GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

00720/12/FR

WP193

Avis 3/2012 sur l'évolution des technologies biométriques

Adopté le 27 avril 2012

Note de synthèse

Les systèmes biométriques sont étroitement liés à une personne car ils peuvent utiliser un trait unique propre à une personne à des fins d'identification ou d'authentification. Si les données biométriques d'une personne peuvent être supprimées ou modifiées, ce n'est généralement pas le cas de la source dont elles proviennent.

Utilisées efficacement et avec succès dans la recherche scientifique, les données biométriques sont essentielles à la science médico-légale et sont un élément précieux des systèmes de contrôle d'accès. Elles peuvent contribuer à augmenter le niveau de sécurité, à faciliter et accélérer les procédures d'identification et d'authentification et à les rendre opportunes. Auparavant, l'utilisation de cette technologie était onéreuse et, partant, avait un impact limité sur les droits des personnes à la protection de leurs données. Au cours des dernières années, cette situation a radicalement changé. L'analyse d'ADN est devenue plus rapide et accessible à presque tout le monde. Grâce aux progrès technologiques, la puissance des ordinateurs et l'espace de stockage coûtent moins cher, ce qui a permis l'apparition d'albums de photos en ligne et de milliards de photographies sur les réseaux sociaux. Les lecteurs d'empreintes digitales et les dispositifs de vidéosurveillance sont devenus des gadgets peu onéreux. Le développement de ces technologies a facilité nombre d'opérations, contribué à résoudre de nombreux crimes et augmenté la fiabilité des systèmes de contrôle d'accès, mais il a également créé de nouvelles menaces pour les droits fondamentaux. La discrimination génétique est devenue un véritable problème. Le vol d'identité n'est plus une menace théorique.

Si d'autres nouvelles technologies qui ciblent de grands groupes de population et qui ont récemment soulevé des inquiétudes en matière de protection des données ne se concentrent pas nécessairement sur l'établissement d'un lien direct avec une personne en particulier, ou si la création de ce lien requiert des efforts considérables, les données biométriques sont, en soi, directement reliées à une personne. Ce n'est pas toujours un avantage, cela implique même plusieurs inconvénients. Par exemple, équiper les systèmes de vidéosurveillance et les téléphones intelligents de systèmes de reconnaissance faciale utilisant les bases de données de réseaux sociaux pourrait mettre un terme à l'anonymat et aux mouvements non tracés des personnes. Par ailleurs, les lecteurs d'empreintes digitales, les lecteurs de réseau veineux ou simplement un sourire à une caméra pourraient remplacer les cartes, codes, mots de passe et signatures.

Le présent avis aborde ces questions et d'autres événements récents pour sensibiliser les personnes concernées et les organes législatifs. Ces innovations techniques, qui sont très souvent présentées comme des technologies qui ne font qu'améliorer l'expérience de l'utilisateur et le côté pratique des applications, pourraient entraîner une perte progressive de la vie privée si des mesures de protection adéquates ne sont pas mises en œuvre. En conséquence, le présent avis recense les mesures techniques et organisationnelles qui visent à atténuer les risques en matière de vie privée et de protection de données et qui peuvent contribuer à prévenir les répercussions négatives sur la vie privée des citoyens européens et sur le droit fondamental de ces derniers à la protection des données à caractère personnel.

LE GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

institué en vertu de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995,

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

vu son règlement intérieur,

ADOPTE LE PRÉSENT AVIS

1. Champ d'application de l'avis

Dans le document de travail sur la biométrie de 2003 (WP80), le groupe de travail «article 29» (ci-après le «groupe de travail») s'est penché sur les questions de protection des données liées à l'utilisation des nouvelles technologies qui permettaient de lire et de traiter les données biométriques par voie électronique. Au cours des dernières années, l'utilisation de ces technologies s'est généralisée dans les secteurs public et privé et plusieurs nouveaux services ont été mis en place. Les technologies biométriques qui nécessitaient auparavant d'importantes ressources financières ou informatiques sont devenues bien plus rapides et moins onéreuses. L'utilisation de lecteurs d'empreintes digitales est aujourd'hui monnaie courante. Par exemple, certains ordinateurs portables sont dotés d'un lecteur d'empreintes digitales pour le contrôle d'accès biométrique. Grâce aux progrès dans l'analyse de l'ADN, il est à présent possible d'obtenir les résultats en quelques minutes. Certaines des technologies récemment développées, comme la reconnaissance du réseau veineux ou la reconnaissance faciale, sont déjà au point. Elles ne tarderont pas à être utilisées dans différentes applications de notre vie quotidienne. Les technologies biométriques sont étroitement liées à certains traits d'une personne, dont certains peuvent être utilisés pour révéler des données sensibles. Par ailleurs, bon nombre d'entre elles permettent le pistage, le suivi ou le profilage automatisés de personnes et, partant, peuvent avoir un impact considérable sur la vie privée et le droit des personnes à la protection des données. Cet impact augmente à mesure que ces technologies se développent. Chaque personne est susceptible d'être enregistrée dans un ou plusieurs systèmes biométriques.

Cet avis a pour but de fournir un cadre révisé et actualisé pour des directives et des recommandations générales unifiées sur la mise en œuvre des principes de protection des données et de la vie privée dans des applications biométriques. Il s'adresse aux autorités législatives nationales et européennes, à l'industrie des systèmes biométriques et aux utilisateurs de ces technologies.

2. Définitions

Les technologies biométriques ne sont pas nouvelles et elles ont déjà été abordées dans différents avis du groupe de travail. La présente section cherche à compiler les définitions pertinentes et à fournir une mise à jour chaque fois que nécessaire.

Données biométriques. Aux termes utilisés par le groupe de travail dans l'avis 4/2007 (WP136), les données biométriques peuvent se définir comme:

> *«des propriétés biologiques, des aspects comportementaux, des caractéristiques physiologiques, des caractéristiques vivantes ou des actions reproductibles lorsque ces caractéristiques et/ou actions sont à la fois propres à cette personne physique et mesurables, même si les méthodes utilisées dans la pratique pour les mesurer techniquement impliquent un certain degré de probabilité».*

Les données biométriques changent de manière irrévocable la relation entre le corps et l'identité car elles rendent les caractéristiques physiques «lisibles par une machine» et sujettes à une utilisation ultérieure.

Les données biométriques peuvent être stockées et traitées de plusieurs manières. Les informations biométriques d'une personne sont parfois stockées et traitées à l'état brut, permettant la reconnaissance de leur source sans nécessité d'avoir des connaissances particulières, par ex., la photographie d'un visage, la photographie d'une empreinte digitale ou l'enregistrement de la voix. Dans d'autres cas, les informations biométriques brutes sont traitées de sorte que seuls certains traits ou caractéristiques sont extraits et conservés sous forme de modèle biométrique.

Source de données biométriques. Les données biométriques peuvent provenir de différentes sources, qui couvrent les caractéristiques physiques, physiologiques, comportementales ou psychologiques d'une personne. Selon l'avis 4/2007 (WP136):

> *«les sources de données biométriques (comme les prélèvements de tissus humains), bien que n'étant pas des données biométriques en soi, sont des sources d'informations dont on peut extraire des données biométriques».*

Comme le précise le document WP80, on peut distinguer deux catégories principales de techniques biométriques:

- [e]n 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, l'analyse des pores de la peau, etc.;
- [e]n 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, la manière de marcher ou de se mouvoir, des modèles indiquant une certaine pensée subconsciente comme le mensonge, etc.

Une nouvelle série de techniques basées sur la **psychologie** doit également être prise en considération. Elle englobe l'évaluation de la réaction à des situations concrètes ou à des tests spécifiques pour correspondre à un profil psychologique.

Modèle biométrique. Les principales caractéristiques peuvent être extraites de données biométriques brutes (par ex., mesures du visage à partir d'une image) et stockées pour un traitement ultérieur plutôt que les données brutes elles-mêmes. Ils constituent le modèle biométrique des données. Il est crucial de déterminer la taille (la quantité d'informations) du modèle. D'un côté, le modèle doit être suffisamment grand pour assurer la sécurité (éviter les

chevauchements entre différentes données biométriques ou les substitutions d'identité); de l'autre, le modèle ne doit pas être trop grand afin d'éviter les risques de reconstitution des données biométriques. La production du modèle doit être un processus unidirectionnel, de sorte qu'il ne devrait pas être possible de reconstituer les données biométriques brutes à partir du modèle.

Systèmes biométriques. Selon le document WP80, les systèmes biométriques sont:

> *«des applications de technologies biométriques, qui permettent l'identification et/ou l'authentification/vérification automatiques d'une personne. 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».*

Du fait des récents progrès technologiques, il est à présent possible d'utiliser les systèmes biométriques pour la catégorisation/ségrégation.

Les risques que posent les systèmes biométriques découlent de la nature même des données biométriques utilisées lors du traitement. En conséquence, une définition plus générale parlerait d'un système qui extrait des données biométriques et les traite ultérieurement.

Le traitement des données biométriques dans un système biométrique implique en général différents processus comme l'inscription, le stockage et l'établissement de correspondances.

- L'inscription de données biométriques englobe tous les processus qui se déroulent au sein d'un système biométrique afin d'extraire les données biométriques d'une source biométrique et de relier ces données à une personne. La quantité et la qualité des données nécessaires durant la phase d'inscription doivent être suffisantes pour permettre une identification, une authentification, une catégorisation ou une vérification précises sans enregistrer trop de données. Le volume de données extraites d'une source biométrique au cours de la phase d'inscription doit être suffisant pour permettre le traitement et le niveau de résultats du système biométrique.

La phase d'inscription est généralement le premier contact qu'une personne peut avoir avec un système biométrique spécifique. Dans la plupart des cas, l'inscription requiert la participation directe de la personne (par ex., dans le cas de la prise d'empreintes digitales) et peut donc être une occasion appropriée de fournir des informations et une notification de traitement loyal. Il est également possible d'inscrire des personnes sans leur consentement ou à leur insu (par ex., systèmes de CCTV dotés d'une fonction de reconnaissance du visage). La précision et la sécurité du processus d'inscription sont essentielles au fonctionnement de l'ensemble du système. Une personne peut se réinscrire dans un système biométrique pour actualiser les données biométriques enregistrées.

- Le stockage des données biométriques: les données recueillies au cours de la phase d'inscription peuvent être stockées localement dans le centre d'opération où l'inscription a eu lieu (par ex., dans un lecteur) pour une utilisation ultérieure ou sur un dispositif porté par une personne (par ex., sur une carte à puce) ou elles peuvent être envoyées ou stockées dans une base de données centralisée accessible par un ou plusieurs systèmes biométriques.

- L'établissement de correspondances biométriques est le processus consiste à comparer des données/modèles biométriques (entrés pendant la phase d'inscription)

avec les données/modèles biométriques collectés à partir d'un nouvel échantillon à des fins d'identification, de vérification/authentification ou de catégorisation.

Identification biométrique. L'identification d'une personne par le biais d'un système biométrique consiste généralement à comparer les données biométriques d'une personne (acquises au moment de l'identification) avec plusieurs modèles biométriques stockés dans une base de données (autrement dit, un processus de comparaison «un-à-plusieurs»).

Vérification/authentification biométrique. La vérification d'une personne par un système biométrique consiste généralement à comparer les données biométriques d'une personne (acquises au moment de la vérification) et un modèle biométrique unique stocké dans un dispositif (autrement dit, un processus de comparaison «un-à-un»).

Catégorisation/ségrégation biométrique. La catégorisation/ségrégation d'une personne par un système biométrique consiste généralement à établir si les données biométriques d'une personne appartiennent à un groupe qui présente certaines caractéristiques prédéfinies en vue de prendre des mesures spécifiques. Dans ce cas, l'important n'est pas l'identification ou la vérification d'une personne, mais son inscription automatique dans une certaine catégorie. Par exemple, un panneau publicitaire peut afficher différentes annonces selon la personne qui le regarde, en fonction de l'âge ou du sexe de cette dernière.

Biométrie multimodale. Elle peut se définir comme l'association de différentes technologies biométriques en vue d'améliorer la précision ou les résultats du système (elle est également appelée «biométrie multiniveaux»). Les systèmes biométriques utilisent au moins deux traits/modalités biométriques de la même personne lors du processus d'établissement de correspondances. Ces systèmes peuvent travailler de différentes manières, soit en collectant différentes données biométriques avec différents capteurs soit en collectant plusieurs unités des mêmes données biométriques. Certaines études englobent également dans cette catégorie les systèmes qui procèdent à plusieurs lectures des mêmes données biométriques et les systèmes qui utilisent plusieurs algorithmes pour l'extraction de traits du même échantillon biométrique. Parmi les systèmes biométriques multimodaux, on retrouve le passeport électronique au niveau de l'UE ainsi que le système d'identification biométrique US-VISIT aux États-Unis.

