GROUPE DE TRAVAIL "ARTICLE 29"
SUR LA PROTECTION DES DONNEES

12168/02/FR
GT 80

Document de travail sur la biométrie

Adopté le 1er août 2003

LE GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL, institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995[1],

vu l'article 29 et l'article 30, paragraphe 1, point a) et paragraphe 3 de ladite directive,

vu son règlement intérieur, et notamment les articles 12 et 14 de celui-ci,

a adopté le présent document de travail:

1. INTRODUCTION

Les progrès rapides des technologies biométriques ainsi que la généralisation de leur application durant ces dernières années nécessitent un examen attentif sur le plan de la protection des données[2]. Une utilisation répandue et non contrôlée de la biométrie suscite des inquiétudes en ce qui concerne la protection des libertés et des droits fondamentaux des personnes. Les données de ce genre 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[3].

Aujourd'hui, il est souvent fait recours au traitement de données biométriques dans des procédures automatisées d'authentification/vérification et d'identification, notamment lors du contrôle de l'entrée dans des zones physiques et virtuelles (c'est-à-dire l'accès à des systèmes ou services électroniques particuliers).

Précédemment, l'utilisation de la biométrie se limitait pour l'essentiel aux domaines de l'ADN et de la vérification d'empreintes digitales. Les empreintes digitales étaient collectées en particulier à des fins de répression (par exemple dans le cadre d'enquêtes judiciaires). Si la société encourage le développement de bases de données d'empreintes digitales ou d'autres bases de données biométriques en vue d'autres applications courantes, elle pourrait accroître les possibilités de réutilisation de ces données par des tiers comme éléments de comparaison et de recherche dans le cadre de leurs propres activités, sans que cet objectif ait été envisagé initialement; les autorités chargées d'appliquer la loi pourraient figurer parmi les tiers précités.

Une préoccupation spécifique liée aux données biométriques consiste dans le risque d'une désensibilisation du public, en raison d'une utilisation toujours croissante de ces données, aux conséquences que leur traitement peut avoir sur la vie quotidienne. Par

---

[1] Journal officiel L 281 du 23.11.1995, p. 31, disponible à l'adresse suivante: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm.

[2] Depuis le 11 septembre 2001, la biométrie a souvent été présentée comme un moyen valable d'améliorer la sécurité publique. Au niveau de l'UE, l'intégration d'éléments biométriques dans les cartes d'identité, passeports, documents de voyage et visas est à l'étude. Les États-Unis exigeront bientôt des identifiants biométriques pour les étrangers entrant sur leur territoire et quittant celui-ci. La convention n° 108 de l'OIT a été modifiée en 2003 par l'introduction du recours obligatoire à la biométrie pour les gens de mer. Des discussions se poursuivent également dans d'autres enceintes internationales, telles que le G8, l'OCDE, etc.

[3] Cependant, cette identification certaine dépend de différents facteurs, dont la taille de la base de données et le type d'éléments biométriques utilisés.

exemple, le recours à la biométrie dans les bibliothèques scolaires peut rendre les enfants moins conscients des risques qui sont liés à la protection des données et qui peuvent avoir des conséquences pour eux plus tard dans la vie.

Le présent document a pour but de contribuer à l'application efficace et homogène des dispositions nationales adoptées en vertu de la directive 95/46/CE aux systèmes biométriques. Il porte principalement sur les applications biométriques servant à des fins d'authentification et de vérification. Le groupe de travail entend proposer des orientations uniformes au niveau européen, notamment pour l'industrie des systèmes biométriques et pour les utilisateurs de ces technologies.

2. DESCRIPTION DES SYSTEMES BIOMETRIQUES

Les systèmes biométriques sont des applications de technologies biométriques, qui permettent l'identification et/ou l'authentification/vérification automatiques d'une personne[4]. Des applications d'authentification/vérification sont fréquemment utilisées pour l'exécution de diverses tâches relevant de domaines totalement différents et sous la responsabilité d'un vaste éventail d'entités différentes.

Chaque technique biométrique, qu'elle vise l'authentification/vérification ou l'identification, dépend plus ou moins de l'élément biométrique concerné, qui peut être:
- **universel :** l'élément biométrique est présent chez tous les individus[5];
- **unique** : l'élément biométrique doit être propre à chaque personne;
- **permanent :** chaque personne conserve au cours du temps la propriété de l'élément biométrique.

