Code de conduite (et commentaire) sur l'utilisation des données biométriques dans les documents d'identité

Version mars 2009

Elodie Maître-Arnaud

Docteur en droit

Remarques préliminaires

Le Code de conduite et son commentaire ont été rédigés dans le cadre du Projet n° 108294 financé par le Fonds National Suisse de la Recherche Scientifique (FNS), « *Applying Biometrics to Identity Documents: Technological, Legal and Security Challenges and Implications* ». Ce projet FNS pluridisciplinaire a été dirigé par le Professeur Christophe Champod (Ecole des Sciences Criminelles de l'Université de Lausanne), le Professeur Bertil Cottier (Université de la Suisse italienne) et par le Professeur Andrzej Drygajlo (Ecole Polytechnique Fédérale de Lausanne).

Structure du Code et méthodologie

Le Code de conduite comporte sept titres. Les titres I à IV sont relatifs au préambule, à l'objet, au champ d'application et à la terminologie utilisée dans le Code. Le titre V traite des dispositions relatives à la collecte des données biométriques ; le titre VI des dispositions relatives à l'usage des données biométriques ; le titre VII des droits des personnes concernées par un traitement de données biométriques.

Le présent Code comporte deux séries de dispositions :

- le rappel des principes généraux de protection des données personnelles ;
- des recommandations spécifiques dérivant de leur application en matière de données biométriques.

I. Préambule

Le présent Code a pour objectif de :

- veiller au respect des libertés individuelles, à la protection de la vie privée et à la protection des données personnelles des personnes physiques dans le cadre de l'utilisation de leurs données biométriques dans des documents d'identité ;
- consacrer, là où elles sont nécessaires, des règles spécifiques de protection des données, pour l'utilisation de la biométrie dans des documents d'identité.

Il rappelle et tient compte des principes de protection des données personnelles posés notamment par :

- la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981[1] ;
- la Directive européenne relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel et à la libre circulation de ces données du 24 octobre 1995[2].

Le présent Code est susceptible d'être modifié, révisé ou complété afin d'adapter ses règles à l'apparition de nouvelles pratiques et/ou à l'évolution des règlementations relatives à la protection des données et/ou à l'adoption de règlementations spécifiques à la protection des données biométriques ou encore dans le but de renforcer son efficacité.

II. Objet

Le présent Code a pour objet de définir des règles de conduite en matière de collecte, de conservation et d'usage de données biométriques dans le cadre de l'établissement et de l'utilisation des documents d'identité.

III. Champ d'application

Le présent Code s'adresse à toute personne, physique ou morale, publique ou privée, chargée de la mise en œuvre d'un traitement de données biométriques dans le cadre de l'établissement et de l'utilisation des documents d'identité.

Il s'adresse en particulier aux personnes chargées de la collecte et de la conservation des données biométriques prélevées dans le cadre de l'établissement des documents d'identité, aux personnes chargées de la délivrance des documents d'identité, aux personnes responsables de tout contrôle douanier ou de police portant sur des documents d'identité ou de tout autre usage des données biométriques contenues dans des documents d'identité.

---

1 http://conventions.coe.int/Treaty/fr/Treaties/Html/108.htm

2 http://europa.eu/scadplus/leg/fr/lvb/l14012.htm.

IV. Terminologie

Biométrie

Ensemble des techniques de mesure, d'analyse et de reconnaissance des caractéristiques physiques, physiologiques ou comportementales des êtres humains dont l'objectif est l'identification ou la vérification de leur identité.

Donnée biométrique

Toute information représentant une caractéristique propre du corps ou du comportement d'une personne physique identifiée ou identifiable.

Paramètres ou Features biométriques

Description numérique des données biométriques.

Gabarit ou Template biométrique

Modèle mathématique décrivant des paramètres biométriques.

Système biométrique

Dispositif automatisé permettant notamment :

- la collecte de données biométriques ;
- l'extraction des informations discriminantes à partir de ces données ;
- la comparaison de ces informations avec celles contenues dans un ou plusieurs gabarits servant de référence ;
- la communication de la reconnaissance ou du rejet à la personne concernée.

Enrôlement

Acquisition d'une série de données biométriques en vue de constituer un gabarit permettant l'identification ou la vérification de l'identité.

Traitement de données biométriques

Toute opération ou ensemble d'opérations portant sur des données biométriques, quel que soit le procédé utilisé à cet effet, automatisé ou manuel, telle que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

Base de données

Fichier ou ensemble de fichiers, centralisé ou décentralisé, permettant le stockage, permanent ou temporaire, et l'accès à des informations structurées.

Authentification ou Vérification d'identité

Procédé permettant de vérifier l'identité déclarée d'une personne dans lequel les données biométriques fournies par un individu sont comparées aux données biométriques, paramètres ou gabarits de référence, enregistrés dans la base de données biométriques du système.

Identification

Procédé permettant, sur la base de données biométriques uniquement, de déterminer l'identité d'une personne, dans lequel les données biométriques fournies par un individu sont comparées à

plusieurs données biométriques, paramètres ou gabarits, contenus dans la base de données du système.

Support de stockage individuel décentralisé

Tout support de stockage dont la personne concernée a un contrôle exclusif, tel qu'une carte à puce ou magnétique

Autorité de contrôle

Autorité publique indépendante chargée de surveiller l'application des dispositions relatives à la protection des données.

Responsable du traitement

Toute personne physique ou morale, autorité publique ou organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données personnelles.

V. Dispositions relatives à la collecte des données biométriques

1. Les formalités préalables à la collecte des données biométriques

Le responsable du traitement ou, le cas échéant, son représentant, doit adresser à l'autorité de contrôle compétente une notification préalable à la mise en œuvre d'un traitement de données personnelles, ou ensemble de traitements de données personnelles ayant une même finalité ou des finalités liées, à moins qu'il n'ait procédé à la nomination d'un détaché à la protection des données.

2. L'information préalable des personnes concernées par un traitement de données biométriques – Principe de transparence

Rappel des principes généraux de protection des données

Le responsable du traitement respectera le principe de transparence en fournissant aux personnes dont les données sont collectées, antérieurement ou au plus tard au moment de la collecte, les informations suivantes :

- l'identité du responsable du traitement et, le cas échéant, celle de son représentant ;
- les finalités poursuivies par le traitement pour lequel les données sont collectées ;
- les catégories de données concernées ;
- le caractère obligatoire ou facultatif des réponses ;
- les conséquences d'un éventuel défaut de réponse (refus d'acquisition d'une donnée biométrique) ;
- les destinataires ou catégories de destinataires des données ;
- les droits d'accès, de rectification, d'opposition et de suppression des données personnelles ;
- les transferts de données envisagés vers un État ne disposant pas d'une législation relative à la protection des données adéquate.

