport sur un ferry, au contrôle du temps de travail, tests de présence ou au contrôle d'accès à des installations ou à des systèmes informatiques. La biométrie pourrait ainsi remplacer nos codes d'accès aux ordinateurs ou aux guichets bancaires automatisés. Elle pourrait permettre d'effectuer des transactions sécurisées sur Internet et rendre nos cartes de crédit superflues. Cette banalisation, qui fait du corps un mot de passe, se voit renforcée par la baisse des coûts et le développement de nouvelles technologies qui risquent de favoriser une prolifération d'applications diverses et de banques de données biométriques. Elle est également encouragée par la commodité de certaines de ces applications. «Le champ d'application de ces techniques s'étend sans cesse grâce aux progrès réalisés dans la qualité et la miniaturisation des appareils de capture, ainsi que dans l'augmentation de puissance des microprocesseurs. » [3]. Les préoccupations de sécurité ne sont ainsi pas le seul fait des autorités publiques, mais concernent également les entreprises, notamment en lien avec l'accès à des informations ou des installations sensibles.

La biométrie est en soi la forme la plus ancienne d'identification : tout homme est reconnaissable à son visage. Ce qui rend la biométrie attractive est la possibilité de stockage des informations dans des banques de données.

---

[1] Brigitte Wirtz, Biometrische Verfahren, dans DuD 23 (1999) 3, p. 199.

[2] Christian Cabal, Les Méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en oeuvre, Rapport de l'Office parlementaire d'évaluation des choix scientifiques et technologiques à l'Assemblée nationale et au Sénat français, juin 2003 (1ère partie) (ci-après Rapport Cabal). Voir aussi Claudia Golembiewski, Thomas Probst, Datenschutzrechtliche Anforderungen an den Einsatz biometrischer Verfahren in Ausweispapieren und bei ausländerrechtlichen Identitätsfestellungen, Rapport publié par Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel, juillet 2003; Hans-Jürgen Burger, Biometrie, Medium zur Katalogisierung des Menschen ?, dans Datenschutz Nachrichten, 2/2004, p. 5; Lukas Gundermann, Marit Köhntopp, Biometrie zwischen Bond und Big Brother, dans DuD 23 (1999) 3, p. 143.

[3] CNIL, 24e Rapport d'activité 2003, p. 36.

La biométrie se base sur l'analyse de données liées à l'individu et peut être classées en trois grandes catégories :

- le traitement basé sur l'analyse morphologique, telle que l'empreinte digitale, la forme de la main, le réseau veineux de la rétine ou l'iris ;
- l'examen des traces biologiques, telles que l'odeur, la salive, l'urine, le sang ou l'ADN ;
- le traitement basée sur l'analyse comportementale, telle que la dynamique du tracé de la signature ou la frappe sur un clavier d'ordinateur[4].

Le processus de reconnaissance biométrique[5] est en règle générale toujours le même. On prélève tout d'abord un échantillon de référence, lequel est enregistré dans une banque de données (c'est la phase d'enrôlement). Sur le base du traitement de cet échantillon, un gabarit est créé et stocké en relation avec une identité déclarée. Cette saisie initiale peut se faire à la connaissance de la personne concernée et avec sa participation. Elle peut aussi intervenir à son insu, notamment lors de la collecte d'empreintes digitales sur des objets ou de prises de vue (photos, vidéo). Pour reconnaître une personne, on procède ensuite à une deuxième collecte d'échantillon biométrique dont le gabarit sera comparé avec le gabarit de référence. En cas d'équivalence, la reconnaissance est positive.

Le recours à la biométrie présente des avantages pour les entreprises et les personnes concernées[6] pour autant que les systèmes offrent un haut degré de fiabilité :

- identification positive, notamment dans le cadre de transactions commerciales ;
- lutte contre la fraude lors de l'utilisation de cartes de crédit ;
- prévention contre la vol d'identité ;
- rétablissement d'identité
- sécurité des données (accès aux données)
- authentification des données (chiffrement des données avec une clef biométrique)
- contrôle d'accès physique.

Il ne faudrait cependant pas voir dans la biométrie la solution à tous nos problèmes de sécurisation des systèmes d'informations ou d'installations sensibles. Il faut rester prudent quant aux utilisations qui peuvent en être faites. Cette technique a tendance à créer un faux sentiment de sécurité, notamment du fait du caractère publique et non répudiable de la donnée biométrique, de la multiplication des banques de données biométriques et des possibilités relativement aisées d'usurpation de l'identité d'une personne[7].

Le recours à la biométrie présente en outre des risques quant au respect des droits et des libertés fondamentales et est par conséquent un enjeu de taille pour la protection des données.

---

[4] CLUSIF, Techniques de contrôle d'accès par biométrie, 2003, https://www.clusif.asso.fr/fr/production/ouvrages/pdf/ControlesAccesBiometrie.pdf

[5] Claudia Golembiewski, Thomas Probst, Datenschutzrechtliche Anforderungen an den Einsatz biometrischer Verfahren, op. cit.; CLUSIF, op. cit., p. 17ss.