On peut distinguer deux catégories principales de techniques biométriques, selon que des données stables ou des données dynamiques sur le comportement sont utilisées[6].

En premier lieu, il existe des techniques basées sur l'aspect physique et la **physiologie** qui mesurent les caractéristiques physiologiques d'une personne; elles comprennent la vérification des empreintes digitales, l'analyse de l'image du doigt, la reconnaissance de l'iris, l'analyse de la rétine, la reconnaissance faciale, la géométrie de la main, la reconnaissance de la forme de l'oreille, la détection de l'odeur corporelle, la reconnaissance vocale, l'analyse de la structure de l'ADN[7], l'analyse des pores de la peau, etc.

---

[4] La différence entre l'authentification (vérification) et l'identification est importante. L'authentification répond à la question: suis-je celui ou celle que je prétends être? Le système certifie l'identité de l'individu en traitant des données biométriques qui se réfèrent à la personne posant la question et prend une décision oui/non (comparaison 1:1). L'identification répond à la question: qui suis-je? Le système reconnaît l'individu qui pose la question en le distinguant d'autres personnes dont les données biométriques sont également enregistrées. Dans ce cas, le système prend une décision "1 sur n" et répond que la personne posant la question est X.

[5] À cet égard, tous les éléments biométriques ne sont pas équivalents, et le taux de différenciation d'une personne par rapport à une autre varie considérablement en fonction des éléments biométriques utilisés. Les éléments biométriques les plus distinctifs semblent être l'ADN, la rétine et l'empreinte digitale.

[6] Certaines techniques peuvent reposer à la fois sur la physiologie et sur le comportement.

[7] Bien que l'utilisation de l'ADN à des fins d'identification biométrique soulève des questions spécifiques, celles-ci ne seront pas examinées dans le présent document. On peut noter qu'il ne semble

En second lieu, on dispose de techniques **comportementales** qui mesurent le comportement d'une personne; elles comprennent la vérification de la signature manuscrite, l'analyse de la frappe sur le clavier, l'analyse de la démarche, etc.

De nombreux systèmes biométriques tiennent compte de l'évolution rapide des technologies et du souci accru de sécurité, et fonctionnent en associant diverses modalités biométriques de l'utilisateur avec d'autres technologies d'identification ou d'authentification. Certains systèmes combinent par exemple la reconnaissance faciale et l'enregistrement de la voix. Pour effectuer une authentification, trois méthodes différentes peuvent être utilisées conjointement: l'identification se fera alors sur la base de quelque chose qu'une personne sait (mot de passe, numéro personnel d'identification, etc.), de quelque chose qu'une personne possède (jeton, clé CAD, carte à puce, etc.) et de quelque chose qu'une personne est (une caractéristique biométrique). Sur un ordinateur, on pourrait, par exemple, introduire une carte à puce, taper un mot de passe et présenter son empreinte digitale.

La collecte d'échantillons biométriques, appelés "données biométriques", telles que l'empreinte digitale, la photographie de l'iris ou de la rétine, l'enregistrement de la voix), est réalisée durant une phase d'"inscription" à l'aide d'un capteur spécifique pour chaque type d'élément biométrique. Le système biométrique extrait de ces données des traits spécifiques à l'utilisateur pour construire un "modèle" biométrique. Celui-ci est une réduction structurée d'une image biométrique, c'est-à-dire la mesure biométrique enregistrée d'un individu. C'est le modèle sous sa forme numérisée qui sera enregistré, et non l'élément biométrique lui-même. En outre, les données biométriques peuvent être traitées comme des données brutes (une image) en fonction du système biométrique qui est utilisé.[8]

La phase d'inscription a une importance primordiale car c'est la seule où les données brutes, les algorithmes d'extraction et de protection (cryptographie, hachage, etc.) et les modèles sont présents simultanément. À cet égard, il convient de souligner que, si les données brutes révèlent des informations qui peuvent être considérées comme sensibles au sens de l'article 8 de la directive 95/46/CE, le processus d'inscription de ces données doit se dérouler conformément à cette disposition (voir plus loin, point 3.7).