La protection spécifique des données biométriques

Le responsable du traitement ou son représentant s'engage à :

- communiquer au moment de la collecte la durée de conservation des données biométriques prélevées ;
- collecter des données biométriques directement auprès de la personne concernée ou à sa connaissance ;
- renoncer à, et prévenir toute collecte de données biométriques à l'insu de la personne concernée ;
- procéder à la comparaison des données du titulaire d'un document d'identité, à des fins d'identification ou d'authentification, uniquement avec un échantillon prélevé directement auprès de la personne concernée ;
- privilégier la collecte d'éléments biométriques ne laissant pas de trace et difficiles à acquérir à l'insu de la personne concernée, tels le contour de la main ou l'iris par exemple ;
- privilégier des supports de stockage décentralisés dont la personne concernée par le traitement a l'usage exclusif.

3. Le principe de finalité

Rappel des principes généraux de protection des données

Les finalités du traitement doivent être explicites et légitimes ; elles doivent aussi être déterminées lors de la collecte des données. Les finalités de traitements ultérieurs à la collecte doivent être compatibles avec les finalités telles que spécifiées à l'origine.

La protection spécifique des données biométriques

Le responsable du traitement ou son représentant s'engage à :

- recourir à un système d'*identification* biométrique uniquement lorsque la mise en place d'un système d'*authentification* se révèle inadapté eu égard aux finalités explicites et légitimes du traitement, déterminées au moment de la collecte.
- mettre en œuvre des mesures techniques permettant d'éviter tout détournement de finalité, notamment le déchiffrage uniquement en présence de la personne concernée par une identification ou vérification d'identité.

4. Le principe de proportionnalité

Rappel des principes généraux de protection des données

Les données collectées doivent être adéquates, pertinentes et non excessives au regard des finalités poursuivies par le traitement.

La protection spécifique des données biométriques

Le responsable du traitement ou son représentant s'engage à renoncer à traiter des données biométriques si l'authentification ou l'identification des personnes peuvent être réalisées avec la même efficacité et sécurité sans de telles données.

Le responsable du traitement ou son représentant s'engage à ne pas conserver les données biométriques au-delà de ce qui est nécessaire au regard de la finalité du traitement.

5. Les possibilités de collectes alternatives

Le responsable du traitement ou son représentant ne saurait se retrancher derrière une impossibilité technique pour justifier toute forme de discrimination.

Le responsable du traitement ou son représentant doit mettre en place des procédures de collecte alternatives pour les personnes ne présentant pas les caractéristiques biométriques nécessaires lors de l'enrôlement ou de la vérification.

Le responsable du traitement doit doubler le système de vérification/identification biométrique avec un autre mode de reconnaissance.

VI. Dispositions relatives à l'usage des données biométriques

1. Identification du responsable du traitement

Rappel des principes généraux de protection des données

Le responsable du traitement ou son représentant sont tenus d'informer la personne concernée par un traitement de données personnelles de l'identité du responsable du traitement et, le cas échéant, de celle de son représentant.

Lorsque les finalités et les moyens du traitement sont déterminés par des dispositions législatives ou réglementaires, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par la loi.

2. Obligation de sécurité

Rappel des principes généraux de protection des données

Le principe de sécurité des traitements de données personnelles implique que le responsable du traitement mette en œuvre les mesures techniques et d'organisation appropriées pour protéger les données contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé, ainsi que contre toute autre forme de traitement illicite.

La protection spécifique des données biométriques

Le responsable du traitement ou son représentant sera particulièrement sensible aux risques d'usurpation d'identité, de faux rejet ou de fausse acceptation. Afin de prévenir ces risques, il s'engage notamment à :

- ne pas utiliser les données biométriques comme identifiant unique pour des applications différentes ;
- chiffrer les données biométriques dès leur enrôlement puis à les détruire ;
- mettre en place des protocoles de transmission permettant de vérifier la conformité des données reçues à celles émises ;
- vérifier régulièrement l'intégrité des gabarits utilisés dans le cadre du traitement ;

- recourir régulièrement à des procédures d'audit et de certification effectuées par des experts indépendants agréés par l'autorité de protection des données compétente ;
- favoriser les systèmes dits d'*Open Source*.

Les personnes concernées par un traitement de données biométriques peuvent accéder à leurs données par le biais d'un identifiant biométrique, ou par tout autre moyen d'authentification.

Le transfert de données biométriques ne peut avoir lieu que sous forme chiffrée.

3. Mode et durée de conservation des données

Le responsable du traitement ou son représentant s'engage à privilégier des supports de stockage décentralisés dont la personne concernée par le traitement a l'usage exclusif.

Le responsable du traitement ou son représentant s'engage à ne pas conserver des données biométriques sous forme nominative au-delà de la durée nécessaire à la finalité du traitement.

4. Choix des données biométriques traitées

Le responsable du traitement ou son représentant s'engage à privilégier la collecte d'éléments biométriques ne laissant pas de trace et difficiles à acquérir à l'insu de la personne concernée, tels le contour de la main ou l'iris par exemple.

5. Transferts des données biométriques vers l'étranger

Rappel des principes généraux de protection des données

Le transfert de données personnelles vers un pays tiers ne peut avoir lieu que si le pays tiers assure un niveau de protection adéquat. Des dérogations sont apportées à cette exigence, notamment lorsque le transfert est nécessaire ou juridiquement obligatoire pour la sauvegarde d'un intérêt public important ou lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'au regard de l'exercice de ses droits.

La protection spécifique des données biométriques

Le transfert de données biométriques vers un pays tiers ne peut avoir lieu que sous forme chiffrée.

Les responsables de traitement doivent mettre en place des protocoles de transmission permettant de vérifier la conformité des données reçues à celles émises. Ils doivent par ailleurs mettre en place des systèmes d'authentification du destinataire des données.

6. Pouvoirs des autorités de contrôle

L'autorité de contrôle exerce en toute indépendance les missions dont elle est investie. Elle dispose notamment de pouvoirs d'investigation, de pouvoirs effectifs d'intervention et du pouvoir d'ester en justice.

VII. Droit des personnes concernées par un traitement de données biométriques

1. Le droit d'accès

Rappel des principes généraux de protection des données

Le droit d'accès recouvre la possibilité pour toute personne concernée par un traitement de données personnelles de demander la communication de ses données et d'en contrôler l'exactitude.

La protection spécifique des données biométriques

Les personnes concernées par un traitement de données biométriques peuvent à tout moment contrôler l'usage qui est fait de leurs données biométriques.