[6] Ann Cavoukian, Consumer Biometric Applications: A Discussion Paper, September 1999, http://www.ipc.on.ca/docs/cons-bio.pdf

[7] Philippe Wolf, De l'authentification biométrique, dans Sécurité Informatique – octobre 2003 n° 46, www.cnrs.fr/Infosecu/Revue.html; Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada, Satoshi Hoshino, Impact of Artificial « Gummy » Fingers on Fingerprint Systems, janvier 2002, http://cryptome.org/gummy.htm ; voir aussi étude de la Deutsche Bank citée par Rapport Cabal, p. 51

2. Enjeux liés aux droits et libertés fondamentales

2.1. Caractéristique propre à tout être humain

Par rapport aux enjeux liés aux droits et libertés fondamentales et notamment le droit à la protection des données, l'utilisation de la biométrie apparaît complexe, voire ambiguë. Il convient en premier lieu de rappeler et de souligner que la biométrie ne peut pas simplement être ramenée à une technique ou une technologie et ainsi favoriser la banalisation des conséquences ou des risques pour les droits fondamentaux des individus. L'information biométrique est d'abord et avant tout une caractéristique propre de tout être vivant et par conséquent un élément de la personne humaine. Il s'agit d'éléments humains révélant des informations de la personne. Le terme « biométrie » nous vient du grec « bios » (vie) et « metron » (mesure).

Les données biométriques sont « d'une nature particulière puisqu'elles ont trait aux caractéristiques comportementales et physiologiques d'une personne et peuvent permettre de l'identifier sans ambiguïté. »[8] Pour une part, elles proviennent de la « capture » directe ou indirecte de caractéristiques du corps humain. La collecte et le traitement de ces caractéristiques peuvent porter atteinte à son intégrité, voire même à la dignité humaine.

2.2. Dignité humaine

La dignité humaine sera atteinte dès lors qu'un être humain est réduit à un objet et à un moyen qui débouche sur un dénigrement de son identité personnelle. Tel peut être le cas lorsque des données biométriques sont prélevées sous contrainte, lorsqu'il y a des risques de connecter des données provenant de différentes sources, lorsque l'individu n'a aucun contrôle sur ce qui se passe avec les données le concernant ou lorsque des données supplémentaires sont prélevées au moment du traitement des données biométriques [9] : Par exemple, un système d'accès basé sur le scan de la rétine qui mesurerait en même temps si l'employé a consommé de l'alcool ou des drogues et qui le cas échéant bloquerait l'accès aux installations.

Certaines personnes seront indifférentes à l'utilisation de données biométriques les concernant. D'autres éprouveront une résistance psychologique à l'idée que leur corps soit utilisé comme une source d'information. D'autres encore n'accepteront pas qu'une partie de leur corps, ne serait-ce qu'un doigt, soit « analysée » par une machine. Enfin, certaines personnes exprimeront leur inquiétude face à la banalisation du corps humain qui semble se dessiner dans les décisions concernant l'utilité d'appliquer telle technique plutôt qu'une autre. Cette résistance peut dépendre de facteurs socioculturels, religieux ou propres à chaque individu.[10]

La biométrie n'est pas un simple moyen d'identification. Elle pourrait mettre en péril le sens de l'individualité[11] et la liberté individuelle, les possibilités d'utiliser plusieurs identités et

---

[8] Groupe de travail „Article 29" sur la protection des données, Document de travail sur la biométrie, adopté le 1er août 2003

[9] Lukas Gundermann, Marit Köhntopp, op. cit., dans DuD 23 (1999) 3, p. 146s.

[10] Comité consultatif de la Convention 108, Projet de rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement de données biométriques, Rapport non encore publié ; voir aussi Ann Cavoukian, Consumer Biometric Applications: A Discussion Paper, September 1999, http://www.ipc.on.ca/docs/cons-bio.pdf, p. 29s.

[11] Davies, Touching Big Brother, how biometric technology will fuse flesh and machine, dans Information Technology § People, Vol 7, No 4 1994, http://www.privacy.org/pi/reports/biometric.html

favoriser la surveillance ou le contrôle social[12]. Ces considérations ou ces craintes doivent être prises en considération pour définir les mesures de protection des données à respecter.

On ne peut en effet ignorer les craintes de surveillance à partir des données biométriques identifiables. « Les empreintes digitales, et la gamme d'indices habituellement visées par la biométrie, notamment la rétine, l'iris, la main et les empreintes vocales, offrent une preuve irréfutable de l'identité d'une personne puisqu'elles constituent des caractéristiques biologiques uniques qui distinguent une personne d'une autre et ne peuvent être associées qu'à une seule personne. Une empreinte digitale identifiable peut s'avérer un identificateur unique puissant qui permet de regrouper les divers renseignements personnels concernant un particulier. Elle permet également de réunir des renseignements personnels provenant de sources différentes et de réaliser un profil de la personne, à son insu. »[13]

La biométrie peut aussi être source de discrimination. Certaines personnes handicapées pourraient se voir préjudicier selon le type de données biométriques retenues. Le risque que la biométrie s'impose dans de grands secteurs d'activités de la société pourrait entrainer une marginalisation des personnes qui ne peuvent ou ne veulent pas utiliser des systèmes biométriques[14].