Précision: lorsque des systèmes biométriques sont utilisés, il est difficile d'obtenir des résultats 100 % exempts d'erreur. La raison est peut-être à chercher dans des différences d'environnement lors de l'acquisition de données (éclairage, température, etc.) et dans des différences dans le matériel utilisé (caméras, scanners, etc.). Les paramètres d'évaluation des performances les plus souvent utilisés sont le taux de fausses acceptations (TFA) et le taux de faux rejets (TFR), qui peuvent être adaptés en fonction du système utilisé:

- le taux de fausses acceptations (TFA) est la probabilité qu'un système biométrique identifie de manière incorrecte une personne ou ne réussisse pas à rejeter un imposteur. Il mesure le pourcentage d'intrants non valides qui sont acceptés à tort. Il est également connu sous le nom de «taux de faux positifs»;

- le taux de faux rejets (TFR) est la probabilité qu'un système produise un faux rejet. Un faut rejet se produit lorsqu'aucune correspondance n'est établie entre une personne et son modèle biométrique. Il est également connu sous le nom de «taux de faux négatifs».

Avec un réglage correct du système et un bon ajustement de la configuration, les erreurs critiques des systèmes biométriques peuvent être minimisées au niveau permis pour l'utilisation opérationnelle en réduisant les risques d'évaluation incorrecte. Un système parfait présentera un TFA et un TFR de zéro, mais ces taux ont le plus souvent une corrélation négative. L'augmentation du TFA réduit souvent le niveau du TFR.

Il importe d'évaluer la finalité du traitement, le TFA et le TFR ainsi que la taille de la population au moment de déterminer si la précision d'un système biométrique particulier est acceptable ou non. Par ailleurs, l'évaluation de la précision d'un système biométrique peut également tenir compte de la capacité à détecter un échantillon vivant. Par exemple, les empreintes digitales latentes peuvent être copiées et utilisées pour créer des faux doigts. Un lecteur d'empreintes digitales ne doit pas être mystifié et donner une identification positive dans ce type de situation.

3. Analyse juridique

Le cadre juridique applicable est la directive relative à la protection des données (95/46/CE). Le groupe de travail a déjà déclaré dans le document WP80 que les données biométriques sont, dans la plupart des cas, des données à caractère personnel. Par conséquent, elles ne peuvent être traitées que s'il existe une base juridique et si le traitement est adéquat, pertinent et non excessif au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement.

Finalité

Une condition préalable à l'utilisation des données biométriques est une définition claire de la finalité pour laquelle les informations biométriques sont collectées et traitées, qui tient compte des risques en matière de protection des libertés et droits fondamentaux de la personne.

Les données biométriques peuvent par exemple être collectées pour garantir ou augmenter la sécurité de systèmes de traitement par la mise en place de procédures appropriées pour protéger les données à caractère personnel d'un accès non autorisé. En principe, rien n'empêche les responsables du traitement d'appliquer des mesures de sécurité appropriées fondées sur des traits biométriques afin de garantir un niveau de sécurité approprié par rapport aux risques que posent le traitement et la nature des données à caractère personnel à protéger. Il convient toutefois de se rappeler que l'utilisation de la biométrie ne garantit pas en soi une sécurité accrue, car de nombreuses données biométriques peuvent être recueillies à l'insu du sujet concerné. Plus le niveau de sécurité envisagé est élevé, moins les données biométriques pourront atteindre seules cet objectif.

Le principe de finalité doit être respecté, à l'instar des autres principes de protection des données, en particulier les principes de proportionnalité, de nécessité et de minimisation des données, qu'il faut garder à l'esprit lors de la définition des différentes finalités d'une application. Chaque fois que possible, le sujet doit avoir le choix entre les finalités que propose une application aux multiples fonctions, en particulier si l'une ou plusieurs d'entre elles requièrent le traitement de données biométriques.

Exemple
L'utilisation de dispositifs électroniques offrant des procédures d'authentification spécifiques basées sur des données biométriques a été recommandée en rapport avec des mesures de sécurité à prendre en cas:

- de traitement de données à caractère personnel collectées par des opérateurs téléphoniques au cours d'activités d'écoute téléphonique autorisées par un tribunal;
- d'accès à des données relatives au trafic (et à la localisation) conservées à des fins judiciaires par les fournisseurs de services de communications électroniques disponibles publiquement ou des réseaux de communications publiques et d'accès aux locaux connexes où ces données sont traitées;
- de collecte et de stockage de données génétiques et d'échantillons biologiques.

Les **photographies** sur l'internet, sur des réseaux sociaux et dans des applications de gestion ou de partage de photos en ligne ne peuvent être traitées ultérieurement afin d'extraire des modèles biométriques ou de les inscrire dans un système biométrique pour reconnaître automatiquement les personnes sur les photos (reconnaissance faciale) sans base juridique spécifique (par ex., consentement) pour cette nouvelle finalité. Si cette finalité secondaire a une base juridique, le traitement doit également être adéquat, pertinent et non excessif au regard de cette finalité. Si le sujet a accepté que les photographies où il apparaît puissent être traitées pour l'étiqueter automatiquement dans un album de photos en ligne par un algorithme de reconnaissance faciale, ce traitement doit être réalisé dans le respect de la protection des données: les données biométriques qui ne sont plus nécessaires après l'étiquetage des photographies avec le nom, le surnom ou tout autre texte spécifié par le sujet doivent être supprimées. La création d'une base de données biométriques permanente n'est a priori pas nécessaire à cette fin.

Proportionnalité

L'utilisation de la biométrie soulève la question de la proportionnalité de chaque catégorie de données traitées au regard de la finalité pour laquelle elles sont traitées. Le fait que les données biométriques ne peuvent être utilisées que si elles sont adéquates, pertinentes et non excessives invite à évaluer rigoureusement la nécessité et la proportionnalité des données traitées et à établir si la finalité poursuivie ne pourrait pas être atteinte d'une façon moins intrusive.

Il convient de prendre plusieurs éléments en considération lors de l'analyse de la proportionnalité d'un système biométrique proposé. Le premier consiste à déterminer si le système est nécessaire pour répondre au besoin identifié, autrement dit s'il est essentiel pour satisfaire ce besoin plutôt que d'être le plus commode ou rentable. Il faut également savoir si le système est susceptible de répondre à ce besoin eu égard aux caractéristiques spécifiques de la technologie biométrique qu'il est prévu d'utiliser[1]. Un troisième aspect en prendre en considération est de savoir si la perte de vie privée qui en résulte est proportionnelle à tout avantage prévu. Si l'avantage est relativement mineur, comme une commodité accrue ou une

[1] La biométrie sera utilisée pour la vérification ou l'identification: un identifiant biométrique pourrait être jugé techniquement approprié pour l'une et pas pour l'autre (par exemple, les technologies caractérisées par de faibles taux de faux rejets doivent être préférées dans des systèmes destinés à l'identification dans le domaine de l'application des lois).

légère économie de coût, la perte de la vie privée n'est pas appropriée. Enfin, il faut étudier si des moyens moins intrusifs dans la vie privée pourraient atteindre la finalité souhaitée[2].

Exemple
Dans un club de santé et de remise en forme, un système biométrique centralisé basé sur la prise d'empreintes digitales est installé pour permettre l'accès aux locaux et aux services connexes uniquement aux clients qui ont payé leur droit d'entrée.
Pour qu'un tel système fonctionne, il faut stocker les empreintes digitales de tous les clients et de tous les employés. Cette application biométrique semble disproportionnée par rapport à la nécessité de contrôler l'accès au club et de faciliter la gestion des abonnements. On peut facilement imaginer que d'autres mesures, comme une simple liste de contrôle ou l'utilisation d'une étiquette RFID ou d'une carte magnétique, qui ne nécessitent pas le traitement de données biométriques, peuvent être tout aussi pratiques et efficaces.

Le groupe de travail avertit des risques liés à l'utilisation des données biométriques à des fins d'identification dans de grandes bases de données centralisées, vu les conséquences potentiellement dangereuses pour les personnes concernées.

Il faut tenir compte de l'énorme impact sur la dignité humaine des personnes concernées ainsi que des implications de ces systèmes en matière de droits fondamentaux. À la lumière de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et de la jurisprudence de la Cour européenne des droits de l'homme sur l'article 8 de la Convention, le groupe de travail insiste sur le fait qu'il ne faut permettre d'interférence avec le droit à la protection des données qu'à condition qu'elle soit conforme à la loi, et sur le fait qu'il est nécessaire, dans une société démocratique, de protéger un intérêt public majeur[3].

Veiller au respect de ces conditions exige de spécifier la finalité que poursuit le système et d'évaluer la proportionnalité des données à entrer dans le système par rapport à ladite finalité.

À cet effet, le responsable du traitement doit établir si le traitement et ses mécanismes, les catégories des données à collecter et à traiter ainsi que le transfert des informations contenues dans la base de données, sont nécessaires et indispensables. Les mesures de sécurité adoptées doivent être adéquates et efficaces. Le responsable du traitement doit tenir compte des droits à accorder aux sujets auxquels se rapportent les données à caractère personnel et veiller à ce qu'un mécanisme adéquat pour l'exercice de ces droits soit intégré à l'application.

[2] Par exemple, les cartes à puce ou d'autres méthodes qui ne collectent ni ne centralisent d'informations biométriques à des fins d'authentification.

[3] Voir l'arrêt de la Cour européenne de justice du 20 mai 2003 dans les affaires jointes C-465/00, C-138/01 et C-139/01 (Rechnungshof c. Österreichischer Rundfunk et autres), l'arrêt de la Cour européenne des droits de l'homme du 4 décembre 2008 dans l'affaire S. et Marper c. Royaume-Uni (requêtes n° 30562/04 et 30566/04) et l'arrêt de la Cour européenne des droits de l'homme du 19 juillet 2011 dans l'affaire Goggins et autres c. Royaume-Uni (requêtes n° 30089/04, 14449/06, 24968/07, 13870/08, 36363/08, 23499/09, 43852/09 et 64027/09).

Exemple
L'utilisation de données biométriques à des fins d'identification. Les systèmes qui analysent le visage ou l'ADN d'une personne peuvent apporter une contribution très efficace à la lutte contre la criminalité et révéler avec précision l'identité d'une personne inconnue suspectée d'un crime grave. Toutefois, utilisés à grande échelle, ces systèmes ont d'importants effets secondaires. Dans le cas de la reconnaissance faciale, où les données biométriques peuvent facilement être capturées à l'insu du sujet, une utilisation généralisée mettrait un terme à l'anonymat dans les lieux publics et permettrait de suivre des personnes en permanence. Dans le cas des données d'ADN, l'utilisation de la technologie présente le risque que des données sensibles relatives à la santé du sujet soient révélées.

Précision

Les données biométriques traitées doivent être précises et pertinentes par rapport à la finalité pour laquelle elles ont été collectées. Les données doivent être précises au moment de l'inscription et de la comparaison de la personne concernée et des données biométriques. La précision lors de l'inscription est également pertinente pour prévenir l'usurpation d'identité.

Les données biométriques sont uniques et génèrent, pour la plupart, un modèle ou une image unique. Si elles sont utilisées à grande échelle, en particulier sur une grande partie de la population, les données biométriques peuvent être considérées comme un identifiant de portée générale au sens de la directive 95/46/CE. L'article 8, paragraphe 7, de la directive 95/46/CE serait alors applicable et les États membres devraient déterminer les conditions de leur traitement.

Minimisation des données

Le fait que les données biométriques contiennent souvent plus d'informations que celles qui sont nécessaires pour établir des correspondances peut poser un problème spécifique. Le responsable du traitement doit appliquer le principe de minimisation des données. Tout d'abord, cela signifie que seules les informations nécessaires, et non toutes les informations disponibles, doivent être traitées, transmises ou stockées. Ensuite, le responsable du traitement doit garantir que la configuration par défaut encourage la protection des données, sans devoir l'appliquer.

Période de conservation

Le responsable du traitement doit déterminer une période de conservation des données biométriques inférieure à ce qui est nécessaire pour la finalité pour laquelle les données sont collectées et traitées ultérieurement. Le responsable du traitement doit veiller à ce que les données, ou les profils obtenus à partir de ces données, soient définitivement supprimés à l'échéance de cette période légitime.

Il doit y avoir une différence claire entre les données à caractère personnel générales qui peuvent être nécessaires plus longtemps et les données biométriques qui ne sont plus utiles, par ex., lorsque le sujet n'a plus accès à une zone spécifique.

Exemple
Un employé exploite un système biométrique pour contrôler l'accès à une zone réservée. Lorsque la fonction de l'employé ne nécessite plus que ce dernier accède à cette zone (par ex., changement de responsabilité ou de poste), les données biométriques doivent être supprimées étant donné que la finalité pour laquelle elles avaient été collectées n'existe plus.

3.1. Légitimation

Le traitement de données biométriques doit se fonder sur l'un des motifs de légitimation prévus à l'article 7 de la directive 95/46/CE.