Les personnes concernées peuvent accéder à leurs données biométriques par le biais d'un identifiant biométrique ou par tout autre moyen d'authentification.

Des lecteurs accessibles au grand public doivent être mis en place par le responsable de traitement afin de permettre aux personnes concernées d'accéder à leurs données stockées dans leur document d'identité biométrique.

Les personnes concernées par un traitement de données biométriques disposent du droit de recours à un expert indépendant pour déchiffrer leurs données.

2. Le droit de rectification

Rappel des principes généraux de protection des données

Toute personne concernée par un traitement de données personnelles est en droit de faire corriger les données inexactes, incomplètes ou périmées la concernant.

La protection spécifique des données biométriques

Le responsable du traitement doit communiquer aux personnes concernées sa politique des taux d'erreur.

Toute personne concernée par un traitement de données biométriques est en droit de demander un nouvel enrôlement en cas de taux de faux rejets important.

3. Le droit d'opposition

Rappel des principes généraux de protection des données

Toute personne concernée par un traitement de données personnelles est en droit :

- de refuser de répondre (refuser l'acquisition d'une donnée biométrique) lors d'une collecte non obligatoire de données ;
- de demander l'effacement de tout ou partie de ses données contenues dans un/des fichier(s) ;
- de refuser le transfert de ses données.

4. La prohibition des prises de décision automatiques

Toute prise de décision entièrement automatisée est interdite en matière d'identification et d'authentification biométrique. Le responsable du traitement ou son représentant doivent être présents sur tous les lieux de collecte initiale et secondaire de données biométriques.

Le responsable du traitement doublera le système de vérification/identification biométrique avec un autre mode de reconnaissance.

5. La présomption d'innocence

Rappel du principe général

Toute personne est présumée innocente jusqu'à ce que sa culpabilité ait été légalement établie.

La protection spécifique des données biométriques

La charge de la preuve de la fiabilité du système biométrique pèse sur le responsable du traitement.

Toute personne concernée par un traitement de données biométriques est en droit de demander une contre-expertise en cas de litige portant sur ses données.

L'autorité de protection des données compétente dresse la liste des experts indépendants pouvant intervenir en cas de litige portant sur des données biométriques.

Aucune donnée biométrique collectée de manière clandestine ne pourra être utilisée contre la personne concernée.

Commentaire

I. Préambule

Les problèmes spécifiques soulevés par l'utilisation de la biométrie dans les documents d'identité peuvent être traités de deux manières non exclusives l'une de l'autre :

- par l'application du droit général de la protection des données ;
- par la mise en place de normes spécifiques, l'identification de risques spécifiques appelant des normes spécifiques.

La Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, adoptée le 28 janvier 1981[3], dite Convention 108 est le texte fondateur de la protection des données personnelles. Son but est de « *garantir sur le territoire de chaque partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant* »[4]. La Convention 108 demeure aujourd'hui le seul instrument juridique contraignant à vocation universelle; elle est ouverte à l'adhésion de tout pays, y compris non membre du Conseil de l'Europe. A ce jour, 38 États membres l'ont ratifiée[5], 5 autres États l'ont simplement signée[6]. Le Protocole additionnel à la Convention 108 sur les autorités de contrôle et les flux transfrontières de données est ouvert à la signature depuis le 8 novembre 2001[7]. Il impose notamment aux signataires la mise en place d'autorités de contrôle, exerçant leurs fonctions en parfaite indépendance. Il compte à ce jour 4 États parties[8] et 19 signataires[9]. Par ailleurs, afin d'adapter les principes généraux de la Convention 108 aux exigences des différents secteurs, le Conseil de l'Europe a adopté de nombreuses recommandations sectorielles.

A l'échelon régional, la Directive européenne relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données a été adoptée le 24 octobre 1995[10]. Il n'était pourtant pas évident que la question des données personnelles relève de la compétence de la Communauté qui n'a pas pour mission de traiter de la protection des libertés individuelles. Son intervention reposait ainsi initialement sur des

---

3 http://conventions.coe.int/Treaty/fr/Treaties/Html/108.htm

4 Convention 108, article 1er.

5 Albanie, Allemagne, Autriche, Belgique, Bosnie-Herzégovine, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Géorgie, Grèce, Hongrie, Islande, Irlande, Italie, Lettonie, ex-République yougoslave de Macédoine, Liechtenstein, Lituanie, Luxembourg, Malte, Monténégro, Norvège, Pays-Bas, Pologne, Portugal, République tchèque, Roumanie, Royaume-Uni, Serbie-Monténégro, Slovaquie, Slovénie, Suède, Suisse.

6 Andorre, Moldavie, Russie, Turquie, Ukraine.

7 http://conventions.coe.int/Treaty/FR/Reports/Html/181.htm

8 Allemagne, République tchèque, Slovaquie, Suède.

9 Autriche, Belgique, Chypre, Croatie, Danemark, Finlande, France, Grèce, Irlande, Islande, Italie, Lituanie, Norvège, Pays-Bas, Pologne, Portugal, Royaume-Uni, Suisse, Turquie.

10 http://europa.eu/scadplus/leg/fr/lvb/l14012.htm.

considérations relatives au marché intérieur. En effet, les approches différentes suivies par les États membres en matière de protection des données constituaient un obstacle à la libre circulation entre eux des données à caractère personnel, considérées comme des marchandises. Même si elle n'a pas été guidée, à l'instar de la Convention 108, par des considérations relatives aux droits de l'homme, la Directive va pourtant au-delà des principes affirmés par cette dernière. Elle établit des principes directeurs qui précisent et amplifient les principes affirmés en 1981. Ces principes sont relatifs à la qualité des données, à la légitimité des traitements, aux catégories particulières de traitement, à l'information des personnes concernées, au droit d'accès et au droit d'opposition de ces personnes. La Directive vise ainsi à concilier la protection des données personnelles avec leur libre circulation, non seulement au sein de l'Union européenne, mais aussi en direction de pays tiers. L'ensemble des règles de protection édictées par la Directive a pour but d'assurer un niveau de protection adéquat des données personnelles.

II. Objet

L'objet de ce Code de conduite est de transposer au secteur de la biométrie les normes générales relatives à la protection des données personnelles. Ces textes sont en effet abstraits et impliquent des pesées d'intérêts pour expliciter leur application. Il convient au préalable de préciser que les données biométriques sont des données personnelles, voire même des données dites sensibles

Il n'existe pas de définition légale de la biométrie, ni au niveau international, ni au niveau européen ou national. C'est dans les différentes réglementations relatives à la protection des données personnelles qu'il convient de rechercher les contours du régime de la biométrie. La question liminaire est donc de savoir dans quelle mesure les données biométriques doivent être considérées comme des données personnelles.