2.3. Identifiant unique et universel

La biométrie présente également la particularité, du moins lorsqu'il s'agit de caractéristiques physiologiques, d'être composée d'éléments universels, uniques et permanents. Il en résulte qu'en principe, la caractéristique sera inaltérable tout au long de l'existence d'une personne et l'exposera à une identification permanente, avec certains risques de contrôle plus étroit de la part des responsables de traitement, mais aussi d'utilisation illicite des données. Sans garde-fou, la biométrie pourrait être utilisée comme identifiant universel de manière généralisée.

Le caractère non altérable et permanent des données biométriques doit néanmoins être quelque peu relativisé. Une caractéristique physique peut être altérée avec le temps ou selon les circonstances, notamment suite à un accident. Une caractéristique physiologique peut se modifier volontairement ou involontairement, en fonction de la situation, notamment de l'état de stress dans lequel se trouve la personne.

3. Implications de protection des données

3.1. Données à caractère personnel

Pour pouvoir examiner les implications en terme de protection des données de l'utilisation de données biométriques, il convient au préalable d'examiner si ces données sont des données à caractère personnel au sens de l'article 2, lettre a de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, à savoir des informations concernant une personne physique identifiée ou identifiable. L'article 2, lettre a de la directive européenne 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à

[12] Roger Clarke, Biometrics and Privacy, http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html ; Lukas Gundermann, Marit Köhntopp, op. cit., dans DuD 23 (1999) 3, p. 144

[13] Ann Cavoukian, Vie privée et biométrie : concepts opposés ou à réexaminer ?, février 1998, http://www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=11552&N_ID=1&PT_ID=11528&U_ID=0

[14] Simon G. Davies, Touching Big Brother, How biometric technology will fuse flesh and machine, dans Information Technology § People, vol. 7, N° 4 1994, www.privacy.org/pi/reports/biometric.html

caractère personnel et à la libre circulation de ces données précise en outre qu'une personne est réputée identifiable lorsqu'elle « peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale. » Dans plusieurs recommandations du Conseil de l'Europe, il est enfin précisé qu'une personne physique n'est pas considérée comme « identifiable » si cette identification nécessite des délais et des activités déraisonnables[15]. Ainsi, une personne est identifiée lorsqu'il ressort directement des données qui sont traitées qu'il s'agit d'une personne déterminée et d'elle seule. Tel est le cas lorsque les données sont nominatives. Tel pourrait être également le cas lors d'une prise de vue. Une personne est identifiable lorsque les données traitées permettent d'identifier la personne, notamment par corrélation indirecte d'information tirées des circonstances, par mise en relation de données provenant de différentes sources ou par comparaison de données. Une personne ne sera pas identifiable si son identification nécessite des moyens disproportionnés que, selon le cours ordinaire des choses, aucun intéressé ne mettrait en œuvre. Il convient de considérer non seulement les moyens qu'un responsable de traitement ou d'autres personnes peuvent raisonnablement mettre en œuvre pour identifier la personne concernée. Il faut également tenir compte que le caractère identifiable d'une personne est évolutif notamment en fonction du développement de la technique ou de l'exploitation d'une donnée personnelle : une empreinte digitale laissée sur un verre n'aboutira éventuellement à l'identification de la personne concernée que si elle est prélevée et traitée.

En ce qui concerne les données biométriques, nous sommes en présence, en règle générale de données à caractère personnel[16]. Il convient cependant de distinguer entre les données brutes qui forment l'échantillon et les gabarits[17]. Ces derniers, pris de manière isolée, ne paraissent pas constituer sans autre des données à caractère personnel. On peut les qualifier de pseudonymes[18]. Leur « personnalisation » nécessite la mise en relation avec d'autres informations notamment d'identification. Les échantillons ou les données brutes sont des données personnelles se référant à une personne identifiée lorsqu'ils peuvent être attribués sans équivoque à une personne déterminée et à elle-seule (par exemple un visage ou une voix). Il s'agit en outre de données se rapportant à une personne identifiable lorsque l'identification nécessite des auxiliaires ou des connaissances spécifiques (comparaison d'empreintes digitales par ex.). Certaines de ces données brutes peuvent également être sensibles au sens de l'article 6 de la Convention 108 notamment lorsqu'elles révèlent des informations sur la santé ou la race des personnes concernées.

3.2. Respect des exigences de la protection des données

Le recours à des données biométriques doit dès lors intervenir dans un contexte conforme aux exigences de la protection des données. « L'atteinte à la vie privée ne provient pas de l'identification positive assurée par la biométrie, mais de la capacité des tierces parties d'avoir accès à ce renseignement dans une forme identifiable et de le relier à d'autres informations, ce qui mène à un usage secondaire de ce renseignement sans l'autorisation de la personne visée par les données. Cela signifie que le particulier n'a plus de contrôle sur les

[15] Voir par exemple, Recommandation N° R (2002) 9 sur la protection des données à caractère personnel collectées et traitées à des fins d'assurance.
[16] Biovison, Privacy Best Practices in Deployment of Biometric Systems, 28.08.2003
[17] Claudia Golembiewski, Thomas Probst, Datenschutzrechtliche Anforderungen an den Einsatz biometrischer Verfahren, op. cit., p. 18ss.
[18] Biovision, op. cit.

renseignements qui le concernent. »[19] Or, le respect du droit à la protection des données, dans le secteur privé en particulier, implique que l'individu puisse conserver une certaine maîtrise sur les données qui le concernent et qu'il puisse choisir ce qu'il advient de ses données, qui y a accès, pour quelle finalité et dans quelle étendue.