Sur le plan de la protection des données, la forme sous laquelle sont conservés les modèles relatifs aux utilisateurs est également importante. La conservation des modèles dépend du type d'application pour lequel le dispositif biométrique sera utilisé et de la taille des modèles eux-mêmes. Les modèles peuvent être conservés:

a) - dans la mémoire d'un dispositif biométrique;
b) - dans une base de données centrale;
c) - sur des cartes plastiques, des cartes optiques ou des cartes à puce. Cette méthode de conservation permet aux utilisateurs de porter sur eux leurs modèles comme moyens d'identification.

---

pas possible actuellement de générer un profil d'ADN en temps réel en tant que moyen d'authentification.

[8] Le présent document se réfère essentiellement aux systèmes biométriques basés sur des "modèles", mais pourrait également s'appliquer à des données brutes. Toutefois, le caractère spécifique de ces dernières pourrait conduire à une adaptation des exigences en matière de protection des données.

En principe, l'enregistrement des données de référence dans une base de données n'est pas nécessaire aux fins de l'authentification/vérification; un stockage décentralisé des données à caractère personnel est suffisant. En revanche, l'identification n'est réalisable qu'avec un stockage centralisé des données de référence parce que, pour vérifier l'identité de la personne concernée, le système doit comparer le modèle ou les données brutes (image) de cette personne avec ceux de toutes les personnes dont les données sont déjà enregistrées dans une mémoire centrale.

Toujours dans une perspective de protection des données, il est très important de noter que certains systèmes biométriques reposent sur des informations telles que des empreintes digitales ou des échantillons d'ADN, qui peuvent être recueillies à l'insu du sujet concerné car celui-ci peut laisser des traces sans le savoir. Par l'application d'un algorithme biométrique à une empreinte digitale relevée sur un verre, on parviendra peut-être[9] à déterminer si une personne est enregistrée dans une base de données contenant des données biométriques et, le cas échéant, qui est cette personne, en procédant à une comparaison des deux modèles. Cette observation vaut également pour d'autres systèmes biométriques, tels que ceux qui sont basés sur l'analyse de la frappe sur un clavier ou sur la reconnaissance faciale à distance, en raison des caractéristiques spécifiques de la technologie mise en œuvre[10]. Le problème réside dans le fait que, d'une part, cette collecte et ce traitement de données peuvent être réalisés à l'insu de la personne concernée et que, d'autre part, quelle que soit leur fiabilité actuelle, ces technologies biométriques se prêtent à une utilisation généralisée en raison de leur "faible niveau d'intrusion". Il semble dès lors nécessaire de définir des garanties spécifiques à cet égard.

3. APPLICATION DES PRINCIPES DE LA DIRECTIVE 95/46/CE

3.1. Application de la directive 95/46/CE

Conformément à l'article 2, point a), de la directive 95/46/CE, il faut entendre par "données à caractère personnel" 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 (...)". Au considérant 26, il est précisé 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".

Selon cette définition, les mesures d'identification biométrique ou leur version numérisée sous forme de modèle sont, dans la plupart des cas, des données à caractère personnel.[11] Il apparaît que des données biométriques peuvent toujours être considérées comme "des informations concernant une personne physique", puisqu'il s'agit de données qui

---

9 Cela implique cependant que l'on dispose au moins de certains moyens, tels que la possibilité de prélever l'empreinte sur le verre sans l'endommager, l'équipement technique nécessaire pour traiter les données fournies par l'empreinte, ainsi que l'accès à l'algorithme du constructeur et/ou à la base de données des empreintes digitales.

10 Voir point 3 concernant l'application de la directive 95/46/CE, et en particulier le point 3.3 relatif à l'obligation d'informer la personne concernée.

11 Si des données biométriques, telles qu'un modèle, sont stockées de telle manière qu'aucun moyen raisonnable ne peut être mis en œuvre par le responsable du traitement ou une autre personne pour identifier la personne concernée, ces données ne sont pas à qualifier de données à caractère personnel.

fournissent, par leur nature même, des informations sur une personne précise. Dans le contexte de l'identification biométrique, la personne est généralement identifiable, puisque les données biométriques sont utilisées à des fins d'identification ou d'authentification/vérification au moins dans la mesure où la personne concernée est distinguée de toute autre personne[12].