Aux termes de l'article 2 de la Directive du 24 octobre 1995, la notion de donnée personnelle recouvre « *toute information concernant une personne physique identifiée ou identifiable ; est réputée identifiable une personne qui 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* ». Par ailleurs, le considérant 26 de la Directive dispose que « *pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne* ». On retrouve cette même définition des « données de caractère personnel » dans la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, adoptée le 28 janvier 1981, dite Convention 108. La Convention 108 définit en ces termes la notion de donnée à caractère personnel : « *toute information relative à une personne physique identifiée ou identifiable (personne concernée)* ». Par « personne identifiable », il conviendrait d'entendre toute personne pouvant être facilement identifiée, ce qui ne concernerait donc pas l'identification de personnes par des méthodes très complexes. La notion de « personne concernée » exprimerait quant à elle l'idée selon laquelle toute personne possède un droit subjectif par rapport aux informations qui la concernent, même si ces informations sont collectées par d'autres[11].

[11] V. sur ce point le Rapport explicatif du Conseil de l'Europe sur la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel : http://conventions.coe.int/treaty/fr/Reports/Html/181.htm

Certaines catégories de données personnelles sont dites sensibles. La directive européenne du 24 octobre 1995, article 8, souligne l'existence de ces données particulières qui révèlent « *l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que (…) les données relatives à la santé et à la vie sexuelle* ». Il s'agit également des « *données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté* », et enfin, des « *numéros nationaux d'identification* », ou de tout autre identifiant de portée générale. Cette notion de « données sensibles » figure également dans les lois nationales des pays membres de l'Union européenne. L'article 6 de la Convention 108 donne une définition proche de ces données, en incluant également les « *données à caractère personnel concernant des condamnations pénales* ».

La biométrie permet l'identification ; or, les dispositions relatives à la protection des données personnelle s'appliquent aux personnes identifiées ou identifiables. Toutefois, différentes opinions s'opposent sur le point de savoir si les données biométriques sont, ou non, des données personnelles. Les définitions précédemment envisagées conduisent à retenir la qualification de donnée personnelle dès lors que l'on a affaire à une information relative à une personne identifiée ou identifiable. Cette définition peut conduire à réfuter la qualification systématique des données biométriques comme données personnelles. L'argument avancé est qu'il est parfois impossible d'identifier un individu à partir d'une trace biométrique, telle par exemple, une empreinte digitale incomplète. On peut aussi arguer du fait que les données biométriques en tant que telles ne fournissent aucune information sur un individu. Ces deux objections tendent donc à démontrer qu'une donnée biométrique ne permettrait pas de faire nécessairement le lien avec l'identité d'un individu, et, partant, ne constituerait pas nécessairement une information relative à une personne identifiée ou identifiable.

On peut aussi estimer, à l'inverse, que les données biométriques permettent, par leur nature même, l'identification d'une personne dans la mesure où elles peuvent être rattachée de manière unique et permanente à un individu. L'argument purement théorique selon lequel il est parfois impossible d'identifier un individu à partir d'une trace biométrique ne résiste pas à l'analyse ; le perfectionnement des techniques conduira à effectuer des identifications qui peuvent s'avérer difficiles aujourd'hui. Par ailleurs, les circonstances entourant la collecte des données biométriques permettent toujours d'obtenir des informations sur la personne concernée ; il est donc toujours possible, à un moment donné, de faire le lien entre un individu et une donnée biométrique.

Cette seconde opinion est majoritaire ; c'est notamment l'avis du Comité consultatif de la Convention 108, qui estime « *qu'il n'est pas nécessaire de décider si les données biométriques sont des données personnelles ou si c'est le cas seulement dans certaines circonstances* »[12]. Il ajoute que « *dès lors que les données biométriques sont collectées en vue d'un traitement automatisé, la possibilité existe que ces données soient rattachées à une personne identifiable* ». L'autorité de protection des données française, la CNIL (Commission nationale de l'informatique et des libertés) considère que « *Les données biométriques ne sont pas des données personnelles comme les autres. Elles ont la particularité de permettre à tout moment l'identification de la personne concernée sur la base d'une réalité biologique qui lui est propre, qui est permanente dans le temps, et dont elle ne peut s'affranchir* »[13].

---

12 Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques, Conseil de l'Europe, 2005.

13 http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/Position-cnil-CNI-05-2005.pdf.

A la lecture des dispositions particulières énumérant les données sensibles, il convient de considérer que les données biométriques peuvent, dans certains cas, être considérées comme telles. Directement issues de la personne concernée et intimement liées à celle-ci, les données biométriques doivent donc être traitées en considération des risques particuliers qu'elles sont susceptibles de générer. Les données biométriques peuvent ainsi, dans une mesure limitée mais existante, permettre de révéler des informations médicales sur la personne concernée. Elles peuvent également apporter des informations sur son origine ethnique.

III. Champ d'application

Soucieux de mieux contrôler les flux migratoires, notamment depuis les attentats du 11 septembre 2001, ce sont les États-Unis qui ont adopté des mesures contraignant indirectement les autres États à mettre en place des documents d'identité incluant des éléments biométriques. Le Règlement européen n° 2252/2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres a ainsi été adopté le 13 décembre 2004[14]. L'insertion des données biométriques dans les documents d'identité devrait aider à la poursuite des objectifs du Règlement, c'est-à-dire :

- la sécurisation des documents de voyage (protection contre la falsification) ;
- l'établissement d'un lien plus fiable entre le document et son titulaire, (protection contre une utilisation frauduleuse).

Le champ d'application territorial du Règlement est le suivant :

- le Danemark, le Royaume-Uni et l'Irlande n'ont pas participé à l'adoption du Règlement et ne sont pas liés par celui-ci ;
- le Règlement constitue un « développement des dispositions de l'acquis de Schengen » et s'applique en conséquence à l'Islande, la Norvège et la Suisse.

Quant au champ d'application matériel, le Règlement s'applique aux passeports et aux documents de voyage délivrés par les États membres. Il ne s'applique donc pas aux cartes d'identité délivrées par les États membres à leurs ressortissants ou aux passeports et aux documents de voyage temporaires ayant une durée de validité inférieure ou égale à 12 mois.

IV. Terminologie

Pour des questions de cohérence, la plupart des définitions du Code reprennent les définitions généralement utilisées dans les différentes lois sur la protection des données.