3.1.1. Consentement, article 7, paragraphe a)

Le premier motif donné à l'article 7, paragraphe a), est que la personne concernée a indubitablement donné son consentement. Selon l'article 2, paragraphe h), de la directive relative à la protection des données, le consentement est une manifestation de volonté, libre, spécifique et informée de la personne concernée. Il doit être clair que ce consentement ne peut être obtenu librement par l'acceptation obligatoire de conditions générales ou par une possibilité de ne pas utiliser le système. Le consentement doit en outre être révocable. À cet égard, dans son avis sur la définition du consentement, le groupe de travail souligne plusieurs aspects importants de la notion: la validité du consentement, le droit de la personne concernée à retirer son consentement, le consentement doit être donné avant le début du traitement, les exigences concernant la qualité et l'accessibilité des informations[4].

Souvent, lorsque des données biométriques sont traitées, sans une alternative valide comme un mot de passe ou une carte magnétique, le consentement pourrait ne pas être considéré comme librement donné. Par exemple, un système qui découragerait les personnes concernées de l'utiliser (par ex., procédure trop longue pour l'utilisateur ou trop complexe) pourrait ne pas être considéré comme une alternative valide et il n'y aurait donc pas de consentement valide.

Exemples

En l'absence d'autres motifs légitimes alternatifs, un système d'authentification biométrique pourrait être utilisé pour contrôler l'accès à un club vidéo uniquement si les clients sont libres de décider d'utiliser ou non ce système. Cela signifie que des mécanismes alternatifs, moins intrusifs dans la vie privée, doivent être proposés par le propriétaire du club vidéo. Un tel système permettra au client qui ne peut ou ne veut pas donner ses empreintes digitales pour des raisons personnelles d'exprimer son désaccord. Le seul choix entre ne pas utiliser un service et donner ses données biométriques indique fortement que le consentement n'a pas été librement donné et ne peut être considéré comme un motif légitime.

Dans une école maternelle, un dispositif de balayage du réseau veineux est installé pour contrôler tous les adultes qui y entrent (parents et membres de personnel), qu'ils soient autorisés ou non à entrer. Le stockage des empreintes digitales de tous les parents et de tous les membres du personnel serait nécessaire au fonctionnement d'un tel système. Le consentement serait une base juridique discutable en particulier pour les employés vu qu'ils n'auraient pas vraiment le choix de refuser d'utiliser un tel système. Il serait discutable pour les parents étant donné qu'il n'y a pas de méthode alternative pour entrer dans l'école.

S'il peut y avoir une forte présomption que le consentement est faible à cause du déséquilibre typique entre employeur et employé, le groupe de travail n'exclut pas complètement son utilisation, *«à condition qu'il existe des garanties suffisantes que le consentement est véritablement libre»*[5].

[4] WP187 - Avis 15/2011 sur la définition du consentement.

[5] WP187 - Avis 15/2011 sur la définition du consentement.

Partant, le consentement dans le contexte professionnel doit être discuté et dûment justifié. Au lieu de chercher à obtenir un consentement, les employeurs pourraient étudier s'il s'avère nécessaire d'utiliser les données biométriques des employés pour une finalité légitime et soupeser cette nécessité par rapport aux libertés et aux droits fondamentaux des employés. Lorsque la nécessité peut être dûment justifiée, la base juridique du traitement pourrait se fonder sur la réalisation de l'intérêt légitime poursuivi par le responsable du traitement telle qu'elle est définie à l'article 7, paragraphe f), de la directive 95/46/CE. L'employeur doit toujours rechercher le moyen le moins intrusif en choisissant, si possible, un procédé non biométrique.

Toutefois, tel que décrit dans la section 3.1.3, un système biométrique peut reposer sur les intérêts légitimes du responsable du traitement des données dans certains cas. Le consentement ne serait alors pas nécessaire.

Pour qu'un consentement soit valide, il faut que la personne concernée reçoive des informations suffisantes sur l'utilisation des données biométriques. Étant donné que les données biométriques peuvent être utilisées comme un identifiant unique et universel, il convient de considérer la fourniture d'informations claires et facilement accessibles sur la manière dont les données spécifiques sont utilisées comme une absolue nécessité pour garantir un traitement loyal. Il s'agit dès lors d'une exigence cruciale pour un consentement valide dans l'utilisation des données biométriques.

Exemples
Un consentement valide pour un système de contrôle d'accès qui utilise des empreintes digitales requiert des informations, que le système biométrique crée un modèle unique à ce système ou non. Si l'on utilise un algorithme qui crée le même modèle biométrique dans différents systèmes biométriques, la personne concernée doit savoir qu'elle pourrait être reconnue dans des systèmes biométriques différents.

Quelqu'un télécharge une photo dans un album sur l'internet. Inscrire cette photo dans un système biométrique requiert un consentement explicite basé sur des informations exhaustives sur l'utilisation des données biométriques, sur la période de conservation et la finalité pour laquelle elles sont traitées.

Étant donné que le consentement peut être retiré à tout moment, le responsable du traitement doit mettre en œuvre les moyens techniques qui peuvent inverser l'utilisation de données biométriques dans ses systèmes. Un système biométrique qui fonctionne sur la base du consentement doit donc pouvoir efficacement effacer tous les liens d'identité qu'il crée.

3.1.2. Contrat, article 7, paragraphe b)

Le traitement de données biométriques peut être nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci. Il faut cependant signaler que cela s'applique en général uniquement en cas de fourniture de services biométriques purs. Cette base juridique ne peut être utilisée pour légitimer un service secondaire qui consiste à inscrire une personne dans un système biométrique. Si un tel service ne peut être séparé du service principal, le contrat relatif au service principal ne peut légitimer le traitement de données biométriques. Les données à caractère personnel ne peuvent être demandées en échange d'un service. Partant, les contrats qui prévoient ou qui offrent un service uniquement à condition qu'une personne donne son consentement au traitement de ses données biométriques pour un autre service ne peuvent servir de base juridique à ce traitement.

Exemples
a) Deux frères envoient des échantillons de cheveux à un laboratoire pour faire un test d'ADN afin de déterminer s'ils sont réellement frères. Le contrat avec le laboratoire pour faire ce test est une base juridique suffisante pour l'inscription et le traitement des données biométriques.

b) Une personne publie une photo qu'elle veut montrer à ses amis sur un réseau social. Si le contrat (conditions du service) prévoit que l'utilisation du service est liée à l'inscription de l'utilisateur dans un système biométrique, cette disposition n'est pas une base juridique suffisante pour cette inscription.

3.1.3. Obligation légale, article 7, paragraphe c)

Un autre motif légitime pour le traitement de données à caractère personnel est le fait que le traitement soit nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis. C'est le cas par exemple dans certains pays lors de la délivrance ou de l'utilisation de passeports[6] et de visas[7].

3.1.4. Intérêt légitime du responsable du traitement, article 7, paragraphe f)

Aux termes de l'article 7 de la directive 95/46/CE, le traitement des données à caractère personnel peut également être justifié s'il est «nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée».

En d'autres termes, dans certains cas, l'utilisation de systèmes biométriques va dans l'intérêt légitime du responsable du traitement. Cet intérêt n'est toutefois légitime que lorsque le responsable du traitement peut prouver que son intérêt l'emporte objectivement sur les droits des personnes concernées à ne pas être inscrites dans un système biométrique. Par exemple, lorsque la sécurité de zones à haut risque doit être spécifiquement garantie par un mécanisme qui peut vérifier de manière précise si les personnes sont autorisées à y accéder, l'utilisation d'un système biométrique peut être nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement. Dans l'exemple ci-dessous concernant un système biométrique de contrôle d'accès à un laboratoire, le responsable du traitement ne peut proposer à l'employé un mécanisme alternatif sans avoir d'impact direct sur la sécurité de la zone d'accès réservé étant donné qu'il n'existe pas de mesure alternative moins invasive

[6] Les empreintes digitales doivent être intégrées dans les passeports conformément au règlement (UE) n° 2252/2004 du Conseil du 13 décembre 2004, et dans les titres de séjour conformément au règlement (UE) n° 1030/2002 du Conseil du 13 juin 2002.

[7] L'enregistrement d'identifiants biométriques dans le système d'information sur les visas (VIS) est instauré dans le règlement (CE) n° 767/2008 du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (règlement VIS). Voir également WP134 - Avis 3/2007 sur la proposition de règlement du Parlement européen et du Conseil modifiant les instructions consulaires communes adressées aux représentations diplomatiques et consulaires de carrière, en liaison avec l'introduction d'éléments d'identification biométriques et de dispositions relatives à l'organisation de la réception et du traitement des demandes de visa (COM(2006)269 final); WP110 - Avis 2/2005 sur la proposition de règlement du Parlement européen et du Conseil concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (COM (2004) 835 final); et WP96 - Avis 7/2004 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).

permettant d'atteindre un niveau de sécurité adéquat pour cette zone. Il est par conséquent nécessaire à la réalisation de l'intérêt légitime qu'il poursuit d'appliquer le système et d'inscrire un nombre limité d'employés. Leur consentement n'est pas nécessaire. Cependant, lorsque l'intérêt légitime poursuivi par le responsable du traitement est un motif légal valide pour le traitement, comme toujours, tous les autres principes de protection des données restent d'application, en particulier les principes de proportionnalité et de minimisation des données.

Exemple
Dans une société qui fait des recherches sur des virus dangereux, un laboratoire est sécurisé par des portes qui ne s'ouvrent que si l'employé passe avec succès la vérification de ses empreintes digitales et de son iris. Ce système a été mis en place pour s'assurer que seules les personnes qui connaissent les risques spécifiques, qui sont formées aux procédures et qui sont jugées dignes de confiance par la société puissent travailler avec ces substances dangereuses. L'intérêt légitime de la société de veiller à ce que seules les personnes y habilitées puissent entrer dans une zone d'accès limité pour garantir que les risques de sécurité qui découlent de l'accès à cette zone spécifique puissent être fortement réduits, l'emporte de loin sur le souhait des personnes concernées que leurs données biométriques ne soient pas traitées.

En règle générale, l'utilisation de la biométrie pour des exigences générales de sécurité de biens et de personnes ne peut être considérée comme un intérêt légitime qui l'emporte sur les droits et libertés fondamentaux de la personne concernée. Au contraire, le traitement de données biométriques ne peut se justifier en tant qu'outil nécessaire assurant la sécurité de biens ou de personnes, lorsqu'il existe des preuves objectives et documentées de l'existence concrète d'un risque considérable. À cet effet, le responsable du traitement doit prouver que les circonstances spécifiques posent un risque considérable concret, qu'il doit évaluer très soigneusement. Afin de respecter le principe de proportionnalité, le responsable du traitement doit, en présence d'une de ces situations à haut risque, vérifier si d'éventuelles mesures alternatives pourraient être tout aussi efficaces mais moins intrusives au regard de la finalité poursuivie, et choisir ces alternatives.

L'existence de ces circonstances doit également être régulièrement contrôlée. Sur la base des résultats de cet examen, toute opération de traitement des données qui se révèle ne plus être justifiée doit être suspendue ou arrêtée.

3.2. Responsable du traitement et sous-traitant

La directive 95/46/CE impose des obligations aux responsables du traitement concernant le traitement des données à caractère personnel. Dans le cadre de la biométrie, différents types d'organismes peuvent être responsables du traitement, par exemple les employeurs, les services répressifs et de l'immigration.

Le groupe de travail rappelle les orientations qu'il a fournies dans son avis sur les notions de responsable du traitement et de sous-traitant[8], qui contient des précisions efficaces sur la manière d'interpréter ces définitions fondamentales de la directive.

3.3. Traitement automatisé (art 15 de la directive)

Lorsqu'un système basé sur le traitement de données biométriques est utilisé, il convient de prêter une attention particulière aux éventuelles conséquences discriminatoires pour les personnes rejetées par le système. En outre, afin de protéger le droit des personnes de ne pas

[8] WP169 - Avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant».

être soumises à des mesures les affectant uniquement sur la base du traitement automatisé de données, il est nécessaire d'introduire des garanties appropriées, comme des interventions humaines, des solutions ou des mécanismes permettant à la personne concernée de faire valoir son point de vue.

Aux termes de l'article 15 de la directive 95/46/CE, *«les États membres reconnaissent à toute personne le droit de ne pas être soumise à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité, tels que son rendement professionnel, son crédit, sa fiabilité, son comportement, etc.»*.

3.4. Transparence et information de la personne concernée

Conformément au principe de traitement loyal, la personne concernée doit être informée de la collecte ou de l'utilisation de ses données biométriques (art. 6 de la directive 95/46/CE). Tout système qui collecte ces données à l'insu du sujet doit être évité.