Conformément à l'article 3, paragraphe 1, de la directive 95/46/CE, les principes de la protection des données s'appliquent au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel faisant partie ou appelées à faire partie d'un fichier. La directive ne s'applique pas aux données qui sont traitées par une personne physique dans le cadre d'une activité purement personnelle ou domestique. De nombreuses applications biométriques dans le cadre domestique relèveront de cette catégorie.

Au-delà de ces exclusions spécifiques, le traitement de données biométriques ne peut être considéré comme licite que si toutes les procédures concernées - à commencer par l'inscription - sont mises en œuvre dans le respect des dispositions de la directive 95/46/CE.

Le présent document ne couvre pas toutes les questions soulevées par l'application de la directive 95/46/CE aux données biométriques, mais uniquement les plus pertinentes. Il ne dresse donc pas un tableau complet des conséquences de l'application de cette directive.

3.2. Principes de finalité et de proportionnalité

Selon l'article 6 de la directive 95/46/CE, les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités. De plus, les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement (principe de finalité).

Le respect de ce principe implique tout d'abord une définition claire de la finalité pour laquelle les informations biométriques sont collectées et traitées. En outre, une évaluation du respect des principes de proportionnalité et de légitimité est nécessaire et doit être effectuée en tenant compte des risques concernant la protection des libertés et des droits fondamentaux de la personne; il s'agit notamment d'établir si la finalité poursuivie ne pourrait pas être atteinte d'une façon moins intrusive. La proportionnalité a été le critère déterminant dans presque toutes les décisions relatives au traitement de données biométriques qui ont été prises jusqu'ici par les autorités chargées de la protection des données[13].

Le groupe de travail est d'avis que l'utilisation, à des fins de contrôle d'accès (authentification/vérification), de systèmes biométriques se référant à des caractéristiques physiques qui ne laissent pas de traces (par exemple la forme de la main, mais non les

---

[12] L'identifiabilité de la personne dépend également de la disponibilité d'autres données qui - conjointement et séparément - permettent d'identifier la personne en question. La possibilité d'une "identification directe" par référence à "un ou plusieurs éléments spécifiques propres à son identité physique" est expressément mentionnée dans la définition des données à caractère personnel à l'article 2, point a), de la directive 95/46/CE.

[13] Par exemple les décisions des autorités néerlandaises, françaises, allemandes, italiennes et grecques.

empreintes digitales) ou de systèmes biométriques se référant à des caractéristiques physiques qui laissent des traces, mais dont les données ne sont pas enregistrées dans une mémoire détenue par une personne autre que la personne concernée (autrement dit, les données ne sont pas mises en mémoire dans le dispositif de contrôle d'accès ou dans une base de données centrale), crée moins de risques pour la protection des libertés et des droits fondamentaux de la personne.[14] Plusieurs autorités de protection des données se sont ralliées à cette opinion et ont indiqué que les éléments biométriques devraient, de préférence, être conservés non pas dans une base de données, mais plutôt dans un dispositif exclusivement accessible à l'utilisateur, tel qu'une carte à puce, un téléphone portable ou une carte bancaire[15]. En d'autres termes, les applications d'authentification/vérification qui peuvent être mises en œuvre sans enregistrement central de données biométriques ne devraient pas faire appel à des techniques d'identification excessives.

C'est la raison pour laquelle le groupe de travail estime qu'avant de mettre en place d'autres types d'applications (fondées par exemple sur la mise en mémoire de modèles d'empreintes digitales dans des terminaux d'accès ou dans une base de données centrale), il y a lieu de les soumettre à une évaluation minutieuse. Toutefois, si ce type de système est mis en œuvre, par exemple dans le cas d'installations de haute sécurité[16], il peut être considéré comme un traitement de données qui présente des risques au sens de l'article 20 de la directive 95/46/CE, et donc être soumis au contrôle préalable des autorités chargées de la protection des données conformément à la législation nationale (voir point 3.5).