V. Dispositions relatives à la collecte des données biométriques

1. Les formalités préalables à la collecte des données biométriques

Les responsables de traitements sont soumis à un certain nombre d'obligations préalables à la collecte des données biométriques, notamment l'accomplissement de formalités auprès de l'autorité de protection des données compétente. Selon la loi applicable et selon le degré de gravité du risque

[14] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0001:0006:FR:PDF

d'atteinte aux droits et libertés des personnes concernées, différentes formalités peuvent être envisagées, notamment :

- dispense de formalités ;
- déclaration simplifiée auprès de l'autorité de protection des données compétente ;
- demande d'autorisation de l'autorité de protection des données compétente ;
- demande d'autorisation par voie réglementaire après avis conforme de l'autorité de protection des données compétente.

Notion de détaché à la protection des données :

L'article 18 de la Directive CE/95/46 du 24 octobre 1995 dispose que les États membres peuvent prévoir une simplification de l'obligation de notification ou une dérogation à cette obligation quand le responsable du traitement désigne un détaché à la protection des données à caractère personnel chargé notamment d'assurer, d'une manière indépendante, l'application interne des dispositions nationales prises en application de la Directive, de tenir un registre des traitements effectués par le responsable du traitement et garantissant de la sorte que les traitements ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées. Quelques États membres de l'Union européenne ont à ce jour mis en place un tel dispositif de simplification : l'Allemagne, la Suède, les Pays-Bas, le Luxembourg et la France.

Cas des données sensibles :

Certaines législations sur la protection des données, à l'instar notamment de la loi française[15], imposent des formalités alourdies lorsque les données qui font l'objet d'un traitement sont des données dites sensibles. Ainsi, lorsque le traitement porte sur des données sensibles, le responsable du traitement ou, le cas échéant, son représentant, doit adresser à l'autorité de contrôle compétente une demande d'autorisation préalable à la mise en œuvre d'un traitement de données personnelles, ou d'un ensemble de traitements de données personnelles ayant une même finalité ou des finalités liées.

2. L'information préalable des personnes concernées par un traitement de données biométriques – Principe de transparence

Le droit à l'information de la personne concernée par un traitement de données personnelles est essentiel car c'est celui qui permet le déclenchement de tous les autres. En effet, pour que la personne concernée soit en mesure de faire respecter ses intérêts, il est indispensable qu'elle soit avertie de l'existence d'un traitement.

Le principe de transparence est l'un des éléments constitutifs de la bonne foi et tend à assurer la confiance des personnes concernées par les traitements de données à caractère personnel. Même s'il n'est pas expressément visé par la Directive du 24 octobre 1995, le principe de transparence se déduit néanmoins de celui de loyauté. Le considérant 38 de la Directive souligne en effet que « *le traitement loyal des données suppose que les personnes concernées puissent connaître l'existence des traitements et bénéficier, lorsque des données sont collectées auprès d'elles, d'une information effective et complète au regard des circonstances de cette collecte* ». Le principe de transparence implique donc que la collecte des données ne doit pas être effectuée à l'insu de la personne concernée. Cette dernière doit être en mesure de connaître le responsable du traitement et ses finalités. Elle doit également être informée du type de données collectées. Le principe de transparence induit nécessairement la sincérité et l'exhaustivité de l'information fournie à la

[15] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

personne concernée ; la transparence n'est assurée que dans la mesure où cette information est authentique et complète. Le principe de transparence implique également que le responsable du traitement s'abstienne de traiter les données pour une autre finalité. Le responsable du traitement doit donc en pratique permettre aux personnes concernées d'exercer pleinement leurs droits, et ce, à toutes les étapes de l'utilisation de ses données personnelles (collecte, enregistrement, conservation, transfert et destruction). Application du droit à l'information, la collecte doit ainsi être effectuée de façon visible et connue de la personne faisant l'objet du traitement. A cet effet, le responsable du traitement doit lui communiquer son identité, la finalité de son traitement, le caractère obligatoire ou facultatif des réponses, les destinataires des informations, l'existence de droits, les transmissions envisagées.

3. Le principe de finalité

La finalité revêt une importance particulière dans les traitements de données biométriques. Elle constitue en effet un élément déterminant au regard des techniques utilisées, en particulier pour le choix entre un système d'authentification et un système d'identification. Un système d'authentification (recherche 1 contre 1 : êtes-vous celui que vous prétendez être ?) soulève beaucoup moins de difficultés au regard de la protection des données qu'un système d'identification (recherche 1 contre N : qui êtes-vous ?). Dès lors que le système d'authentification est d'une fiabilité technique satisfaisante, il permet de certifier, dans les limites des taux d'erreur et de la technologie, que l'individu présentant son titre d'identité est bien celui auquel ce dernier a été délivré. Il permet en outre de vérifier l'unicité de l'identité de cet individu, c'est-à-dire le fait que ses données biométriques ne correspondent qu'à une personne et une seule dans le système utilisé. En revanche, l'identification, dont les applications peuvent être beaucoup plus nombreuses, est porteuse de risques majeurs pour les libertés individuelles. C'est pourquoi, si l'on peut admettre le recours à un système d'identification lors de la collecte initiale des données biométriques, il faudra préférer le recours à un système de vérification lors des contrôles ultérieurs.

La problématique essentielle en la matière réside en pratique dans la formulation de la finalité du traitement. Au regard des exigences communautaires, la finalité doit en premier lieu être déterminée, explicite et légitime. Par « déterminée », il convient d'entendre que la finalité doit être fixée avant le début du traitement, et ce, d'une manière suffisamment précise afin qu'il soit possible d'apprécier si elle justifie le traitement et si l'objectif poursuivi ne pourrait pas être atteint sans avoir recours à un traitement de données personnelles. L'adjectif « explicite » est sans doute superflu, dans la mesure où il opère, semble-t-il, un renvoi à l'obligation d'information de la personne concernée sur les finalités du traitement. Il met également l'accent sur l'obligation pesant sur le responsable du traitement de communiquer à l'autorité de protection des données les véritables finalités. Ainsi, si un même traitement sert plusieurs finalités distinctes, l'ensemble de ces finalités doit être communiqué dans un souci de transparence. Il ne saurait en effet être question de se contenter d'un ensemble approximatif de différents objectifs. La légitimité des finalités doit quant à elle être appréciée au cas par cas. En second lieu, il convient de s'assurer que les données ne sont pas traitées ultérieurement de manière incompatible avec les finalités initiales. Cette obligation pèse sur le responsable du traitement qui doit en permanence s'assurer de cette compatibilité. L'appréciation de la compatibilité s'avère néanmoins délicate, à l'instar de la question de l'appréciation des détournements d'usage. Il convient en effet de savoir dans quelle mesure la personne concernée peut, au vu d'une première finalité, raisonnablement s'attendre à ce que ses données soient traitées conformément à une autre finalité ou si l'on a bel et bien affaire à un détournement de finalités. Par ailleurs, dans l'hypothèse où les finalités d'un traitement évoluent en raison d'une modification de la loi, la question se pose de savoir si les nouvelles finalités doivent être considérées comme automatiquement compatibles avec les finalités initiales.