Le responsable du traitement doit veiller à ce que la personne concernée soit correctement informée des principaux éléments du traitement conformément à l'article 10 de la directive relative à la protection des données, comme l'identité du responsable du traitement, les finalités du traitement, les catégories de données, la durée du traitement, le droit d'accès aux données la concernant et de rectification ou d'effacement de ces données, et le droit de retirer son consentement et d'être informée concernant les destinataires ou les catégories de destinataires des données auxquels les données sont communiquées. Étant donné que le responsable du traitement d'un système biométrique a l'obligation d'informer la personne concernée, les données biométriques ne peuvent être collectées à l'insu de cette dernière.

3.5. Droit d'accès aux données biométriques

La personne concernée a le droit d'obtenir du responsable du traitement un accès à ses données, y compris à ses données biométriques. Elle a également le droit d'accéder à d'éventuels profils basés sur ces données biométriques. Si le responsable du traitement doit vérifier l'identité de la personne concernée pour accorder cet accès, il est essentiel que l'accès soit octroyé sans traitement d'autres données à caractère personnel.

3.6. Sécurité des données

Le responsable du traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés ainsi que contre toute autre forme de traitement illicite[9].

Toute donnée collectée et stockée doit être sécurisée de manière appropriée. Les concepteurs de systèmes doivent travailler en collaboration avec des experts en sécurité compétents pour garantir que les failles de sécurité sont correctement gérées, en particulier en cas de migration des systèmes existants vers l'internet.

[9] Article 17, paragraphe 1, de la directive 95/46/CE.

3.7. Garanties pour les personnes qui ont des besoins spécifiques

L'utilisation de la biométrie pourrait avoir un impact important sur la dignité, la vie privée et le droit à la protection des données des personnes vulnérables, comme les jeunes enfants, les personnes âgées et les personnes physiquement incapables de poursuivre le processus de relevé avec succès. Vu les conséquences potentiellement nuisibles pour les personnes concernées, il est indispensable d'établir des exigences plus strictes dans le processus d'évaluation de l'impact de toute mesure interférant dans la dignité d'une personne en termes de remise en question de sa nécessité et sa proportionnalité ainsi que des possibilités d'une personne à exercer son droit à la protection des données, pour que cette mesure soit jugée admissible. Des garanties appropriées doivent être en place pour protéger des risques de stigmatisation ou de discrimination à l'encontre de ces personnes du fait de leur âge ou de leur incapacité à poursuivre le processus de relevé.

Concernant l'introduction d'une obligation légale généralisée de collecter des identifiants biométriques pour ces groupes, en particulier pour les jeunes enfants et les personnes âgées aux contrôles aux frontières à des fins d'identification, le groupe de travail a estimé que, *«pour préserver la dignité de la personne et pour garantir la fiabilité de la procédure, la collecte et le traitement des empreintes digitales doivent être limités pour les enfants et pour les personnes âgées, et que la limite d'âge doit être conforme aux limites d'âge fixées pour d'autres bases de données biométriques importantes de l'Union européenne (Eurodac en particulier)»*[10].

De toute façon, des garanties spécifiques (comme des procédures de repli appropriées) devraient être mises en œuvre afin de garantir le respect de la dignité humaine et des libertés fondamentales de toute personne qui n'est pas capable de poursuivre le processus normal de relevé et d'éviter ainsi que ces individus soient victimes d'un système technique défaillant[11].

3.8. Données sensibles

Certaines données biométriques pourraient être considérées comme sensibles au sens de l'article 8 de la directive 95/46/CE, en particulier les données qui révèlent l'origine raciale ou ethnique ou les données relatives à la santé. Par exemple, les données d'ADN d'une personne renferment souvent des données relatives à la santé ou qui peuvent révéler l'origine raciale ou ethnique. Dans ce cas, les données d'ADN sont des données sensibles et les garanties spécifiques prévues à l'article 8 doivent s'appliquer en plus des principes généraux de protection des données de la directive. Afin d'évaluer la sensibilité des données traitées par un système biométrique, le contexte du traitement doit également être pris en considération[12].

3.9. Rôle des autorités chargées de la protection des données

Compte tenu de la normalisation croissante des technologies biométriques à des fins d'interopérabilité, il est généralement accepté que le stockage centralisé de données biométriques augmente le risque d'utilisation de données biométriques en tant qu'élément permettant de relier plusieurs bases de données entre elles (ce qui pourrait conduire à la

---

10 WP134 - Avis 3/2007 sur la proposition de règlement du Parlement européen et du Conseil modifiant les instructions consulaires communes adressées aux représentations diplomatiques et consulaires de carrière, en liaison avec l'introduction d'éléments d'identification biométriques et de dispositions relatives à l'organisation de la réception et du traitement des demandes de visa (COM(2006)269 final).

11 WP134 - Avis 3/2007, p. 8

12 WP 29 - Advice paper on special categories of data («sensitive data»), réf. Ares (2011)444105 - 20/04/2011.

création de profils détaillés d'un individu), ainsi que les dangers spécifiques de la réutilisation de ces données à des finalités incompatibles, tout particulièrement dans le cas d'un accès non autorisé.

Le groupe de travail recommande que des garanties supplémentaires soient prévues en cas d'utilisation de systèmes basés sur des données biométriques en tant qu'élément pour relier plusieurs bases de données entre elles, étant donné que ce type de traitement est susceptible de présenter des risques particuliers au regard des droits et libertés des personnes concernées (article 20 de la directive 95/46/CE). Afin d'assurer l'adoption de garanties appropriées et en particulier d'atténuer les risques pour les personnes concernées, le responsable du traitement doit consulter les autorités nationales compétentes chargées de la protection des données avant d'introduire ces mesures.

4. Progrès et tendances technologiques, nouveaux scénarios

4.1. Introduction

Pendant longtemps, les technologies biométriques ont été utilisées principalement par les autorités gouvernementales, mais récemment, la situation a peu à peu changé. Aujourd'hui, les organisations commerciales jouent un rôle de premier plan dans l'utilisation de ces technologies et le développement de nouveaux produits.

L'un des principaux moteurs de cette situation est que la technologie a évolué de telle manière que les systèmes biométriques qui, auparavant, ne fonctionnaient bien que dans des conditions contrôlées ont été perfectionnées et conviennent désormais à une utilisation répandue dans un éventail d'environnements différents. En ce sens, la biométrie remplace ou améliore, dans certains cas, les méthodes d'identification conventionnelles, en particulier celles qui se basent sur plusieurs facteurs d'identification nécessaires pour des systèmes d'authentification solides. Les technologies biométriques sont également de plus en plus souvent utilisées dans des applications qui peuvent rapidement et facilement identifier une personne mais avec un faible niveau de précision.

L'utilisation des technologies biométriques s'étend également peu à peu au-delà de leur domaine d'application initial: de l'identification et de l'authentification à l'analyse du comportement, en passant par la surveillance et la prévention de la fraude.

Les progrès réalisés dans les réseaux et les technologies informatiques conduisent également à la montée de ce que l'on considère comme la deuxième génération de systèmes biométriques, basés sur l'utilisation de traits comportementaux et psychologiques, seuls ou associés à d'autres systèmes classiques pour former des systèmes multimodaux. Pour compléter le tableau, on assiste à un passage progressif vers l'utilisation de la biométrie dans des développements informatiques omniprésents et l'intelligence ambiante.

4.2. Nouvelles tendances de la biométrie

Plusieurs technologies biométriques peuvent être considérées comme étant arrivées à maturité et se retrouvent dans différentes applications commerciales, de gouvernement électronique et d'application de la loi. Les empreintes digitales, la géométrie de la main, le balayage de l'iris et certains types de reconnaissance faciale, entre autres, figurent parmi ces technologies. Certaines technologies biométriques basées sur l'analyse des traits corporels font également leur apparition. Si certaines d'entre elles sont nouvelles, certaines technologies biométriques traditionnelles prennent un nouvel élan grâce aux nouvelles capacités de traitement.

Les éléments typiques de ces nouveaux systèmes sont l'utilisation de traits corporels permettant la catégorisation/l'identification de personnes et la collecte à distance de ces traits. Les données collectées sont utilisées pour le profilage, la surveillance à distance voire des tâches encore plus complexes, comme l'intelligence ambiante.

Cette évolution a été possible grâce au développement continu des capteurs permettant la collecte de nouvelles caractéristiques physiologiques ainsi que de nouvelles manières de traiter les données biométriques traditionnelles.

Il convient également de mentionner l'utilisation de la «biométrie douce», qui se définit comme l'utilisation de traits très communs ne permettant pas de distinguer ou d'identifier clairement une personne, mais qui augmente les résultats d'autres systèmes d'identification.

Un autre élément essentiel des nouveaux systèmes biométriques est leur capacité de collecter des informations à distance ou en mouvement, sans que la personne concernée doive coopérer ou faire quoi que ce soit. Même si cette technologie n'est pas encore complètement au point, d'importants efforts sont déployés, en particulier à des fins répressives.

L'utilisation de systèmes multimodaux qui utilisent simultanément différentes données biométriques ou plusieurs unités/lectures des mêmes données biométriques qui peuvent être ajustées afin d'optimiser la sécurité/commodité des systèmes biométriques connaît une rapide progression. Ces systèmes peuvent réduire le taux de fausses acceptations, améliorer les résultats d'un système de reconnaissance ou faciliter la collecte de données d'une population plus large en compensant la non-universalité d'une source de données biométriques en l'associant à une autre.

Les systèmes biométriques sont de plus en plus utilisés par des organismes tant publics que privés; en général, dans le secteur public, les services répressifs utilisent régulièrement les données biométriques; dans les secteurs financier, bancaire et de la santé en ligne, ainsi que dans d'autres secteurs, comme l'éducation, la vente au détail et les télécommunications, l'utilisation de la biométrie connaît une rapide croissance. Cette évolution sera alimentée par les nouvelles caractéristiques découlant de la convergence/fusion des technologies existantes. Un exemple est l'utilisation de système de télévision en circuit fermé pour la collecte et l'analyse de données biométriques et de signatures du comportement humain.

Ce qui précède peut également être considéré comme un changement de perspective dans le développement des systèmes biométriques depuis des outils d'identification à des finalités de reconnaissance flexible, autrement dit, depuis l'identification à la détection du comportement ou de besoins spécifiques de personnes. La porte s'ouvre également à des utilisations bien différentes des applications de sécurité à grande échelle: la sécurité personnelle, les jeux d'argent et la vente au détail bénéficieront d'une meilleure interaction homme-machine dont les possibilités vont bien au-delà de l'identification ou de la catégorisation d'une personne.

4.3. Impact sur la vie privée et la protection des données

Il a été reconnu que les systèmes biométriques présentent, dès le premier moment de leur application, le potentiel de susciter de fortes inquiétudes dans différents domaines, notamment la vie privée et la protection des données, ce qui a certainement influencé leur acceptation sociale et alimenté le débat sur la légalité et les limites de leur utilisation et les garanties nécessaires pour atténuer les risques détectés.

La réticence traditionnelle aux systèmes biométriques a été liée à la protection des droits individuels, et elle l'est encore. Cependant, les nouveaux systèmes et l'évolution des systèmes

existants soulèvent toute une série d'inquiétudes, notamment la possibilité de déguiser la collecte, le stockage et le traitement ainsi que la collecte de matériel contenant des informations hautement sensibles qui peuvent envahir l'espace le plus intime de la personne.

L'évolution progressive des fonctions a été une source de grandes inquiétudes depuis que les technologies et systèmes sont utilisés. Si le risque est bien connu et géré dans la biométrie traditionnelle, il ne fait aucun doute que le potentiel technique plus élevé des nouveaux systèmes informatiques présente le risque que les données soient utilisées pour des finalités incompatibles avec leur finalité initiale.

Les techniques de camouflage permettant l'identification des personnes à leur insu représentent une sérieuse menace à la vie privée et une perte de contrôle sur les données à caractère personnel, entraînant de lourdes conséquences sur la capacité des individus à donner un consentement libre ou à simplement obtenir des informations sur le traitement. En outre, certains systèmes peuvent secrètement collecter des informations concernant l'état émotionnel ou des caractéristiques corporelles et révéler des informations relatives à la santé, ce qui génère un traitement des données non proportionnel ainsi qu'un traitement de données sensibles au sens de l'article 8 de la directive 95/46/CE.

Vu qu'il est impossible de garantir la totale précision des technologies biométriques, il existe toujours un risque implicite d'identifications incorrectes. Le vol d'identité au moyen de sources biométriques volées ou mystifiées peut entraîner de graves préjudices. Contrairement à ce qui se passe dans d'autres systèmes d'identification, la personne concernée ne peut pas simplement recevoir une nouvelle identité sous prétexte que la sienne est compromise.

Il convient également de mentionner le profilage dans le cadre de la prise de décision automatisée ou de la prédiction d'un comportement ou de préférences dans une situation donnée. Certaines données biométriques peuvent révéler des informations physiques sur une personne. Elles peuvent être utilisées pour le ciblage et le profilage mais également entraîner une discrimination, une stigmatisation ou une confrontation non désirée avec des informations non prévues/souhaitées.