Dans le secteur privé, une grande partie des applications fondées sur des données biométriques que nous avons recensées sont des opérations d'authentification (vérification). Cela n'est pas sans importance du point de vue de la protection des données, car cela détermine la manière dont les données biométriques seront utilisées et enregistrées. Le but d'un système de vérification n'est pas obligatoirement de confirmer l'identité d'une personne, mais plutôt d'authentifier l'admissibilité de cette personne à accéder à un lieu déterminé ou à un service particulier ou encore d'obtenir une prestation ou effectuer une transaction. Ainsi, on peut distinguer trois composantes de l'authentification[20] :

a. L'identification : il s'agit d'une phase isolée pour établir l'identité d'un individu de manière non équivoque ;
b. La confirmation de l'admissibilité : il s'agit également d'une phase isolée pour confirmer que l'individu nommé est admis au service ou à la prestation accessible au moyen de données biométriques ;
c. Le titre d'authentification (Authentification Credential): procédure renouvelable qui permet d'identifier l'individu comme légitimé et de donner accès au service ou à la prestation.

Dès lors que l'identité de l'individu a été établie et qu'il remplit les critères d'accès à un lieu déterminé ou d'admission à un service ou à une prestation, il n'est plus nécessaire d'identifier la personne à chaque fois et par conséquent, il n'est pas en principe nécessaire d'avoir d'autres données personnelles que celles nécessaires à permettre l'accès. Il faut du moins clairement dissocier les données biométriques nécessaires à l'authentification, des autres données nécessaires au service ou prestation pour lequel l'accès a été donné. Par exemple, dans la banque de données sur le temps de travail d'une entreprise, on ne devrait pas retrouver les données biométriques, mais uniquement les données pertinentes relatives à la gestion et au calcul du temps de travail. Lors de l'utilisation d'une carte de crédit avec un système d'authentification basé sur des données biométriques, le commerçant n'a pas obligatoirement besoin de connaître l'identité de la personne. Ce qui est important pour lui, c'est qu'il puisse être payé pour sa prestation.

Du point de vue de la protection des données, il convient en outre de prendre en considération la forme sous laquelle les gabarits seront conservés (base de données centrale, support de données en mains de la personne concernées). En règle générale, lorsque la fonction des données biométriques est de permettre l'authentification d'une personne, il n'est pas nécessaire de recourir à un enregistrement centralisé des données ou des gabarits. Un stockage décentralisé sous contrôle de la personne concernée est en soi suffisant. La situation est différente s'il s'agit d'une fonction d'identification. Dans ce cas, les données doivent être enregistrées dans une banque de données gérée par un tiers afin de permettre la comparaison des données d'une personne avec toutes les données des autres personnes enregistrées dans le système. Enfin, l'appréciation des implications en terme de protection des données dépendra aussi du choix des données biométriques. S'agit-il de données laissant

[19] Ann Cavoukian, Vie privée et biométrie : concepts opposés ou à réexaminer ?, février 1998, http://www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=11552&N_ID=1&PT_ID=11528&U_ID=0
[20] Ann Cavoukian, Consumer Biometric Applications: A Discussion Paper, September 1999, http://www.ipc.on.ca/docs/cons-bio.pdf, p. 3

des traces, comme l'empreinte digitale ou de données sans trace, comme le contour de la main ?

La collecte et le traitement de données biométriques doit ainsi être conforme aux principes de base de la protection des données que sont en particulier:

- licéité du traitement
- bonne foi (principe de transparence)
- respect de la finalité
- proportionnalité
- exactitude des données
- sécurité des données
- garantie particulière pour le traitement de données sensibles
- droit des personnes concernées, notamment droit d'accès et de rectification