4. Le principe de proportionnalité

Le principe de proportionnalité est l'un des piliers majeurs de la protection des données personnelles. Il constitue un élément d'appréciation de la légalité d'un traitement. En application du principe de proportionnalité, tout traitement de données personnelles doit ainsi être proportionné à ses finalités au regard du risque qu'il fait peser sur la vie privée des personnes concernées. Le responsable du traitement, chargé d'en définir les finalités, doit aussi déterminer la nature des données nécessaires à leur atteinte. Le principe de proportionnalité apparaît donc comme le moyen de limiter le traitement de données personnelles au strict nécessaire, c'est-à-dire aux données « *adéquates, pertinentes et non excessives* ».

Le principe de proportionnalité est essentiel en matière de données biométriques. Parce qu'elles recèlent des informations intrinsèquement liées à la personne, les données biométriques doivent être utilisées avec une précaution toute particulière. Au regard de la proportionnalité, il convient de s'assurer que l'identification ou l'authentification des personnes ne peuvent pas être assurées de manière aussi sûre et efficace par un autre procédé ; il convient également d'écarter tout système d'identification dès lors qu'un système d'authentification est suffisant au regard de l'objectif poursuivi ; il convient en dernier lieu de privilégier la collecte de données biométriques ne laissant pas de traces et ne pouvant être captées à l'insu de la personne concernée, ainsi que les méthodes d'anonymisation des données.

5. Les possibilités de collectes alternatives

Dans la mesure où la biométrie permet d'établir un lien automatique entre des données abstraites relatives à l'individu et l'individu lui-même, les techniques utilisées doivent être universelles, c'est-à-dire qu'elles doivent être applicables à tous les individus. Or, des problèmes techniques peuvent empêcher la collecte de données biométriques. On parle alors de *Failure to acquire* (FTA). Cette impossibilité peut résulter de caractéristiques physiques particulières de la personne concernée par le prélèvement de données biométriques. Par ailleurs, d'autres « réticences involontaires » peuvent empêcher la collecte de données biométriques : blessures pour les empreintes digitales, maquillage pour la reconnaissance faciale, ou encore un simple rhume pour la reconnaissance vocale.

VI. Dispositions relatives à l'usage des données biométriques

1. Identification du responsable du traitement

Il faut envisager la possibilité d'une désignation par la loi du responsable du traitement des données biométriques des possesseurs de documents d'identité. La recherche du responsable ne doit pas être diluée dans une structure complexe.

Dans les systèmes biométriques, la détermination de l'identité du responsable du traitement n'est en effet pas toujours aisée. En ce qui concerne plus spécialement les données biométriques des porteurs de passeports, s'agit-il du législateur ayant décidé la mise en place d'un tel traitement ou de l'autorité locale ayant en charge leur délivrance ? La question peut être discutée. Si le premier détermine la finalité du traitement des données biométriques contenues dans les passeports et dresse la liste des catégories de données traitées, c'est en pratique la seconde qui a effectivement accès à ces données.

2. Obligation de sécurité

Tout traitement de données personnelles fait peser sur les personnes concernées un risque d'atteinte à leur vie privée. Aux termes du principe de sécurité, le responsable du traitement doit donc prendre toutes les précautions utiles pour préserver la sécurité des données. Il s'agit là d'une obligation de moyens. Il convient de faire application du principe de proportionnalité quant au choix des mesures de sécurité qui doivent être mises en place par le responsable du traitement, la plupart des traitements de données personnelles présentant un risque d'atteinte à la vie privée. Le niveau de sécurité doit toutefois être fonction de l'importance du risque potentiel que le traitement fait peser sur la vie privée de la personne concernée. La nature des données traitées ne peut à cet égard être ignorée : le traitement de données dites sensibles nécessite un niveau de sécurité particulièrement élevé. Les mesures envisagées sont également étroitement liées à l'ensemble des connaissances, outils, et techniques disponibles en matière de sécurité au moment considéré. Cette exigence impose au responsable du traitement d'adapter en permanence les moyens qu'il met en œuvre pour assurer le niveau de sécurité « raisonnable », eu égard au risque d'atteinte à la vie privée des personnes concernées. Enfin, les mesures de sécurité doivent être fonction des coûts de leur mise en œuvre. Mais s'il est légitime que le responsable du traitement prenne en considération ce dernier élément lors du choix des mesures de sécurité qu'il entend mettre en œuvre, le critère du coût doit toutefois s'effacer derrière le risque d'atteinte à la vie privée. Le responsable du traitement ne peut pas se retrancher derrière des considérations financières pour justifier un choix de mesures qui s'avèreront peu fiables au regard de la protection des données. Le critère prépondérant est celui du risque d'atteinte à la vie privée ; il convient ainsi, en toute hypothèse, de s'assurer que le responsable du traitement a bien mis en œuvre un niveau de sécurité raisonnable et proportionné au regard du risque d'atteinte à la vie privée des personnes concernées.

3. Mode et durée de conservation des données

La maîtrise des outils biométriques est la clé de voûte de la protection des personnes concernées par des traitements biométriques. En effet, dès lors que les systèmes sont mis en place et que les données sont collectées, il paraît peu vraisemblable de revenir en arrière.

Le recours à la biométrie ne pose guère de problème dès lors que les données sont conservées sur soi ou sur un appareil dont on a l'usage exclusif et nulle part ailleurs. Techniquement, on parle de stockage centralisé lorsque l'image de l'empreinte biométrique est stockée dans une base de données sur un serveur. L'utilisateur n'a pas d'accès direct à ces données. De plus, l'utilisateur n'a pas de contrôle immédiat sur l'utilisation qui est faite de son empreinte. Or, l'un des aspects majeurs de la protection des données personnelles est le droit d'accès dont dispose la personne concernée sur ses données. A l'inverse, on parle de stockage décentralisé lorsque l'image de l'empreinte est stockée sur un support local. L'utilisateur a accès à cette image et peut contrôler l'utilisation qui est faite de son empreinte.