4.4. Référence à des systèmes et technologies biométriques spécifiques

4.4.1. Réseau veineux et utilisations combinées

Deux grandes technologies utilisées se fondent sur la reconnaissance du réseau veineux: la reconnaissance du réseau veineux de la paume et la reconnaissance du réseau veineux des doigts, toutes deux sont aujourd'hui largement utilisées, en particulier au Japon.

Techniquement, cette technologie repose sur une capture du réseau veineux capturé par une caméra à infrarouge lorsque le doigt ou la main est éclairé par une lumière en proche infrarouge. L'image acquise est traitée pour décrire les caractéristiques du réseau veineux, ce qui donne une image post-traitée du réseau vasculaire. Le principal avantage de cette technologie est que chaque personne ne laisse pas de trace de ses traits biométriques[13] étant donné qu'il n'est pas nécessaire de «toucher» le lecteur. À l'heure actuelle, il est également difficile de collecter les données biométriques sans le consentement de la personne concernée. Enfin, cette technique peut également être utilisée pour détecter si le sujet présenté au système est vivant ou non en analysant le flux sanguin.

[13] Certains auteurs affirment que les technologies liées à la reconnaissance du réseau veineux peuvent révéler des maladies telles que l'hypertension ou des anomalies vasculaires.

La reconnaissance du réseau veineux peut être utilisée pour des applications d'accès logique et d'accès physique à des locaux. Les fabricants offrent également la possibilité d'inclure le capteur dans d'autres produits, en particulier pour des applications bancaires.

Les risques en matière de protection des données liés à l'utilisation des systèmes de reconnaissance du réseau veineux peuvent se décrire comme suit:

- précision: le niveau des résultats de la reconnaissance du réseau veineux est élevé, cette technologie étant considérée comme une alternative viable aux empreintes digitales. La reconnaissance du réseau veineux offre également un faible «taux d'échec d'inscription» (TEI), étant donné qu'il n'y a pas de détérioration du doigt ou de la main. Ces technologies n'ont pas encore été expérimentées/utilisées avec un registre de population très grand (au Japon, le modèle est comparé au modèle enregistré sur la carte à puce). Dans certains cas, cette technologie peut également être affectée par les conditions climatiques qui influencent le système vasculaire (chaleur, pression, etc.);

- impact: les répercussions des systèmes de reconnaissance du réseau veineux sur la protection des données sont restreintes, étant donné que les données biométriques ne sont pas facilement collectées et que l'utilisation de cette technologie se limite aujourd'hui à des applications du secteur privé;

- consentement et transparence: étant donné que les données sur le réseau veineux ne peuvent être collectées qu'en utilisant un éclairage et des caméras en proche infrarouge, on peut considérer que la personne est consciente du traitement et qu'elle y consent en appliquant son doigt ou sa main sur le lecteur. Toutefois, à l'instar de tout système biométrique, cette présomption doit être réduite dans certains cas spécifiques, par exemple lorsque la personne est employée par le responsable du traitement;

- autre(s) finalité(s) du traitement: à l'heure actuelle, les données relatives au réseau veineux présentent des risques limités d'utilisation pour d'autres finalités. Ce risque pourrait augmenter si ce type de traitement se généralisait et si la mystification était facilitée;

- capacité de corrélation: les données relatives au réseau veineux ne fournissent pas d'informations qui peuvent être reliées à d'autres données, sauf à des données relatives au réseau veineux obtenues à partir d'un autre traitement;

- suivi/profilage: le risque de suivi/profilage lié à la reconnaissance du réseau veineux est limité, tant que ce type de technologie n'est pas utilisé à grande échelle, par exemple dans une base de données centrale pour cartes de paiement;

- traitement de données sensibles: les seules données sensibles qui pourraient être obtenues à partir de données relatives au réseau veineux concernent l'état de santé, mais aucune étude formelle n'a été réalisée à ce sujet jusqu'à présent;

- révocabilité: les données relatives au réseau veineux semblent très stables dans le temps, mais cette affirmation doit être confirmée par l'expérience (les systèmes de reconnaissance du réseau veineux sont trop récents pour confirmer les résultats). Les données relatives au réseau veineux doivent donc être considérées comme irrévocables;

- protection contre la mystification: la mystification des données relatives au réseau veineux n'a pas encore été étudiée en profondeur, mais une récente étude a montré qu'il était possible de mystifier un lecteur du réseau veineux de la paume[14]. La principale difficulté que rencontre la mystification des données relatives au réseau veineux consiste à collecter un échantillon des données biométriques.

4.4.2. Empreintes digitales et utilisations combinées

La reconnaissance des empreintes digitales figure parmi les systèmes biométriques les plus anciens, les plus largement étudiés et les plus répandus. L'identification par empreintes digitales est utilisée depuis plus de 100 ans dans le domaine de l'application de la loi à des fins de vérification et d'identification. Elle se base sur le fait que chaque personne possède des empreintes digitales uniques qui présentent des caractéristiques spécifiques qui peuvent être mesurées afin de décider si une empreinte digitale correspond à un échantillon inscrit.

L'inscription requiert la présence physique de la personne concernée et, selon l'utilisation prévue, un personnel bien formé afin de garantir une qualité élevée des données. La prise d'empreintes digitales n'est pas une tâche banale, en ce sens que la précision des correspondances dépendra de la qualité de l'image par rapport à la technique d'image. Les techniques peuvent consister en la prise d'empreintes digitales d'un ou deux doigts, voire des dix doigts, à plat ou roulées. En fonction du système, les empreintes digitales peuvent être utilisées uniquement pour la vérification (1:1) ou pour l'identification et la comparaison avec des traces (1:n). Toutefois, comme l'ont montré certaines études, une fraction de la population est incapable de s'inscrire pour différentes raisons, ce qui pose un problème nécessitant des procédures de repli appropriées, en particulier pour des grands systèmes, afin d'éviter de priver les individus d'une chose à laquelle ils ont droit.

Si cette méthode n'est en principe pas fort invasive, elle peut être ressentie comme telle car elle s'accompagne de l'image négative d'être traité comme un suspect du fait de son utilisation répandue par les services répressifs.

Les empreintes digitales présentent différents traits qui peuvent être utilisés à des fins de vérification/identification, même si une analyse minutieuse reste la technique la plus utilisée. L'élaboration de nouvelles techniques (comme les scanners à haute résolution) permettra l'utilisation d'autres traits. Les techniques se sont également développées davantage en termes de capacités d'identification, ce qui permet d'utiliser de vastes bases de données pour l'identification.

En ce sens, les systèmes les plus avancés sont les «fichiers automatisés d'empreintes digitales» (FAED) utilisés par les services répressifs; ces fichiers peuvent être utilisés pour échanger des données en cherchant dans différents répertoires à des postes transfrontaliers, mais l'échange de données rencontre des problèmes liés aux différents endroits, formats et niveaux de qualité.

Des exemples de FAED au niveau de l'UE sont Eurodac et le système d'information sur les visas qui - selon les prévisions - figureront parmi les plus grandes bases de données du monde, vu qu'environ 70 millions d'empreintes digitales y seront stockées. Dans ses avis antérieurs, le groupe de travail a soulevé plusieurs questions concernant l'utilisation de bases

[14] Voir http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp6-del6.1.forensic_implications_of_identity_management_systems.pdf (en anglais).

de données à grande échelle, au vu de la nécessité de garantir la proportionnalité. Les problèmes de fiabilité en termes de faux positifs et de faux négatifs, le contrôle d'accès efficace à ces bases de données et les problèmes liés à l'utilisation des empreintes digitales des enfants et des personnes âgées doivent être abordés en particulier.

Les modèles sont fréquemment utilisés dans les systèmes biométriques basés sur les empreintes digitales et sont généralement considérés par les fournisseurs de systèmes comme un moyen de protéger les personnes. Toutefois, en fonction du système/de l'algorithme utilisé pour générer le modèle, il existe des risques potentiels quant à la possibilité de relier les modèles à d'autres bases de données d'empreintes digitales afin d'identifier des personnes.

L'utilisation de systèmes pour contourner les dispositifs de reconnaissance des empreintes digitales au moyen de doigts artificiels ou d'empreintes digitales fabriquées en matières synthétiques permettant le vol d'identité, est également un problème pertinent. Il existe différentes approches pour réduire les faiblesses de ces systèmes, comme la détection en direct, des systèmes basés sur la reconnaissance de plusieurs doigts et l'utilisation d'une supervision humaine adéquate pour l'inscription et pour les tâches d'identification/vérification.

Les risques en matière de protection des données liés à l'utilisation des empreintes digitales peuvent se résumer comme suit:

- précision: même si les empreintes digitales ont en fin de compte un taux de précision élevé, leur utilisation peut être compromise du fait des limitations dues à des problèmes liés aux informations (faible qualité des données ou processus d'acquisition non logique) ou à la représentation (traits choisis ou qualité des algorithmes d'extraction) et susceptibles d'entraîner des faux rejets ou des fausses correspondances;

- impact: le caractère irréversible du processus peut réduire la possibilité que la personne concernée exerce ses droits ou de revenir sur des décisions adoptées sur la base d'une fausse identification. La confiance dans la précision de la reconnaissance des empreintes digitales peut rendre la rectification d'éventuelles erreurs plus difficile, ce qui aurait d'énormes conséquences pour les personnes concernées. Cet élément doit être pris en considération lors de l'évaluation de la proportionnalité du traitement eu égard à la décision spécifique à prendre sur la base des empreintes digitales. Il convient également de mentionner le fait que l'absence de mesures de sécurité peut conduire à un vol d'identité pouvant avoir des répercussions considérables pour la personne concernée;

- capacité de corrélation: les empreintes digitales peuvent être mal utilisées étant donné que les données peuvent être reliées à d'autres bases de données. Cette possibilité peut conduire à des utilisations incompatibles avec la finalité initiale. Certaines techniques, comme la biométrie convertible ou le cryptage biométrique peuvent être utilisées pour diminuer le risque;

- traitement de données sensibles: certaines études affirment que les images des empreintes digitales peuvent révéler des informations sur l'origine ethnique d'une personne[15];

[15] http://www.handresearch.com/news/fingerprints-world-map-whorls-loops-arches.htm (en anglais) et http://www.crime-scene-investigator.net/fingerprintpatterns.html (en anglais).

- autre(s) finalité(s) du traitement: le stockage central de données, en particulier dans de vastes bases de données, implique des risques liés à la sécurité des données, à la capacité de corrélation et à l'évolution progressive des fonctions. En l'absence de garanties, cela permet d'utiliser les empreintes digitales pour des finalités autres que la finalité qui justifiait le traitement au départ;

- consentement et transparence: le consentement est au cœur de l'utilisation des empreintes digitales à des finalités autres que l'application de la loi. Les empreintes digitales peuvent être facilement copiées à partir d'empreintes latentes, voire de photographies, à l'insu de la personne concernée. D'autres problèmes liés au consentement concernent l'obtention du consentement d'un enfant et le rôle joué par les parents à cet égard (par ex., pour la prise d'empreintes digitales à l'école) ainsi que la validité du consentement dans un contexte professionnel;

- révocabilité: les données des empreintes digitales sont très stables dans le temps et doivent être considérées comme irrévocables. Un modèle d'empreintes digitales peut être révoqué dans certaines conditions;

- protection contre la mystification: les empreintes digitales peuvent être facilement collectées vu le grand nombre de pistes d'empreintes digitales que laisse une personne. En outre, de fausses empreintes digitales peuvent être utilisées avec de nombreux systèmes et capteurs, en particulier lorsque ces systèmes n'intègrent pas de protection spécifique contre la mystification. La réussite d'une attaque dépend en grande partie du type de capteur (optique, capacitif, etc.) et du matériel utilisé par l'attaquant.

Exemple
Un hôpital utilise des empreintes digitales stockées dans une base de données centrale pour authentifier les patients d'un service de radiothérapie afin de veiller à ce que chaque patient reçoive le traitement correct. Les empreintes digitales sont préférées au réseau veineux car le traitement perturbe le système vasculaire. En outre, une base de données centrale est utilisée car l'état des patients (âge, pathologie) implique un risque élevé de perte de carte, qui empêcherait l'accès au traitement. Dans ce cas, l'utilisation d'empreintes digitales semble être une solution appropriée.

4.4.3. Reconnaissance faciale et utilisations combinées

Le visage, comme les empreintes digitales, est utilisé à grande échelle comme source de données biométriques depuis plusieurs années. Plus récemment, ce n'est pas seulement l'identité qui peut être déterminée à partir d'un visage, mais également des traits physiologiques et psychologiques, comme l'origine ethnique, les émotions et le bien-être. La capacité d'extraire ce volume de données d'une image et le fait qu'une photographie peut être prise depuis une certaine distance à l'insu de la personne concernée témoignent de l'ampleur des problèmes relatifs à la protection des données qui peuvent découler de ces technologies.