La directive 95/46/CE interdit un traitement ultérieur qui serait incompatible avec les finalités pour lesquelles les données ont été collectées. Par exemple, lorsque des données biométriques sont traitées à des fins de contrôle d'accès, leur utilisation en vue d'évaluer l'état émotionnel de la personne concernée ou de surveiller une personne sur son lieu de travail ne serait pas compatible avec la finalité initiale. Toutes les mesures appropriées doivent être prises pour empêcher ce type de réutilisation incompatible[17]. La directive 95/46/CE prévoit, sous certaines conditions, des dérogations à l'interdiction de soumettre les données à un traitement ultérieur dans un but incompatible avec la finalité initiale.

Il est généralement admis que le risque de réutilisation, pour des finalités incompatibles, de données biométriques obtenues à partir de traces physiques laissées par des personnes à leur insu (empreintes digitales par exemple) est relativement faible lorsque les données sont conservées non pas dans des bases de données centralisées, mais par la personne

---

[14] On peut faire une distinction entre le cas où les données biométriques sont traitées de manière centralisée et celui où les données de référence biométriques sont enregistrées sur un dispositif mobile et où le processus de mise en correspondance s'effectue sur la carte, mais non sur le capteur, voire celui où le capteur fait partie du dispositif mobile.

[15] Les mécanismes prévus pour remédier aux problèmes découlant de la perte, du vol ou de la détérioration des cartes doivent être pris en compte. Les mécanismes n'entraînant pas le stockage de données biométriques devraient être favorisés. Dans toute la mesure du possible, les données devraient être recueillies à nouveau directement auprès de la personne concernée.

[16] Dans l'état actuel de la technologie biométrique, il n'existe pas encore des solutions fiables d'identification pure en temps réel pour une population, quelle qu'en soit la taille, et il est peu probable que des solutions de cette nature soient disponibles dans un avenir proche.

[17] Comme indiqué plus haut, cette finalité doit être clairement définie.

concernée, et qu'elles sont inaccessibles aux tiers. Le stockage centralisé de données biométriques accroît également le risque que ces données soient utilisées comme une clé pour interconnecter différentes bases de données, ce qui pourrait permettre d'obtenir un profil détaillé des habitudes d'un individu, tant dans la sphère publique que dans la sphère privée. La question de la compatibilité des finalités pose également le problème de l'interopérabilité de différents systèmes reposant sur la biométrie. La standardisation qu'exige l'interopérabilité pourrait entraîner une plus forte interconnexion entre les bases de données.

L'utilisation de la biométrie soulève en outre la question de la proportionnalité de chaque catégorie de données traitées à la lumière de la finalité pour laquelle les données sont exploitées. Des données biométriques ne doivent être utilisées que si leur utilisation est adéquate, pertinente et non excessive, ce qui implique une évaluation rigoureuse de la nécessité et de la proportionnalité des données traitées[18]. En France, la CNIL a par exemple refusé que des empreintes digitales soient utilisées pour contrôler l'accès d'enfants à une cantine scolaire[19] , mais a accepté pour cette même finalité le recours à la morphologie de la main. Au Portugal, l'autorité chargée de la protection des données vient de prendre une décision défavorable à l'utilisation d'un système biométrique (empreintes digitales) par une université dans le but de contrôler l'assiduité et la ponctualité du personnel non enseignant[20]. L'autorité allemande de protection des données a rendu une décision favorable à l'introduction de caractéristiques biométriques dans les documents d'identité afin d'empêcher la falsification de ceux-ci, à condition que les données soient conservées dans la micropuce de la carte, et non dans une base de données, en vue de la comparaison avec les empreintes digitales du propriétaire.

Une difficulté particulière peut résulter du fait que les données biométriques contiennent souvent davantage d'informations que ne nécessitent les fonctions d'identification ou d'authentification. Cela risque surtout d'être le cas pour l'image originale (données brutes) parce que, du point de vue technique, le modèle peut et doit être construit de manière à exclure le traitement de données qui ne sont pas nécessaires. Les données non nécessaires doivent être détruites dès que possible[21]. En outre, certaines données biométriques peuvent révéler l'origine raciale ou concerner l'état de santé (voir plus loin, point 3.7).

---

[18] En outre, l'anonymat ou l'utilisation de pseudonymes doivent rester possibles dans certaines circonstances. Les mécanismes prévus pour remédier aux problèmes découlant de la perte, du vol ou de la détérioration des cartes doivent être pris en compte dans ce contexte. Les mécanismes n'entraînant pas le stockage de données biométriques doivent être favorisés. Dans toute la mesure du possible, les données devraient être recueillies à nouveau directement auprès de la personne concernée.