Quant à la durée de conservation des données, il convient d'envisager le devenir des données biométriques. A l'instar de ce qui se produit dans d'autres domaines (notamment dans le domaine des biotechnologies), on doit se demander de quelle maîtrise dans le temps on peut disposer sur les données biométriques : une fois prélevées, que va-t-on en faire ? La plus grande prudence est donc de mise sur l'avenir de ces données, le caractère unique et permanent des données biométriques soulevant d'importants problèmes. Le Groupe de l'article 29 a ainsi rendu un avis[16] dans lequel il exprime les plus grandes réserves quant à la conservation des données biométriques dans une base de données au-delà de la période nécessaire aux contrôles relatifs à la délivrance, à la production et

[16] Avis 7/2004 du 11 août 2004 sur l'insertion d'éléments biométriques dans les visas et titres de séjour en tenant compte de la création du système d'information Visas (VIS).

à la remise aux demandeurs de leurs documents d'identité, et ce, en raison notamment des traces que toute personne est susceptible de laisser derrière elle dans les actes de la vie quotidienne.

4. Choix des données biométriques traitées

De nombreux systèmes biométriques permettent la conservation des données prélevées lors des collectes secondaires, c'est-à-dire les données afférentes à l'utilisation du système. On parle techniquement de « données associées » ou de « données de trafic ». Ces traces laissées par tout individu qui a été en contact avec le système permettent de déterminer le moment et le lieu de ce contact.

Du point de vue de la protection des données, il est ainsi préférable de choisir un élément biométrique ne laissant pas de trace et ne pouvant être capté à l'insu de la personne concernée (contour de la main ou iris par exemple) afin notamment de minimiser les risques de détournement de finalité ou de traçage des individus. Le risque de traçage est en effet maximum lorsque l'élément biométrique choisi est l'empreinte digitale, dans la mesure où chacun en laisse un peu partout malgré lui. Cette empreinte pourrait ainsi être exploitée à des fins d'identification à partir d'objets les plus divers et les plus usuels. On glisse alors du risque de traçage au risque de détournement de fonction de la base de données.

5. Transferts des données biométriques vers l'étranger

L'utilisation croissante du traitement automatisé de données personnelles facilite leur transfert par-delà les frontières entre pays avec des niveaux de protection très différents. Depuis quelques années, l'activité quotidienne des autorités de protection des données comporte une dimension internationale importante. La globalisation des échanges explique cette évolution[17]. Toutefois, même si les objectifs qui sous-tendent ces transferts internationaux de données sont légitimes (lutte contre le terrorisme, sécurité des marchés financiers…), leur réalisation doit avoir lieu dans des conditions qui garantissent le respect de la vie privée des personnes concernées.

Aux termes de la Directive européenne du 24 octobre 1995, le principe est simple : un transfert de données personnelles vers l'étranger ne peut avoir lieu que si le pays tiers assure un « *niveau de protection adéquat ou suffisant* » de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet. L'article 25 prévoit que le caractère adéquat du niveau de protection doit être apprécié au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données. Sont ainsi prises en compte : la nature des données, la finalité et la durée du ou des traitements envisagés, le pays d'origine et la destination finale des données, mais aussi les règles de droit générales ou sectorielles en vigueur dans les pays tiers ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées. La Commission européenne a le pouvoir de reconnaître qu'un pays dispose d'un niveau de protection adéquat ou suffisant, en rendant, à cet effet une « décision d'adéquation ».

A ce jour, les 27 pays de l'Union européenne ont transposé la Directive du 24 octobre 1995. Toutes ces législations doivent dès lors être considérées comme *équivalentes*, les transferts entre ces pays sont libres. Notons que la transposition de la Directive a été un critère permettant l'adhésion des nouveaux États membres. Par ailleurs, l'Islande, le Liechtenstein et la Norvège, membres de l'Association Européenne de Libre Échange (AELE), ont également transposé la Directive en

---

[17] Sur ce point, V. E. Maître Arnaud, « Le droit comparé et la globalisation des échanges, le cas des flux transfrontières de données personnelle*s »,* in : *Legal Engineering and Comparative Law/L'ingénierie juridique et le droit comparé : Rapports préparés par les collaborateurs ISDC à l'occasion du 25e anniversaire de l'Institut suisse de droit comparé*, Tome 1**,** Publications de l'Institut suisse de droit comparé, vol. 61, Zurich, Schulthess, 2008, p.203 à 27.

application des obligations imposées par l'accord sur l'Espace Économique Européen (EEE). Les transferts entre ces États et les États membres de l'Union européenne sont libres. La Suisse est membre de l'AELE, mais ne fait pas partie de l'EEE. Elle a toutefois fait l'objet d'une décision d'adéquation de la Commission européenne en 2000,[18] permettant les transferts de données avec les États membres de l'Union européenne. En Europe, Guernesey,[19] Jersey,[20] ou encore l'Île de Man[21] ont également fait l'objet d'une telle décision.

6. Pouvoirs des autorités de contrôle

Ces pouvoirs sont variables en fonctions des pays. Toutes les autorités de protection des données devraient au moins disposer du pouvoir de mener des enquêtes sur la façon dont est conduit le traitement des données biométriques des possesseurs de documents d'identité. Il convient également de souligner la nécessaire indépendance des autorités de protection des données par rapport aux États.

La plupart des États disposant d'une réglementation relative à la protection des données personnelles sont également dotés d'une autorité de contrôle. La mise en place d'une telle autorité est même obligatoire pour les États membres de l'Union européenne. L'article 28 de la Directive du 24 octobre 1995 dispose en effet que « *chaque État membre prévoit qu'une oui plusieurs autorités publiques sont chargées de surveiller l'application, sur son territoire, des dispositions adoptées (…) en application de la présente Directive. Ces autorités exercent en toute indépendance les missions dont elles sont investies* ».

Chaque autorité de contrôle doit être consultée lors de l'élaboration de mesures administratives ou réglementaires relatives à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel.

Les autorités de contrôle disposent de différents pouvoirs :

- pouvoirs d'investigation,
- pouvoirs d'intervention (avis préalables à la mise en œuvre de traitements, interdictions de traitements, saisine d'institutions politiques nationales),
- pouvoirs d'ester en justice.

Les autorités de contrôle peuvent être saisies par toute personne ou toute association les représentant. Elles doivent établir, à intervalles réguliers, un rapport d'activités.

Hors Union européenne, d'autres États se sont également dotés d'autorités de contrôle. Tel est bien entendu le cas de l'Islande, du Liechtenstein et de la Norvège, membres de l'Association Européenne de Libre Échange, qui ont transposé la Directive en application des obligations imposées par l'Accord sur l'Espace économique européen. Tel est le cas également des pays ayant fait l'objet d'une « décision d'adéquation » de la Commission européenne ; d'autres pays disposent également d'une autorité de contrôle, bien que leur niveau de protection n'ait pas fait l'objet d'une décision d'adéquation.