La reconnaissance faciale comme moyen d'identification et de vérification n'a pas échappé à l'attention des services répressifs, des autres autorités publiques ou même des organisations privées. Les photographies apparaissent sur les passeports, les permis de conduire, les cartes d'identité nationales et les photos signalétiques depuis de nombreuses années. Il n'est pas rare qu'une photo soit imprimée sur une carte de contrôle d'accès ou d'autres cartes d'identification d'organisation. Ces images sont en général prises dans des conditions d'éclairage contrôlé et se limitent à une vue de face ou de profil d'une personne. L'utilisation

d'un tel ensemble contrôlé d'images était un point de départ naturel pour le traitement et la reconnaissance automatiques de personnes. Cette capacité a depuis été dépassée et la technologie est arrivée à un point où l'identification est possible à partir d'images utilisant un éventail de caméras, de points de vue et de conditions d'éclairage. Un volume colossal d'images est également disponible publiquement sur l'internet, comme celles téléchargées sur des réseaux sociaux et autres galeries accessibles au public. Ces risques ne se limitent pas aux images traditionnelles car la reconnaissance faciale a été intégrée avec succès dans les flux vidéo en temps réel. En ajoutant de nouvelles capacités de traitement à un système existant (par ex., la reconnaissance faciale à un système CCTV), les responsables du traitement doivent reconnaître que cela peut changer la ou les finalité(s) spécifiée(s) du système initial et réévaluer l'impact de ce changement sur la vie privée.

Les risques en matière de protection des données liés à l'utilisation de systèmes de reconnaissance faciale peuvent être décrits comme suit:

- précision: l'absence de garantie relative à la qualité des images risque de compromettre la précision. Si un visage n'est pas capturé (caché par les cheveux ou un chapeau), il est évident qu'il ne peut y avoir d'établissement de correspondance ou de catégorisation sans un degré élevé d'erreur. Les variations de pose et d'éclairage resteront un grand défi pour la reconnaissance faciale et affectent fortement la précision.

- impact: les répercussions spécifiques d'un système déterminé de reconnaissance faciale sur la protection des données dépendra de sa finalité et des circonstances particulières. Un système de catégorisation visant à dresser un relevé démographique des visiteurs d'une attraction sans capacité d'enregistrement aura un impact différent par rapport à un système utilisé pour la surveillance secrète par les services répressifs en vue d'identifier des fauteurs de troubles potentiels;

- consentement et transparence: un risque en matière de protection des données, que l'on ne retrouve pas dans bon nombre d'autres types de traitement de données biométriques, découle du fait que les images peuvent être capturées et traitées depuis une série de points de vue et de conditions environnementales et à l'insu de la personne concernée. Dans l'avis 15/2011 sur la définition du consentement, le groupe de travail souligne que pour que le consentement constitue une base juridique pour le traitement, il doit être «informé». Ce ne peut être le cas si la personne concernée n'a pas connaissance du traitement des images aux fins de la reconnaissance faciale. Même si la personne concernée est consciente qu'une caméra fonctionne, il peut ne pas y avoir d'indices visuels permettant de faire la différence entre un système de télévision en circuit fermé en direct ou qui enregistre et un objectif capturant des images pour un système de reconnaissance faciale;

- autre(s) finalité(s) du traitement: une fois capturées, légitimement ou non, les images numériques peuvent facilement être partagées ou copiées pour être traitées dans des systèmes différents de ceux auxquels elles étaient à l'origine destinées. Ce phénomène apparaît clairement dans le cadre des médias sociaux où les utilisateurs téléchargent leurs photographies personnelles pour les partager avec leur famille, leurs amis et leurs collègues. Une fois sur la plateforme des médias sociaux, les images peuvent être réutilisées par la plateforme elle-même pour un éventail de finalités, dont certaines peuvent être introduites dans la plateforme quelque temps après que l'image a été capturée ou téléchargée;

- capacité de corrélation: un grand nombre de services en ligne permettent aux utilisateurs de télécharger une image à relier au profil de l'utilisateur. La reconnaissance faciale peut être utilisée pour relier les profils de différents services en ligne (par l'image de profil), mais également entre le monde en ligne et le monde hors ligne. Il n'est pas impossible de prendre une personne en photographie dans la rue et de déterminer en temps réel son identité en recherchant dans ses images de profil publiques. Des services de tiers peuvent également parcourir les photographies de profil et autres qui sont publiquement disponibles pour créer d'énormes collections d'images en vue d'associer une identité réelle à ces images;

- suivi/profilage: un système d'identification pourrait également être utilisé sans connaître l'identité réelle de la personne. Dans un centre commercial ou une aire publique similaire, un système de reconnaissance faciale pourrait être mis en œuvre pour suivre les itinéraires et les habitudes d'acheteurs particuliers. Les finalités pourraient être la gestion efficace des files ou le placement de produits afin d'améliorer l'expérience des clients. Toutefois, la capacité de suivre ou de localiser une personne particulière s'accompagne de la capacité de profilage et d'offre de publicités ciblées ou d'autres services spécifiques;

- traitement de données sensibles: comme nous l'avons mentionné plus haut, le traitement de données biométriques pourrait être utilisé pour déterminer des données sensibles, en particulier celles ayant des repères visuels, comme l'origine raciale ou ethnique ou peut-être une affection médicale;

- révocabilité: une personne peut facilement changer l'apparence de son visage (barbe, lunettes, chapeau, etc.), ce qui peut suffire à tromper des systèmes de reconnaissance faciale, en particulier lorsque ces derniers fonctionnent dans un environnement non contrôlé. Toutefois, les principaux traits du visage d'une personne sont stables dans le temps et les systèmes peuvent également améliorer la reconnaissance en collectant et en associant différents «visages» connus d'une personne;

- protection contre la mystification: de nombreux systèmes de reconnaissance faciale peuvent facilement être mystifiés, mais les fabricants tentent d'améliorer la protection contre la mystification par des techniques telles que l'imagerie en 3D ou l'enregistrement vidéo. Néanmoins, la plupart des systèmes de base utilisés dans des applications publiques n'intègrent pas ce type de protection.

Exemple

Un exemple extrêmement imaginaire serait l'installation dans un centre commercial d'un système de vidéosurveillance de prochaine génération , capable de reconnaître les personnes, de suivre automatiquement leurs mouvements et de différencier les traits du visage comme le sourire ou la colère. Il pourrait reconnaître les clients réguliers qui entrent dans le parc de stationnement du centre commercial et les orienter vers des places de stationnement préférées. Lorsque les clients entrent dans la galerie marchande, le système pourrait identifier leurs vêtements pour leur suggérer des magasins à visiter en fonction des offres disponibles, de l'historique d'achat ou d'un ensemble prédéterminé d'indicateurs. La publicité personnalisée dans les vitrines de magasin ou le refus automatique d'accès à des magasins, restaurants et autres peuvent également être organisés. Les voleurs de voiture potentiels pourraient être identifiés et suivis avant même qu'ils touchent une voiture. Si nécessaire, des véhicules aériens téléguidés (drones) équipés de caméras et autres capteurs pourraient garder la piste des suspects jusqu'à ce que le soupçon soit confirmé ou écarté. Les objets cachés dans des

vêtements (couteaux ou objets dérobés) pourraient être détectés. Cette technologie ne se base pas uniquement sur des nouveaux systèmes biométriques. Elle combine et traite des informations qui sont déjà disponibles avec d'autres données provenant de plusieurs systèmes différents.

Une application similaire a été conçue dans le cadre du projet Indect (système d'information intelligent facilitant l'observation, la recherche et la détection pour la sécurité des citoyens en milieu urbain), où les technologies sont combinées pour lutter contre des actes de terrorisme et des crimes potentiels avant qu'ils se produisent. Le groupe de travail insiste fortement sur le fait que l'utilisation de ce type de systèmes biométriques nécessiterait une base juridique appropriée et des considérations strictes concernant la nécessité et la proportionnalité de ces mesures.

4.4.4. Reconnaissance vocale et utilisations combinées

En plus d'utiliser la reconnaissance vocale comme mesure biométrique pour l'identification, une utilisation relativement fréquente se caractérise par l'identification de traits spécifiques dans l'empreinte vocale pour catégoriser celui qui parle. Un exemple consisterait à analyser les réponses d'une personne tout au long d'une conversation téléphonique afin de déceler les accentuations et les irrégularités de la parole et mettre au jour des cas de fraude potentiels.

Des témoignages publiés par des fabricants font état du fait que, en mettant en œuvre cette technologie, des sociétés de services financiers ont augmenté les taux de détection de fraude et ont permis de régler plus rapidement les véritables demandes.

Les risques en matière de protection des données dans un système de catégorisation sont légèrement différents de ceux d'un système d'identification biométrique, dans le sens où il ne doit pas y avoir de phase d'inscription ni de stockage à long terme d'un modèle biométrique. Toutefois, si une conversation téléphonique est enregistrée, comme c'est généralement le cas pour une institution financière, des contrôles appropriés doivent être en place pour garantir la sécurité de ces données.

- Précision: un risque en matière de protection des données lié à un tel système réside dans les taux de détection, en particulier les faux positifs et les faux négatifs, à savoir combien de personnes sont identifiées à tort comme frauduleuses ou combien de demandes frauduleuses ne sont pas décelées? Si un système de catégorisation peut tolérer des taux d'erreur supérieurs à ceux de la vérification ou l'identification, il est encore possible d'avoir des procédures pour traiter de manière opportune les cas qui sont peut-être mal catégorisés.

- Consentement et transparence: une approche respectueuse de la vie privée peut être appliquée à ces technologies comme le fait de veiller à ce que les appels soient filtrés en fonction de leur pertinence et que les personnes concernées soient informées du processus en cours. Dans une étude de cas, les personnes étaient jugées comme inaptes pour un essai si leur langue maternelle n'était pas l'anglais, si elles souffraient d'une déficience auditive ou cognitive, ou si elles n'avaient pas accès à un téléphone. Les demandeurs étaient libres de refuser de prendre l'appel et de fournir des informations de manière traditionnelle mais aussi, pour ceux qui ne le souhaitaient pas ou ne pouvaient pas, de participer à un tel système sans être défavorisés.

- Autre(s) finalité(s) du traitement: tandis que, dans la majorité des cas, cette technologie nécessiterait des changements d'infrastructure spécifiques à mesure que

les secteurs public et privé consolident leurs infrastructures de TI pour intégrer des technologies telles que la voix sur IP, il est possible qu'à l'avenir les technologies de reconnaissance vocale s'intègrent de plus en plus facilement sans tenir dûment compte des obligations du responsable du traitement en matière de protection.

- Révocabilité: si une personne peut délibérément modifier sa voix, l'empreinte vocale est assez stable et peut permettre d'identifier une personne sans ambiguïté, en particulier lorsque cette dernière n'est pas informée (et n'est donc pas encline à modifier sa voix).

- Protection contre la mystification: un enregistrement vocal peut être utilisé pour mystifier des systèmes de reconnaissance vocale. Les techniques de lutte contre la mystification englobent les questions/réponses sur des sujets contextuels (en demandant la date du jour ou de répéter des mots bizarres).

4.4.5. ADN

Les améliorations apportées aux dispositifs utilisés pour le séquençage et la comparaison d'ADN ainsi que la disponibilité de matériel pour les analyses d'ADN à un prix abordable nous poussent à reconsidérer certaines des hypothèses du précédent document de travail sur la biométrie (WP80).

L'un des principaux changements survenus dans les technologies de profilage d'ADN est la réduction du temps nécessaire aux opérations de séquençage et de comparaison d'ADN. Les progrès permanents réalisés au fil des ans par la recherche universitaire et les concepteurs de biotechnologie ont réduit le temps nécessaire à la production d'un profil d'ADN de plusieurs jours à quelques heures, voire une fraction d'heure.

Le lancement d'un marché des services en ligne d'ADN constitue une menace pour les droits des personnes à la protection des données, en particulier lorsque le service requiert le transfert d'échantillons et de données biométriques entre différents pays (y compris des pays hors UE), plusieurs sous-traitants et l'absence de garanties pour le traitement de données génétiques ou relatives à la santé.

Il est très probable que dans un avenir proche, il sera possible de réaliser en temps réel (ou quasi réel) un profilage d'ADN et une comparaison d'échantillons en utilisant des dispositifs portables, qui seront le point de départ pour le développement de systèmes biométriques d'identification/authentification d'ADN présentant des niveaux de précision supérieurs à l'authentification par des empreintes digitales, la reconnaissance vocale et faciale.