3.2.1 Collecte licite

Dans le secteur privé, le recours à des données biométriques ne peut en règle générale intervenir qu'avec le consentement des personnes concernées. C'est particulièrement vrai lors de l'utilisation de la biométrie à des fins commerciales (carte bancaire, transaction sur Internet, moyen de paiement, etc.). L'utilisation de la biométrie doit demeurer volontaire. Le consentement doit être libre, spécifique et informé. Cela suppose que le consommateur (la personne concernée) ait à disposition d'autres alternatives s'il ne souhaite pas que des données biométriques le concernant soient collectées et traitées. La personne concernée doit pouvoir faire valoir son point de vue par rapport au traitement et éventuellement l'influencer. Le consentement sera en particulier libre si elle n'éprouve pas de réticence par rapport à l'utilisation de données biométriques la concernant. Lorsqu'il n'est pas possible d'obtenir un consentement libre, notamment lorsque la personne concernée se trouve dans une situation de subordination ou dans un rapport déséquilibré qui ne lui laisse pas de véritable choix, - c'est particulièrement le cas dans le domaine de l'emploi -, le recours à la biométrie ne peut intervenir que si la loi le prévoit ou si le responsable de traitement peut faire valoir un intérêt prépondérant prévalant l'intérêt ou les droits et libertés fondamentaux de la personne concernée au respect de sa vie privée. Tel sera généralement le cas de l'utilisation de la biométrie pour l'accès à des informations sensibles. Il peut aussi être lié à l'exécution d'un contrat auquel la personne concernée est partie, dans la mesure où l'utilisation de la biométrie se situe clairement dans la finalité du contrat. Ce pourrait être le cas si le traitement est nécessaire à respecter les obligations ou à garantir les droits résultant du contrat[21]. Dans un contrat de travail, une telle utilisation pourrait s'avérer nécessaire s'il est prévu d'employer une personne dans un secteur sensible (accès à des installations nucléaires ou à des secrets de fabrication).

3.2.2 Principe de la transparence

La collecte et le traitement des données biométriques doivent être conformes au principe de la bonne foi, c'est-à-dire la procédure doit être transparente. La collecte ne doit pas avoir lieu à l'insu de la personne concernée. Celle-ci doit connaître pour le moins les finalités et le responsable du traitement. Elle devrait également savoir si d'autres données personnelles sont nécessaires et quelles données devraient être collectées. Elle devrait être informée des possibilités éventuelles d'une authentification anonyme, ainsi que des conséquences d'une participation ou d'une non participation au système (risque et avantage) et notamment ce

[21] Lukas Gundermann, Marit Köhntopp, op. cit., dans DuD 23 (1999) 3, p. 149.

qu'il advient en cas de retrait du consentement une fois l'enrôlement effectué. Le risque d'abus sera d'autant moins élevé que le responsable de traitement renonce à collecter d'autres données que celles nécessaires à l'authentification en vue de l'accès à un service ou à une prestation. Plus la transparence sera grande, plus la méfiance de la personne concernée diminuera. Or du fait que le fonctionnement de ces systèmes reposent sur la coopération des personnes concernées, l'élément de confiance est un facteur fondamental qui passe par le respect des exigences de protection des données.

3.2.3 Respect du principe de finalité

La finalité de la collecte et du traitement de données biométriques doit être clairement définie et respectée. C'est un élément déterminant pour le choix des techniques biométriques qui seront utilisées : authentification ou identification. Ces techniques sont au service de la finalité. Si une technique d'authentification – moins attentatoire à la vie privée – permet d'atteindre la finalité du traitement, on ne cherchera pas à résoudre des problèmes de vérification avec un système d'identification. Si ces données sont utilisées pour permettre l'accès à un bâtiment, elles ne doivent pas être utilisées pour d'autres finalités qui n'ont rien à voir avec le contrôle de l'accès à ce bâtiment. Par exemple, leur utilisation en vue d'évaluer l'état émotionnel de la personne concernée ou de surveiller son comportement est incompatible avec la finalité originelle d'accès[22]. Le respect de ce principe est d'autant plus important que les données biométriques revêtent le caractère d'un identifiant universel. Elles peuvent permettre de connecter des informations de sources différentes, d'avoir un suivi sur les activités et le comportement d'un individu et de prendre des mesures à son détriment. Le risque pour la vie privée de l'individu ne résulte pas de l'identification positive que permet la biométrie, mais de la possibilité d'avoir accès à des données biométriques et de les relier à d'autres données personnelles issues d'une utilisation non autorisée. Cela affaiblit la maîtrise des individus sur leurs propres informations[23]. Des informations qui ne sont pas nécessaires à l'identification ou l'authentification d'une personne pourraient également être extraites des données biométriques. Il est par exemple possible d'obtenir des informations sur la santé d'une personne à partir de certaines données biométriques : l'empreinte digitale peut révéler des informations médicales ; l'examen de l'iris ou de la rétine peut démontrer par exemple que la personne souffre de diabète, d'artériosclérose ou d'hypertension[24].

3.2.4 Respect principe proportionnalité

Le principe de proportionnalité est un des principes les plus importants de la protection des données dans le contexte de la biométrie. La majorité des décisions des différentes autorités de protection des données que nous avons examinées ont basé leur examen de manière déterminante sur ce principe. A noter qu'on constate des différences d'appréciation dans le caractère proportionné d'une mesure selon les pays d'où émanent ces décisions. C'est ainsi que l'autorité danoise a jugé proportionné le recours à l'empreinte digitale pour s'acquitter d'un titre de transport sur un ferry, alors que la CNIL s'oppose à la création de bases de données d'empreintes digitales en l'absence d'un impératif de sécurité incontestable, que le préposé fédéral suisse à la protection des données estime disproportionné le recours à un système d'empreintes digitales pour le calcul du temps de travail, que la commission

[22] Groupe de travail „Article 29" sur la protection des données, Document de travail sur la biométrie, 1er août 2003, p. 7.
[23] Ann Cavoukian, Consumer Biometric Applications: A Discussion Paper, September 1999, http://www.ipc.on.ca/docs/cons-bio.pdf, p. 34
[24] Ann Cavoukian, Consumer Biometric Applications: A Discussion Paper, September 1999, http://www.ipc.on.ca/docs/cons-bio.pdf, p. 35 et auteurs cités.

grecque de protection des données s'est opposée à l'usage d'un système d'identification biométrique pour l'enregistrement des passagers à l'aéroport d'Athènes ou que le Garante en Italie a jugé disproportionné la prise d'empreinte digitale pour accéder à une banque.