---

18 Décision 2000/518/EC du 26 juillet 2000, JOUE L218 du 25 août 2000.

19 Décision du 21 novembre 2003, JOUE L308 du 25 novembre 2003.

20 Décision 2008/393/CE du 8 Mai 2008, JOUE L138 du 28 mai 2008.

21 Décision 2004/411/CE du 28 avril 2004, JOUE L151 du 30 avril 2004.

Notons enfin que l'article 1 Protocole additionnel à la Convention 108 sur les autorités de contrôle et les flux transfrontières de données, ouvert à la signature depuis le 8 novembre 2001,[22] énonce que chaque État partie prévoit qu'une ou plusieurs autorités sont chargées de veiller au respect des mesures donnant effet, dans son droit interne, aux principes énoncés dans la Convention 108 et dans le Protocole additionnel.

VII. Droit des personnes concernées par un traitement de données biométriques

1. Le droit d'accès

Le droit d'accès tend à permettre à la personne concernée de s'assurer notamment de l'exactitude des données biométriques et de la licéité du traitement. Ce droit d'accès est le pendant logique du droit à l'information. La personne concernée est en effet passive dans l'exercice de son droit à l'information ; elle dépend du bon vouloir du responsable du traitement qui doit lui fournir cette information. L'exercice du droit d'accès est quant à lui actif, il suppose une initiative de la personne concernée qui prend contact avec le responsable du traitement afin de faire valoir ses droits.

Le droit d'accès est en principe gratuit mais la plupart des législations relatives à la protection des données prévoient des exceptions à cette gratuité ; ces exceptions sont toutefois limitées eu égard aux impératifs de protection des libertés fondamentales sous-jacents à l'exercice du droit d'opposition.

2. Le droit de rectification

L'exactitude des données est l'un des principes majeurs de la protection des données. Toutefois, même si les données biométriques stockées dans le système sont exactes, les résultats donnés par le traitement peuvent être faux. Tout système biométrique comporte en effet un élément de probabilité. Il est ainsi parfaitement envisageable qu'une personne soit rejetée à tort. Dans cette hypothèse, il est donc juridiquement impossible de considérer que les données enrôlées sont exactes au regard de la finalité poursuivie par leur traitement, c'est-à-dire, en matière de documents d'identité, l'authentification du porteur du titre.

Ainsi, il est indispensable de prévoir, à la charge des responsables de traitements, une obligation d'accéder à la demande d'un individu qui souhaiterait faire jouer son droit de rectification face à un taux de faux rejets important. L'exercice du droit de rectification emporte en pratique la possibilité pour la personne concernée de pouvoir être enrôlée une nouvelle fois. Il convient de préciser ce que l'on entend par « importance du taux de faux rejets ». Il faut en effet prévenir tout litige relatif à l'appréciation du degré acceptable de faux rejets. Une politique des taux d'erreur doit être mise en place en amont et portée à la connaissance du public concerné. L'application du principe de transparence doit ici être mise en balance avec la confidentialité des ajustements opérés par le responsable du traitement en vue de réduire le taux acceptable de faux rejets.

3. Le droit d'opposition

Le droit d'opposition emporte pour la personne concernée le droit de s'opposer, dans certaines hypothèses, au traitement de ses données personnelles. Toute personne est donc en principe en mesure de s'opposer au traitement de ses données pour des motifs légitimes. Notons que le droit d'opposition exercé par une personne concernée ne porte que sur ses données personnelles et n'a donc aucune incidence sur le traitement lui-même qui peut se poursuivre sur les données d'autres personnes concernées.

---

[22] http://conventions.coe.int/Treaty/FR/Reports/Html/181.htm

Le droit d'opposition n'est pas absolu et la plupart des législations relatives à la protection des données personnelles prévoient des exceptions à son exercice. L'exercice du droit d'opposition peut ainsi notamment être écarté :

- lorsque le traitement de données répond à une obligation légale ;
- lorsque l'application du droit d'opposition a été écartée par une disposition expresse de l'acte autorisant le traitement.

4. La prohibition des prises de décision automatiques

Il est essentiel de prévoir légalement la possibilité pour la personne concernée de demander, en toutes circonstances, un réexamen de ses données avec une présence humaine en dernier recours. Ceci sous-entend qu'un représentant du responsable du traitement doit être présent sur tous les lieux de prélèvement secondaire de données biométriques.

5. La présomption d'innocence

L'utilisation de la biométrie comporte un risque au regard de la présomption d'innocence, consacrée notamment à l'article 9 de la Déclaration universelle des droits de l'homme : « *Tout homme étant présumé innocent jusqu'à ce qu'il ait été déclaré coupable, s'il est jugé indispensable de l'arrêter, toute rigueur qui ne serait pas nécessaire pour s'assurer de sa personne doit être sévèrement réprimée par la loi* ». En effet, le droit à la présomption d'innocence existe indépendamment de toute reconnaissance future de culpabilité ou d'innocence, et l'individu suspecté peut ainsi protéger son honneur et sa réputation contre les tiers.

Que devient cependant la présomption d'innocence quand l'utilisation de la biométrie permet d'appréhender des individus à des fins d'identification, et ce, quel que soit le caractère répréhensible, ou non, de leur comportement ? Le principe même de la présomption d'innocence semble renversé par l'intervention, en amont d'une procédure, de la biométrie qui pourrait conduire, à elle seule, à déterminer la culpabilité ou l'innocence d'un individu. De plus, le risque d'atteinte à la présomption d'innocence est inversement proportionnel aux taux d'erreurs : plus un système sera jugé fiable, moins les taux d'erreurs seront élevés, plus il sera difficile de prouver une éventuelle confusion d'identité.

Les résultats issus de l'application de techniques biométriques ne devraient pas pouvoir produire directement des effets juridiques, leur portée étant essentiellement pratique en ce qui concerne les titres d'identité. La biométrie pourrait néanmoins permettre de fournir des indices. Il est encore tôt pour apprécier les effets de leur utilisation sur le plan contentieux : les résultats obtenus au moyen de la biométrie seront-ils considérés comme un moyen de preuve suffisant ? La « preuve » biométrique ne doit pas devenir une preuve automatique restreignant l'appréciation souveraine du juge. D'autres moyens de preuve doivent pouvoir en effet être produits et c'est au juge, saisi d'un éventuel litige, qu'il doit appartenir de décider de la valeur qu'il entend accorder à cet indice de nature technique.