Les progrès dans le profilage d'ADN sont également dus à l'intérêt croissant que portent les gouvernements, les juges et les services répressifs aux biotechnologies pour les enquêtes pénales. Vu la fiabilité de la comparaison d'ADN et le fait que les échantillons d'ADN peuvent être collectés à l'insu de la personne concernée, plusieurs États membres ont créé ou lancé au fil du temps des initiatives en vue de mettre en place des bases de données centralisées de profils d'ADN des personnes condamnées et d'échantillons trouvés sur des scènes de crime.

En mai 2005, sept États membres de l'UE ont signé un accord connu sous le nom de «traité de Prüm» en vue d'améliorer la coopération dans le cadre de la justice et des enquêtes pénales transfrontalières par l'échange d'informations. L'accord établit de nouvelles dispositions en matière de coopération étant donné qu'il fournit aux signataires certains droits d'accès à des bases de données nationales d'ADN uniquement dans le cadre des services répressifs

(poursuite de délits), des données d'empreintes digitales, des données à caractère personnel et non personnel, ainsi que des données sur l'immatriculation de véhicules. Depuis lors, d'autres États membres ont signé le traité et les fondements de l'accord ont été intégrés à la décision 2008/615/JAI du Conseil.

En vertu de ce cadre juridique, plusieurs États membres de l'UE disposent ou disposeront bientôt d'une base de données nationale fonctionnelle contenant les profils d'ADN de personnes condamnées et des preuves de scènes de crime, ce qui suscite certaines inquiétudes concernant ce traitement de données spécifique.

L'un des principaux problèmes liés à la création de bases de données d'ADN est que les données génériques obtenues à partir des échantillons d'ADN (loci) peuvent révéler - pas immédiatement pendant la phase de collecte - des informations relatives à l'état de santé, la prédisposition à des maladies ou l'origine ethnique. C'est pourquoi la constitution de bases de données d'ADN pose un risque important à la dignité humaine et aux droits fondamentaux. Ce risque a été examiné dans la résolution 2009/C 296/01 du Conseil. Des dispositions spécifiques limitent l'analyse d'ADN à des zones chromosomiques n'ayant aucune expression génétique en utilisant un ensemble spécifique de marqueurs d'ADN inconnus pour fournir des informations sur des caractéristiques héréditaires spécifiques (également connu sous le nom d'«ESS» - ensemble européen de référence).

Cependant, la possibilité que l'un des marqueurs extraits repris dans une base de données nationale d'ADN puisse révéler à l'avenir certains traits héréditaires ou d'autres informations sensibles requiert que l'on prête une attention constante à l'évolution de la biologie. En conséquence, si cette situation regrettable venait à se produire, certaines des informations de la base de données devraient être immédiatement supprimées. En outre, vu que ces bases de données d'ADN collectent les profils de personnes condamnées, l'analyse statistique des données doit être strictement limitée afin d'éviter le profilage basé sur le genre ou la race.

En ce qui concerne les bases de données d'ADN pour la police et la justice pénale, la Cour européenne des droits de l'homme a prononcé un arrêt selon lequel il fallait différencier clairement le traitement de données à caractère personnel et les profils génétiques de suspects et de personnes condamnées pour une infraction pénale[16].

Il existe également un risque potentiel que l'analyse d'ADN puisse être utilisée pour identifier les membres de la famille ou les parents liés à des crimes non résolus ou des personnes condamnées, car les profils d'ADN peuvent être cherchés dans la base de données en utilisant des ensembles partiels de marqueurs ou caractères génériques. Cette fonctionnalité soulève la question des implications du suivi des informations tirées d'une recherche familiale.

Il convient également de signaler qu'il existe des risques spécifiques liés à l'utilisation d'ensembles de données génomiques dans le cadre de la recherche. Le groupe de travail considère que l'accès aux échantillons et aux données doit être strictement limité à la communauté de la recherche et autorisé uniquement à des fins de recherche. En outre, il est nécessaire de préciser les circonstances dans lesquelles les conclusions et résultats de la recherche seront communiqués aux personnes (en tenant également compte de leur droit de ne pas savoir) ou seront enregistrés dans les dossiers médicaux.

[16] CEDH, arrêt du 4.12.2008, affaire S. et Marper c. Royaume-Uni (requêtes n° 30562/04 et 30566/04), en particulier le paragraphe 125.

Les risques en matière de protection des données liés à l'utilisation de l'ADN comme mesure biométrique peuvent se décrire comme suit:

- précision: même si l'ADN présente un degré très élevé de précision, il faut tenir compte du fait que la précision dépendra du nombre de marqueurs (loci) analysés. Tester les systèmes devrait garantir le niveau le plus élevé de précision;

- impact: l'utilisation de l'ADN peut être considérée comme extrêmement intrusive pour la personne concernée. Les données génétiques peuvent révéler des informations sensibles. L'analyse statistique des données peut être utilisée également pour le profilage et peut entraîner une discrimination à l'égard du sujet;

- autre(s) finalité(s) du traitement: de nouvelles technologies permettent aujourd'hui un volume croissant d'échange de données. C'est pourquoi il est indispensable de définir clairement qui peut avoir accès aux informations d'une base de données d'ADN. La recherche familiale et le ciblage racial peuvent être considérés comme une nouvelle technologie qui remet en question la finalité initiale du traitement dans les bases de données d'ADN actuellement disponibles;

- consentement et transparence: des services sont actuellement proposés en vue de procéder à des analyses d'ADN sur des échantillons biologiques envoyés par courrier postal (par ex., salive) dont les résultats sont disponibles via l'internet. Des contrôles d'identité insuffisants peuvent permettre à des particuliers ou des organismes de présenter des échantillons d'autres personnes et d'obtenir ensuite des données à caractère personnel sensibles sur d'autres personnes;

- capacité de corrélation: vu le volume et la variété d'informations qui peuvent être obtenues à partir du séquençage d'ADN, l'ADN peut faire l'objet d'une utilisation abusive étant donné que les données extraites peuvent être facilement reliées à d'autres bases de données permettant le profilage de la personne. Une recherche familiale permet également de relier une personne à des parents;

- traitement de données sensibles: l'ADN peut révéler des informations relatives à l'état de santé, à la prédisposition à des maladies ou à l'origine ethnique de la personne. Appliquer le principe de minimisation des données lors du choix des loci pertinents revêt dès lors une importance cruciale. Les informations d'ADN peuvent être extraites à partir de nombreux échantillons pour une longue période de sorte qu'il est recommandé de veiller à ce que l'accès aux échantillons soit strictement limité aux utilisateurs autorisés et pour des utilisations autorisées uniquement;

- révocabilité: l'ADN est irrévocable;

- protection contre la mystification: a priori, il est très difficile de mystifier l'ADN. Toutefois, il est souvent facile de collecter des échantillons de l'ADN d'une personne (par ex., cheveux) à son insu.

4.4.6. Reconnaissance biométrique de la signature

La reconnaissance biométrique de la signature peut être considérée comme un exemple des nouvelles utilisations des technologies biométriques traditionnelles. Il s'agit de techniques biométriques qui évaluent le comportement d'une personne tel que l'exprime la dynamique de la signature manuscrite. Si la reconnaissance traditionnelle de la signature se base sur

l'analyse des caractéristiques statiques ou géométriques de l'image visuelle de la signature (à quoi ressemble la signature), la reconnaissance biométrique de la signature se réfère plutôt à l'analyse des caractéristiques dynamiques de la signature (comment la signature a été faite), raison pour laquelle ces techniques sont souvent désignées sous le nom de «signature dynamique».

Les caractéristiques dynamiques typiques mesurées par ce type de système (comme une tablette de numérisation) sont le niveau de pression, l'angle d'écriture, la rapidité et l'accélération du stylo, la formation des lettres, l'orientation des traits de la signature et d'autres caractéristiques dynamiques uniques. L'utilisation et l'importance de ces caractéristiques dépendent d'un vendeur à l'autre et des dispositifs sensibles au contact sont en général utilisés pour les collecter. Certains dispositifs de reconnaissance de la signature peuvent réaliser une vérification en associant l'analyse de caractéristiques statiques (l'image visuelle) et dynamiques (pression, angle, vitesse, etc.) d'une signature.

Les risques en matière de protection des données liés à l'utilisation de la reconnaissance biométrique de la signature peuvent se décrire comme suit:

- précision: il se peut que les personnes ne signent pas toujours de la même manière, de sorte qu'elles pourraient rencontrer des problèmes au cours de la phase d'inscription, ainsi que lors de la vérification de leur identité;

- impact: les données biométriques basées sur des traits comportementaux comme une signature peuvent ne pas être uniques dans le temps et peuvent être modifiées par la personne concernée. Les changements dans la signature peuvent également avoir une origine physiologique et peuvent gêner la réussite d'une vérification, faisant naître la nécessité de procédures alternatives afin de vérifier l'identité de personnes;

- protection contre la mystification: si l'image graphique d'une signature traditionnelle peut être facilement reproduite et contrefaite par une personne entrainée, par photocopie ou avec un logiciel graphique, une signature dynamique est plus sûre car le processus de vérification contrôle également les caractéristiques dynamiques qui sont complexes et uniques au style d'écriture manuscrite d'une personne.

5. Orientations générales, recommandations spécifiques au secteur et mesures techniques et organisationnelles

Le déploiement d'un système biométrique repose sur la coopération de plusieurs acteurs:

- les fabricants, qui conçoivent et testent les capteurs biométriques et déterminent les performances de technologies biométriques;
- les intégrateurs, qui conçoivent le produit final qui sera vendu au consommateur - ils choisissent la technologie biométrique et déterminent en partie les finalités du système (en choisissant les clients auxquels il est destiné);
- les revendeurs, qui commercialisent le produit final au client - ils informent généralement le client des performances, des risques et éventuellement, du cadre juridique;
- les installeurs, qui installent le produit dans les locaux du client;
- les clients, qui décident d'acheter un système biométrique - ils définissent la finalité et les moyens du traitement et sont, partant, les responsable du traitement des données;
- les sujets, qui fournissent les données biométriques utilisées par le système.

Certains acteurs remplissent une ou plusieurs missions parmi celles précitées. Chaque mission doit garantir une utilisation de systèmes biométriques respectueuse de la vie privée: par exemple, l'installeur peut ne pas installer la caractéristique de sécurité définie par l'intégrateur.

5.1. Principes généraux

Concernant les données biométriques, la sécurité doit être une préoccupation centrale car les données biométriques sont irrévocables: en conséquence, une violation de données biométriques menace l'utilisation ultérieure de données biométriques en toute sécurité et le droit à la protection des données des personnes concernées, pour lesquelles il est impossible d'atténuer les effets de la violation.

Les risques augmentent parallèlement au nombre d'applications qui utilisent ces données (en particulier le risque de violations des données et d'évolution progressive des fonctions). Plus les données biométriques sont utilisées, plus la probabilité de vol de données biométriques est élevée.

Le groupe de travail reconnaît la tendance actuelle qui permet un accès à distance aux systèmes biométriques, par exemple, via des interfaces fournies sur l'internet. Cette tendance engendre une nouvelle série de problèmes de sécurité, dont bon nombre sont bien connus de l'industrie des TI. Le déploiement d'un tel système doit associer du personnel de sécurité technique approprié de l'industrie des TI dès les premiers stades de la conception.

Le groupe de travail recommande un niveau élevé de protection technique pour le traitement des données biométriques, grâce à l'utilisation des dernières techniques. À cet égard, le groupe de travail recommande de suivre les normes de l'industrie concernant la protection des systèmes dans lesquels les données biométriques sont traitées.

5.2. Respect de la vie privée dès la conception

Le respect de la vie privée dès la conception est le concept qui consiste à intégrer de manière proactive la vie privée dans la technologie elle-même.

Ce concept concerne l'ensemble de la chaîne de valeur des systèmes biométriques:

- les fabricants doivent appliquer les principes du respect de la vie privée dès la conception de nouvelles technologies et de nouveaux capteurs: il peut s'agir de la suppression automatique des données brutes après le calcul du modèle ou de l'utilisation du cryptage pour le stockage des données biométriques (que ce soit dans une base de données centrale ou sur une carte à puce). Les fabricants doivent également se concentrer sur le développement de technologies biométriques qui respectent la vie privée;
- les intégrateurs et les revendeurs doivent également appliquer les principes du respect de la vie privée dès la conception lorsqu'ils définissent le produit final qui sera vendu, en choisissant des technologies qui respectent la vie privée et en ajoutant des mesures de sécurité au produit final, comme la décentralisation de la base de données;
- les clients (futurs responsables du traitement) doivent appliquer les principes du respect de la vie privée dès la conception lorsqu'ils demandent un système biométrique particulier ou qu'ils définissent les caractéristiques techniques du système. Dans ce cas, les fabricants et les intégrateurs doivent offrir un certain niveau

de flexibilité dans leur produit afin de répondre aux principes de proportionnalité, de limitation des finalités, de sécurité et de minimisation des données.