Selon ce principe, il ne doit y avoir collecte de données personnelles que si celles-ci sont nécessaires (adéquates, pertinentes et non excessives) au regard de la finalité pour laquelle elles devraient être collectées et traitées. Ce principe de proportionnalité comporte trois volets : la règle d'aptitude ou d'adéquation qui exige que le moyen choisi soit propre à atteindre le but visé ; la règle de nécessité qui impose qu'entre plusieurs moyens adaptés, on choisisse celui porte l'atteinte la moins grave aux intérêts en cause (par exemple la liberté de mouvement, la santé, l'intégrité des personnes concernées par un relevé biométrique) ; la règle de proportionnalité au sens étroit qui requiert de mettre en balance les effets de la mesure choisie sur la situation des personnes concernées avec le résultat escompté du point de vue du but visé[25]. Dans la mesure où la proportionnalité de la mesure est avérée, seules les données personnelles nécessaires à atteindre l'objectif recherché doivent être collectées et traitées. Deux éléments doivent être vérifiés : faut-il des données personnelles ou ne peut-on pas atteindre le résultat recherché sans données personnelles ? Si des données personnelles sont néanmoins indispensables, il faut limiter leur étendue au strict nécessaire. Ce principe revêt un caractère important face à la biométrie. Les données biométriques sont des caractéristiques de tout être humain et touchent à son intégrité et à sa dignité. Elles requièrent une certaine retenue dans leur traitement (principe de précaution). Il faudra mettre en balance les avantages du recours à un système biométrique et les inconvénients pour la vie privée des personnes concernées. On tiendra compte des solutions alternatives dans la prise de décision. Le choix ne doit pas être guidé uniquement par des raisons de commodité d'utilisation. Il faut en effet tenir compte des aspects sociaux et culturels et des réticences possibles à l'égard de l'utilisation de ce type de données. On renoncera à leur collecte et à leur utilisation si l'identification ou l'authentification des personnes dans le cadre recherché peut être réalisé avec la même efficacité et sécurité par un système sans données biométriques. A cet égard on peut par exemple se demander si l'accès à une cantine scolaire et le paiement d'un repas nécessitent le recours à des moyens biométriques.

Si le recours à la biométrie s'avère nécessaire, le choix du système doit également tenir compte des exigences de la proportionnalité. Il n'est ainsi pas nécessaire de mettre en place un système d'identification lorsqu'une procédure d'authentification est suffisante. De même, on privilégiera la collecte de données biométriques ne laissant pas de traces. Lors de l'enrôlement, on évitera d'extraire des informations qui ne sont pas nécessaires à l'identification ou à l'authentification. En outre, on privilégiera des méthodes qui permettent d'anonymiser les données et d'authentifier la personne sans l'identifier, ainsi que de chiffrer les données biométriques.

3.2.5 Sécurité des données

La donnée biométrique est une information intrinséquement liée à la personne. En cas de falsification ou d'usurpation, cette personne ne pourra pas sans autre modifier ses caractéristiques biométriques et pourra difficilement démontrer qu'elle n'a pas commis les actes qui lui sont reprochés et qui sont le fait d'un usurpateur. Ainsi, la sécurité des données et des systèmes d'informations biométriques est fondamentale. Elle l'est non seulement par rapport au risque d'accès ou d'utilisation non autorisés des données, mais également par rapport à la fiabilité du système. Des failles de sécurité peuvent avoir des conséquences

[25] Arrêt du Tribunal fédéral du 13 juillet 2004 dans la cause X contre Office cantonal de l'inspection et des relations du travail du canton de Genève, « système de localisation GPS », considérant 5 et arrêt cité.

graves, voire irréversibles à l'égard des personnes concernées. Les mesures de sécurité doivent être prises dès la collecte des données et en particulier durant la phase d'enrôlement.

Il ne devrait pas y avoir d'enregistrement ni de conservation de l'image biométrique actuelle et brute. Le gabarit biométrique devrait être une représentation mathématique enregistrée sous forme chiffrée afin de garantir l'utilisation au seule fonction d'authentification.