[19] Il semble cependant qu'au Royaume-Uni, l'autorité de protection des données ait accepté l'utilisation des empreintes digitales dans un cas similaire où des garanties appropriées avaient été mises en place.

[20] L'autorité portugaise de protection des données était d'avis que le recours à de tels systèmes était disproportionné et excessif au regard de la finalité du traitement des données. Le système devait stocker ces données dans un dispositif biométrique et le nombre des personnes à contrôler était d'environ 140.

[21] Cette suppression est également justifiée par le fait que l'article 6, paragraphe 1, point e), de la directive 95/46/CE dispose que les données à caractère personnel ne sont conservées que pendant une durée *n'excédant pas* celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées.

Enfin, il importe de noter que l'utilisation de systèmes biométriques pourrait être conçue de telle manière qu'on pourrait y voir une technologie améliorant la protection de la vie privée, entre autres en raison d'un moindre recours au traitement d'autres données à caractère personnel, telles que le nom, l'adresse, la résidence, etc.

3.4. Collecte loyale et information de la personne concernée

Le traitement de données biométriques, et en particulier leur collecte, doivent se faire de manière loyale.[22] Le responsable du traitement des données doit informer la personne concernée conformément aux articles 10 et 11 de la directive 95/46/CE[23]. Cette information comprend en particulier la définition exacte de la finalité et l'identité du responsable du fichier (qui sera souvent la personne gérant le système biométrique ou appliquant la technique biométrique).

Les systèmes qui collectent des données biométriques à l'insu des personnes concernées doivent être proscrits. Certains systèmes biométriques, tels que la reconnaissance faciale à distance, la collecte d'empreintes digitales ou l'enregistrement de la voix, présentent davantage de risques à cet égard.

3.4. Critères de légitimation du traitement de données

Le traitement de données biométriques doit être fondé sur l'un des motifs de légitimité prévus à l'article 7 de la directive 95/46/CE. Le groupe de travail souligne que, si le consentement est utilisé comme motif de légitimité par le responsable du fichier, ce consentement doit respecter les conditions fixées à l'article 2 de la directive 95/46/CE (toute manifestation de volonté, libre, spécifique et informée, par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement).

3.5. Contrôle préalable – notification

Comme il a été indiqué plus haut, le groupe de travail est favorable à l'utilisation de systèmes biométriques qui ne mémorisent pas de traces dans des terminaux d'accès ou dans une base de données centrale (voir point 3.2.). Mais s'il est prévu d'utiliser de tels systèmes, et compte tenu du risque d'une (ré)utilisation des données pour des finalités différentes, ainsi que des risques spécifiques inhérents à un accès non autorisé, le groupe de travail recommande que les États membres envisagent de les soumettre au contrôle préalable des autorités chargées de la protection des données conformément à l'article 20 de la directive 95/46/CE, car un tel traitement des données présentera probablement des risques particuliers pour les droits et libertés des personnes concernées. Si les États membres ont l'intention d'instaurer un contrôle préalable en relation avec le traitement de données biométriques, il importe que les autorités nationales chargées de la protection des données soient valablement consultées avant la mise en place de mesures de cette nature.

---

[22] Article 6, paragraphe 1, point a), de la directive 95/46/CE.

[23] Les exemptions de l'obligation d'informer les personnes concernées, prévue aux articles 10 et 11 de la directive 95/46/CE, devraient être fondées sur des mesures législatives et constituer une mesure nécessaire pour réduire la portée de l'obligation d'information en vue de sauvegarder les intérêts énumérés à l'article 13 de la directive 95/46/CE (sécurité publique, prévention, recherche, détection et poursuite d'infractions pénales, etc.).

3.6. Mesures de sécurité

Conformément à l'article 17 de la directive 95/46/CE, le responsable du traitement doit prendre toutes les mesures de sécurité techniques et organisationnelles appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite ou la perte accidentelle, la modification, l'accès ou la communication non autorisés, notamment si le traitement des données biométriques implique leur transmission par un réseau. Des mesures de sécurité doivent être prises lorsque des données biométriques font l'objet d'un traitement (conservation, transmission, extraction de certaines caractéristiques et comparaison, etc.), et en particulier lorsqu'elles sont transmises par le responsable via Internet. Les mesures de sécurité pourraient inclure le cryptage des modèles et un système de protection des clés de cryptage, venant s'ajouter au contrôle d'accès et à la protection, et rendant pratiquement impossible la reconstitution des données originales à partir de ces modèles.