La conservation des données biométriques sur un support hors ligne sécurisé en mains de la personne concernée, comme une carte à puce, permet d'exploiter les capacités techniques conformes à la vie privée (PET). Une telle solution permet d'éviter de connecter les données biométriques avec d'autres données de la personne concernée. Elle permet d'authentifier l'individu sans avoir à connaître l'identité de cette personne[26]. Lorsque les données sont enregistrées dans une base de données gérée par un tiers, elles sont souvent connectées à d'autres données personnelles comme le nom et l'adresse. Dans ce cas, le chiffrement de la biométrie peut également être utilisé comme solution conforme à la vie privée afin dépersonnaliser les autres informations qui y sont enregistrées (séparation de l'identité des autres données). Le lien entre l'identité de la personne et les autres informations se fait par l'intermédiaire de la personne concernée qui utilise sa biométrie pour permettre l'identification. Cela a pour avantage que la personne concernée possède un certain contrôle sur la banque de données.[27]

4. Quelques pistes pour garantir la protection des données lors de l'utilisation de données biométriques

D'un point de vue de la protection des données, l'utilisation de la biométrie peut présenter des risques importants, notamment liés aux possibilités de traçage des individus et d'interconnexion des informations et des fichiers. Elle peut également se révéler bénéfique, notamment pour sécuriser l'accès à des données[28] : « L'élément biométrique joue le rôle d'une clef qui permet d'entrer chez soi ! »[29]. Elle peut également devenir un élément de la protection de la vie privée[30].

Enfin, il faut être conscient que la biométrie n'est pas la solution à tous les problèmes de contrôle ou de gestion. Les procédures biométriques présentent des défauts et des faiblesses tant sous l'angle de la fiabilité des résultats (rejet ou acceptation erronés) que de la sécurité des données[31] : les données biométriques sont des identifiants uniques, mais ils ne sont pas secrets[32] ! Le degré de sécurité peut varier en fonction du type de caractéristiques

---

[26] John Borking, Paul Verhaar, Biometrie und Datenschutz, dans DuD 23 / 1999 3, p. 140s.; Ann Cavoukian, Consumer Biometric Applications: A Discussion Paper, September 1999, p. 25ss, http://www.ipc.on.ca/docs/cons-bio.pdf, p. 39 et auteur cité.

[27] ibidem

[28] PFPD, 8e rapport d'activités 2000/2001, p. 202 et 9e rapport d'activités 2001/2002, p. 29; voir aussi George J. Tomko, Biometric Encryption – New Developments in Biometrics, 18e Conférence internationale des commissaires à la protection des données, 19 septembre 1996, www.privcom.gc.ca/speech/archive/02_05_a_960918_01_e.asp ; Georges J. Tomko, Biometrics as Privacy-Enhancing Technology : Friend or Foe of Privacy), Privacy Laws § Business 9th Privacy' / Data Protection Authorities Workshop, September 1998 Santiago de Compostela, www.dss.state.ct.us/digital/tomko.htm .

[29] CNIL, 22e rapport d'activité 2001, p. 169

[30] Ann Cavoukian, Vie privée et biométrie : concepts opposés ou à réexaminer ?, février 1998, http://www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=11552&N_ID=1&PT_ID=11528&U_ID=0; Brigitte Wirtz, op. cit., p. 133.

[31] Ann Cavoukian, Consumer Biometric Applications: A Discussion Paper, September 1999, p. 25ss, http://www.ipc.on.ca/docs/cons-bio.pdf

[32] Bruce Schneider, Biometrics : Truths and Fictions, www.schneier.com/crypto-gram-9808.html#biometrics

biométriques utilisées et selon la manière dont elles sont utilisées. Le recours à la biométrie peut aussi être source de discrimination[33].

Toutefois, il serait erroné de cultiver une méfiance ou une défiance exagérée par rapport à l'utilisation de technologies basées sur des informations biométriques. Il faut bien plus se pencher sur les usages que l'on veut en faire et voir qu'elles sont les enjeux en présence dans une société basée sur le respect des droits et des libertés fondamentales. Il s'agit d'exploiter les potentialités qu'offre la technologie basée sur la biométrie pour diminuer, voire supprimer tout risque d'atteinte au respect de la vie privée. Face à un traitement de données biométriques, on ne peut que rappeler la pertinence des principes de base de la protection des données énoncés notamment dans la Convention 108 et repris dans nos législations nationales pour rechercher un équilibre entre les besoins des responsables de traitement et les droits des personnes concernées. Des choix que nous ferons dépendra le contour de la société de demain. Celle-ci se doit de demeurer respectueuse des droits et libertés fondamentales, afin de maintenir des espaces de libertés sans contrôle et de préserver le droit à l'oubli. Cela implique que toutes les traces que nous laissons dans nos activités quotidiennes ne soient pas systématiquement conservées.

Ainsi, nous pouvons dégager les thèses de protection des données suivantes[34] :

- On ne recourra 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 de sécurité des données.
- La finalité du traitement doit être strictement respectée.
- Les personnes concernées doivent être clairement informées et associées au processus de traitement (pas de collecte cachée).
- Les données biométriques doivent être collectées directement auprès de la personne concernée ou du moins à sa connaissance.
- Pour éviter des discriminations non justifiées, il est nécessaire de prévoir des alternatives pour les personnes qui ne sont pas en mesure d'utiliser un système biométrique.
- L'identification de données biométriques doit se faire uniquement par la comparaison avec un échantillon prélevé auprès de la personne concernée.
- Les données biométriques originales doivent être détruites une fois la procédure d'enrôlement effectuée.
- Les technologies basées sur l'utilisation de données biométriques n'impliquant pas le stockage de gabarits dans une base de données gérée par un responsable de traitement autre que la personne concernée ne soulèvent en principe pas de problèmes particuliers du point de vue de la protection des données, dès lors que le gabarit est conservé sur un support dont la personne concernée a l'usage exclusif (carte à puce, téléphone mobile, ordinateur portable, etc.).
- Si une base de données est constituée et gérée par un responsable de traitement autre que la personne concernée, l'élément biométrique retenu peut avoir des conséquences pour le respect des droits et des libertés fondamentales. Tel sera en particulier le cas lorsque nous sommes en présence d'un élément biométrique qui laisse des traces, comme l'empreinte digitale. Le recours à un tel élément devrait répondre à un intérêt prépondérant qualifié de sécurité.

---

[33] CNIL, 22e rapport d'activité 2001, p. 158 ; Simon G. Davies, Touching Big Brother, How biometric technology will fuse flesh and machine, dans Information Technology § People, vol. 7, N° 4 1994, www.privacy.org/pi/reports/biometric.html

[34] Voir aussi CNIL, 22e rapport d'activité, p. 171 ; CoE …. ; Art. 29

- En l'absence d'un tel intérêt, il convient de recourir à un élément biométrique qui limite le risque d'abus, tel que celui qui ne laisse pas de trace, comme le contour de la main.
- Lors du recours à des éléments laissant des traces et stockés dans une banque de données, il convient de prendre des mesures pour éviter un détournement de finalité, notamment en recourant au chiffrement de l'élément contenu dans la base de données à l'aide du gabarit, de sorte que le déchiffrement ne puisse se faire qu'en présence de la personne à laquelle l'information biométrique se rapporte[35]. Le gabarit doit être propre à l'application concernée pour éviter les possibilités de relier des données ou d'avoir accès à des applications différentes.
- Il faut prendre les mesures nécessaires pour éviter d'utiliser l'information biométrique comme un identifiant unique universel.
- Il faut éviter de déduire d'autres données sur la personne, notamment sur des maladies à partir des données biométriques.
- Dans un système d'authentification (vérification), il convient d'éviter de collecter et de traiter d'autres données personnelles que celles nécessaires à l'authentification et par conséquent de privilégier des solutions ne nécessitant pas de révéler l'identité de la personne (authentification anonyme), à moins que l'identification ne soit indispensable à la finalité du traitement (principe de l'économicité du traitement).
- Dans un système d'authentification, les données biométriques ne doivent pas être utilisées pour d'autres raisons que la vérification, sauf justification légale notamment à des fins de poursuite pénale.
- Pour améliorer la sécurité des données et diminuer les risques d'accès non autorisé, notamment par appropriation de données de tiers, il convient de doubler le système biométrique avec d'autres moyens d'identification ou d'authentification (par ex. code d'accès) ou de cumuler les éléments de reconnaissance biométrique. Il convient également d'avoir des lecteurs biométriques sécurisés permettant aux personnes légitimées de présenter directement leurs données ou de recourir à des systèmes dans lesquels les données biométriques sont intégrées à des dispositifs sécurisés, comme une carte à puce[36].
- Les données biométriques doivent être chiffrées dès leur enrôlement. Lors d'une communication électronique de ces données notamment au travers d'un réseau, la communication doit être chiffrée.
- Les données biométriques enregistrées (gabarit) doivent être périodiquement vérifiées quant à leur degré de fiabilité (ré-enrôlement périodique). L'échantillon biométrique présenté par la personne peut en effet varier avec le temps en fonction de différents facteurs.
- Les droits des personnes concernées doivent être garantis. En particulier, elles doivent avoir la possibilité de contrôler l'usage qui est fait de leurs données biométriques et d'en obtenir la destruction le cas échéant.
- Les systèmes d'informations biométriques devraient faire l'objet d'une procédure de certification et d'audit en matière de protection des données. Ces systèmes devraient être également évalués sous l'angle des risques avant leur mise en fonction[37]. Un

[35] George J. Tomko, Biometric Encryption – New Developments in Biometrics, 18e Conférence internationale des commissaires à la protection des données, 19 septembre 1996, www.privcom.gc.ca/speech/archive/02_05_a_960918_01_e.asp ; Georges J. Tomko, Biometrics as Privacy-Enhancing Technology : Friend or Foe of Privacy), 9th Privacy' / Data Protection Authorities Workshop, September 1998 Santiago de Compostela. CNIL, 22e rapport d'activité, p. 168.

[36] Ann Cavoukian, Consumer Biometric Applications: A Discussion Paper, September 1999, http://www.ipc.on.ca/docs/cons-bio.pdf, p. 27

[37] Hans-Jürgen Burger, op. cit.. p. 6.

concept de protection devrait être élaboré définissant notamment les processus de traitement.

- Il faut continuer à encourager les milieux professionnels, les associations, les industriels à établir des standards et des procédures permettant de pas utiliser les données biométriques de manière contraire aux exigences de la protection des données. En ce sens, il convient de saluer les travaux de Biovision et de l'International Biometric Industry Association (IBIA) ou les initiatives Bioprivacy[38].

[38] http://www.bioprivacy.org/best_practices_main.htm