Dans ce contexte, il y a lieu de tenir compte de certaines technologies nouvelles. La possibilité d'utiliser des données biométriques comme clés de cryptage constitue une évolution intéressante. Une telle solution engendrerait a priori moins de risques pour la personne concernée car le décodage ne pourrait se faire que sur la base d'une nouvelle collecte de données biométriques auprès de l'intéressé lui-même, ce qui éviterait la création de bases de données contenant des modèles de données biométriques susceptibles d'être réutilisés à des fins tout à fait différentes.

Il y a lieu de prendre les mesures de sécurité requises dès le début du traitement des données, en particulier durant la phase d'"inscription" au cours de laquelle les données biométriques sont transformées en modèles ou en images. Il importe de comprendre que, si les bases de données devaient perdre leurs qualités d'intégrité, de confidentialité et de disponibilité, cela pénaliserait manifestement toutes les applications futures basées sur les informations contenues dans ces bases de données et infligerait un préjudice irréversible aux personnes concernées. Si, par exemple, les empreintes digitales d'une personne autorisée étaient associées avec l'identité d'une personne non autorisée, cette dernière pourrait accéder indûment aux services réservés au propriétaire des empreintes. Il en résulterait un vol d'identité qui, détecté ou non, rendrait les empreintes digitales de la personne non fiables pour des applications ultérieures et limiterait ainsi la liberté de cette personne.

Les erreurs qui se produisent à l'intérieur de systèmes biométriques peuvent avoir des conséquences graves pour la personne concernée, en particulier lorsqu'il s'agit du rejet erroné de personnes autorisées et de l'acceptation indue de personnes non autorisées, qui peuvent être à l'origine de problèmes sérieux à plusieurs niveaux différents. A priori, l'utilisation de données biométriques devrait réduire le risque de telles erreurs, mais elle pourrait également donner l'illusion que l'identification ou l'authentification/vérification de la personne concernée est toujours correcte. Il peut être difficile, voire impossible pour la personne concernée d'apporter la preuve du contraire. Ainsi, un système pourrait identifier erronément une personne comme quelqu'un qui ne doit pas être autorisé à monter à bord d'un avion ou à entrer dans un pays donné, et cette personne n'aura guère la possibilité de résoudre le problème lorsqu'une telle preuve "incontestable" lui sera opposée. Il convient de souligner à nouveau que, quand des cas pareils se produisent, toute décision produisant des effets juridiques à l'égard d'une personne ne doit être prise qu'après vérification du résultat du traitement automatisé, conformément à l'article 15 de la directive 95/46/CE.

Enfin, il convient de noter que l'utilisation de la biométrie pourrait améliorer les procédures de contrôle dans le cas de l'accès à des données à caractère personnel concernant des tiers, par exemple en cas de vol ou d'utilisation abusive (procédures d'autorisation).

3.7. Données sensibles

Certaines données biométriques pourraient être considérées comme sensibles au sens de l'article 8 de la directive 95/46/CE, notamment celles qui révèlent l'origine raciale ou ethnique ou encore les données relatives à la santé. Dans les systèmes biométriques reposant sur la reconnaissance faciale, par exemple, il est possible de traiter des données révélant l'origine raciale ou ethnique. Dans ces cas-là, les garanties spéciales prévues à l'article 8 seront applicables en plus des principes généraux de protection énoncés par la directive.

Cela ne signifie pas que tout traitement de données biométriques couvrira nécessairement des données sensibles. Dire si un traitement englobe des données sensibles est une question d'appréciation liée à la caractéristique biométrique spécifique qui est utilisée et à l'application biométrique elle-même. Cela risque davantage d'être le cas lorsque l'on traite des données biométriques sous forme d'images, puisque les données brutes ne peuvent en principe pas être reconstituées à partir du modèle.

3.8. Identifiant unique

Les données biométriques sont uniques et la plupart d'entre elles génèrent un modèle (ou une image) unique. Dans le cas d'une large utilisation, en particulier pour une partie importante de la population, elles peuvent être considérées comme un identifiant de portée générale au sens de la directive 95/46/CE. L'article 8, paragraphe 7, de cette directive serait alors applicable et les États membres devraient déterminer les conditions de leur traitement.

Quand des données biométriques doivent être utilisées comme une clé permettant de mettre en relation des bases de données contenant des données à caractère personnel[24], des problèmes particulièrement délicats peuvent se poser si la personne concernée n'a aucune possibilité de s'opposer au traitement de données biométriques, comme cela peut arriver fréquemment dans les rapports entre les citoyens et les autorités publiques.

De ce point de vue, il serait souhaitable que les modèles et leurs représentations numériques soient traités à l'aide de manipulations mathématiques (cryptage, algorithmes ou fonctions de hachage) faisant appel à des paramètres différents pour chaque produit biométrique utilisé, afin d'éviter la combinaison de données à caractère personnel provenant de plusieurs bases de données, grâce à la comparaison de modèles ou de représentations numériques

3.9. Code de conduite et utilisation des technologies renforçant la protection de la vie privée

Le groupe de travail encourage le secteur à développer des systèmes biométriques qui facilitent la mise en œuvre des recommandations contenues dans le présent document de travail et, si des normes européennes ou internationales devaient être élaborées dans ce

[24] Voir également plus haut, point 3.2 concernant les réutilisations compatibles.

domaine, elles devraient l'être en coordination avec les autorités chargées de la protection des données, afin que soient favorisés des systèmes biométriques dont la conception respecte la protection des données, qui minimisent les risques sociaux et qui préviennent l'emploi abusif de données biométriques. Le groupe de travail souligne l'importance, dans ce contexte, des technologies renforçant la protection de la vie privée (PETS = Privacy Enhancing Technologies) afin de réduire la collecte de données et de prévenir le traitement illicite.

En outre, le groupe de travail insiste sur l'importance des codes de conduite qui devraient contribuer, en fonction de la spécificité des divers secteurs, à la bonne application des principes de la protection des données, conformément à l'article 27 de la directive 95/46/CE. Des codes communautaires peuvent être soumis au groupe de travail qui déterminera, entre autres, si les projets qui lui sont présentés sont conformes aux dispositions nationales relatives à la protection des données, adoptées conformément à la directive 95/46/CE.

CONCLUSIONS

Le groupe de travail estime que la plupart des systèmes biométriques impliquent le traitement de données à caractère personnel. Il est donc nécessaire de les développer en tenant pleinement compte des principes de protection des données énoncés dans la directive 95/46/CE, et notamment de la capacité de collecter des données biométriques à l'insu de la personne concernée et de la quasi-certitude du lien avec ladite personne.

Le respect du principe de proportionnalité, qui constitue l'élément central de la protection garantie par la directive 95/46/CE, implique, tout particulièrement dans le contexte de l'authentification/vérification, qu'une préférence claire soit accordée aux applications biométriques qui ne traitent pas de données obtenues à partir de traces physiques laissées par des personnes à leur insu, ni des données qui ne sont pas stockées dans un système centralisé. Cela permet aux personnes concernées d'avoir un meilleur contrôle sur le traitement des données à caractère personnel les concernant.

Le groupe de travail a l'intention de revoir le présent document de travail à la lumière de l'expérience des autorités chargées de la protection des données, ainsi que des développements technologiques dans le domaine des applications biométriques. Comme des données biométriques sont utilisées dès à présent en vue d'une large gamme d'utilisations dans divers domaines, d'autres travaux devront être entrepris sans tarder, notamment en ce qui concerne l'emploi, les visas, l'immigration et la sécurité des transports.

Si le secteur doit garder la responsabilité d'élaborer des systèmes biométriques conformes aux principes de protection des données, il serait extrêmement utile, à tout point de vue, qu'un dialogue efficace, reposant en particulier sur un projet de code de conduite, soit instauré entre toutes les parties intéressées, y compris les autorités chargées de la protection des données.

Fait à Bruxelles, le 13 juin 2003

Pour le groupe de travail
Le président
Stefano RODOTÀ