Ces principes ont déjà été mis en œuvre avec succès dans certains dispositifs biométriques: certains fabricants ont intégré à un lecteur biométrique spécifique des éléments de cryptage ainsi que des interrupteurs anti-tirage et anti-altération pour prévenir tout accès non autorisé aux données biométriques.

Le groupe de travail recommande que les systèmes biométriques soient conçus en suivant des «cycles de développement» officiels qui se décomposent comme suit:

1. spécification des exigences sur la base d'une analyse des risques et/ou d'une évaluation spéciale de l'impact sur la vie privée;
2. description et justification de la manière dont le projet répond aux exigences;
3. validation par le biais de tests fonctionnels et de sécurité;
4. vérification du respect du cadre réglementaire du projet final.

Le groupe de travail encourage la définition de plans de certification qui pourraient garantir la mise en œuvre des principes de respect de la vie privée dès la conception et renforcer l'information des responsables du traitement concernant les risques en matière de protection des données liés aux systèmes biométriques.

5.3. Cadre d'évaluation de l'impact sur la vie privée

5.3.1. Principes généraux

L'évaluation de l'impact sur la vie privée est un processus où un organisme réalise une évaluation des risques liés au traitement des données à caractère personnel et définit des mesures supplémentaires pour atténuer ces risques. Par exemple, concernant la technologie RFID, le groupe de travail a établi que les exploitants d'application RFID sont chargés d'en évaluer l'impact. Cet organisme peut être le responsable du traitement ou le fournisseur qui conçoit l'application RFID.

Vu les risques spécifiques qu'implique l'utilisation de données biométriques, le groupe de travail recommande que celui qui définit la finalité et les moyens du dispositif procède à l'évaluation d'impact lors de la phase de conception des systèmes qui traitent ce type de données. Il peut s'agir du fabricant, de l'intégrateur ou du client final.

L'évaluation de l'impact sur la vie privée doit tenir compte des éléments suivants:

- la nature des informations collectées;
- la finalité des informations collectées;
- la précision du système, en supposant que des décisions importantes pour une personne pourraient découler d'une correspondance ou non d'un modèle biométrique;
- la base juridique et le respect des lois (le consentement est-il nécessaire?);
- l'accès au dispositif et l'échange interne et externe d'informations par le responsable du traitement, qui impliqueront des techniques et procédures de sécurité pour protéger des données à caractère personnel d'un accès non autorisé;
- les mesures les moins invasives dans la vie privée déjà adoptées (existe-t-il une procédure alternative au dispositif biométrique, comme le fait de demander la carte d'identité?);

- les décisions prises concernant la période de conservation et la suppression de données (quelle est la période appropriée? Toutes les données collectées sont-elles conservées pendant la même période? Existe-t-il un mécanisme automatique de décision et de une procédure de repli appropriée?);
- les droits de la personne concernée.

Les évaluations de l'impact sur la vie privée ne doivent pas uniquement se concentrer sur le recensement des risques, elles doivent également fournir des mesures de protection des données et expliquer comment le responsable du traitement présente des solutions appropriées pour atténuer les risques en matière de protection des données relevés dans la section précédente.

Lorsque le fabricant ou l'intégrateur a procédé à l'évaluation de l'impact sur la vie privée, le déploiement du système biométrique peut également nécessiter une évaluation supplémentaire pour tenir compte des spécificités du responsable du traitement des données. Par exemple, lorsqu'un système biométrique est intégré dans le système d'information du client, le client doit procéder à une autre évaluation de l'impact sur la vie privée qui tient compte de ses propres mesures et procédures de sécurité de TI.

5.3.2. La spécificité des données biométriques

Les données biométriques requièrent une attention particulière car elles identifient sans ambigüité une personne en utilisant ses caractéristiques comportementales ou physiologiques uniques.

C'est pourquoi l'évaluation de l'impact sur la vie privée doit viser à évaluer la manière dont les trois risques suivants peuvent être évités ou fortement limités par le système qu'elle analyse.

Le premier risque est l'usurpation d'identité, en particulier en cas d'identification et d'authentification. Le dispositif biométrique ne doit pas être trompé par une attaque de mystification ou doit garantir que la personne qui tente d'établir des correspondances est réellement celle qui est enregistrée dans le système. Cette menace semble moins importante pour les données biométriques qui ne peuvent être traitées à l'insu de la personne concernée, comme la reconnaissance du réseau veineux[17]. Il s'agit toutefois d'une préoccupation importante en ce qui concerne les dispositifs de reconnaissance faciale ou d'empreintes digitales. Les empreintes digitales sont laissées partout, rien qu'en touchant un objet. Le visage peut également être capturé par une photo à l'insu du sujet.

Le deuxième risque est le détournement de la finalité soit par le responsable du traitement lui-même soit par un tiers, y compris les services répressifs. Cette menace commune pour les données à caractère personnel devient cruciale lorsque les données biométriques sont utilisées. Les fabricants doivent prendre toutes les mesures de sécurité nécessaires pour éviter toute utilisation inappropriée des données et veiller à ce que toutes les données qui ne sont plus nécessaires au traitement soient immédiatement supprimées.

À l'instar de toutes les autres données, les données traitées ou stockées de manière légitime ou les sources de données biométriques ne peuvent être traitées ou inscrites par le responsable du

[17] Même s'il est difficile de prédire les attaques à la technologie de reconnaissance veineuse qui seront possibles dans les années à venir si cette technologie est plus largement utilisée.

traitement pour une finalité nouvelle ou autre, sauf s'il existe des motifs légitimes justifiant le nouveau traitement de ces données.

Le troisième risque est la violation de données qui requiert, dans le cadre des données biométriques, des actions spéciales en fonction du type de données qui ont été compromises. Lorsque le système utilisé crée des données biométriques basées sur un algorithme qui transforme un modèle biométrique en un certain code et que les données biométriques ou l'algorithme sont volés ou compromis, ces derniers doivent être remplacés. Lorsqu'une violation de données implique la perte de données biométriques directement identifiées qui sont très proches de la source de données biométriques, comme des images de visage ou des empreintes digitales, la personne concernée doit être notifiée en détail afin de pouvoir se défendre en cas d'éventuel incident futur où ces données biométriques compromises pourraient être utilisées contre elle comme éléments de preuve.

5.4. Mesures techniques et opérationnelles

Le traitement des données biométriques, en raison de leur nature, requiert des précautions et des mesures techniques et organisationnelles spéciales pour éviter des effets indésirables pour la personne concernée en cas de violation de données - en particulier en raison des risques de conduite illicite entraînant la «reconstitution» non autorisée d'un trait biométrique à partir du modèle de référence, leur corrélation avec différentes bases de données, leur autre «utilisation» à l'insu de la personne concernée pour des finalités non compatibles avec les finalités initiales ou la possibilité que certaines données biométriques puissent être utilisées pour révéler des informations sur l'origine raciale ou relatives à la santé de la personne concernée.

5.4.1. Mesures techniques

- *Utilisation des modèles biométriques*

Les données biométriques doivent être stockées sous forme de modèles biométriques dans la mesure du possible.

Un modèle doit être extrait d'une manière propre à ce système biométrique et non utilisée par d'autres responsables du traitement de systèmes similaires afin de veiller à ce qu'une personne ne puisse être identifiée que dans les systèmes biométriques qui ont une base juridique pour cette opération.

- *Le stockage sur un dispositif personnel par rapport au stockage centralisé*

Lorsque le traitement de données biométriques est autorisé, il est préférable d'éviter le stockage centralisé des données biométriques à caractère personnel.

En particulier pour la vérification, le groupe de travail estime qu'il convient que les systèmes biométriques reposent sur la lecture de données biométriques stockées sous forme de modèles cryptés sur des supports qui sont détenus exclusivement par les personnes concernées (par ex., cartes à puce ou dispositifs similaires). Leurs traits biométriques peuvent être comparés au(x) modèle(s) stocké(s) sur la carte ou le dispositif par des procédures de comparaison standard qui sont appliquées directement sur la carte ou le dispositif concerné, raison pour laquelle la création d'une base de données contenant des données biométriques doit être, en général et si possible, évitée. En effet, si la carte ou le dispositif est perdu ou égaré, les risques que les informations biométriques qu'ils contiennent puissent être mal utilisées sont en réalité limités.

Pour réduire le risque de vol d'identité, des données d'identification limitées concernant la personne en question doivent être stockées dans ces dispositifs.

Toutefois, à des fins spécifiques et en présence de besoins objectifs, une base de données centralisée contenant des informations ou des modèles biométriques peut être considérée comme admissible. Le système biométrique utilisé et les mesures de sécurité choisies doivent limiter les risques précités et veiller à ce que la réutilisation des données biométriques concernées pour d'autres finalités soit impossible ou du moins traçable. Il convient d'utiliser des mécanismes basés sur des technologies cryptographiques, afin de prévenir la lecture, la copie, la modification ou la suppression non autorisées de données biométriques.

Lorsque les données biométriques sont stockées sur un dispositif que la personne concernée contrôle physiquement, il convient d'utiliser une clé de cryptage spécifique pour les lecteurs en guise de protection efficace contre un accès non autorisé. En outre, ces systèmes décentralisés offrent une meilleure protection des données biométriques en soi étant donné que la personne concernée reste maîtresse, physiquement, de ses données biométriques et qu'aucun point unique ne peut être ciblé ou exploité.

Le groupe de travail souligne également que l'idée d'une base de données centralisée couvre un large éventail d'applications techniques qui vont du stockage au sein du lecteur à une base de données hébergée sur un réseau.

- *Capacité de renouvellement et révocabilité*

Étant donné que la source des données biométriques ne peut être modifiée, les systèmes biométriques dont la finalité est d'établir un lien d'identité doivent être conçus de manière à ce que la procédure d'inscription et le traitement des données biométriques permettent que plusieurs modèles biométriques indépendants puissent être extraits de la même source afin de pouvoir les remplacer en cas de violation de données ou de progrès technologique.

Les systèmes biométriques doivent être conçus de manière à permettre la révocation du lien d'identité, soit en vue de le renouveler soit de le supprimer définitivement, à savoir lorsque le consentement est révoqué[18].

- *Forme cryptée*

En ce qui concerne la sécurité, des mesures appropriées doivent être adoptées pour préserver les données stockées et traitées par le système biométrique: les informations biométriques doivent toujours être stockées sous forme cryptée. Un cadre de gestion des clés doit être défini afin de veiller à ce que les clés de décryptage ne soient accessibles qu'en cas de nécessité.

Vu l'utilisation généralisée de bases de données publiques et privées contenant des informations biométriques et l'interopérabilité croissante de différents systèmes utilisant des données biométriques, l'utilisation de technologies ou de formats de données spécifiques qui

[18] Par exemple, la technologie Turbine qui vise à protéger le modèle biométrique par transformation cryptographique des informations de l'empreinte digitale en une clé non inversible qui permet l'appariement par comparaison bit à bit. Les données biométriques transformées sont considérées comme non inversibles et ne peuvent donc pas être retransformées en échantillons biométriques et modèles originaux. En outre, afin de renforcer la confiance de l'utilisateur, cette clé sera également révocable, c'est-à-dire qu'une nouvelle clé indépendante peut être produite afin de délivrer de nouvelles identités biométriques. Voir http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-02-01_FP7_FR.pdf.

rendent les interconnexions de bases de données biométriques et les communications non contrôlées de données impossibles doit être préférée.

- *Lutte contre la mystification*

Pour maintenir la fiabilité d'un système biométrique et prévenir l'usurpation d'identité, le fabricant doit mettre en œuvre des systèmes visant à déterminer si les données biométriques sont à la fois authentiques et encore reliées à une personne physique. Concernant la reconnaissance faciale, il peut être vital de garantir que le visage est réel et non pas, par exemple, une image attachée sur la tête d'un imposteur.

- *Cryptage et décryptage biométriques*

Le cryptage biométrique est une technique utilisant les traits biométriques dans le cadre de l'algorithme de cryptage et de décryptage. Dans ce cas, un extrait des données biométriques est généralement utilisé comme clé pour crypter un identifiant nécessaire au service.

Ce système présente de nombreux avantages[19]. Tout d'abord, on ne stocke pas l'identifiant ou les données biométriques, uniquement le résultat de l'identifiant crypté avec les données biométriques. Ensuite, les données personnelles sont révocables étant donné qu'il est possible de créer un autre identifiant qui peut être protégé par cryptage biométrique également. Enfin, ce système est plus sûr et facile à utiliser pour la personne: il résout le problème de se rappeler de mots de passe longs et complexes.

Toutefois, le problème cryptographique à résoudre n'est pas facile car le cryptage et le décryptage ne tolèrent aucun changement de la clé, tandis que les données biométriques fournissent des modèles différents qui peuvent entraîner des changements dans la clé extraite. Le système doit donc pouvoir calculer la même clé à partir de données biométriques légèrement différentes, sans augmenter le taux de fausses acceptations.

Le groupe de travail convient que la technologie de cryptage biométrique est un terrain fertile pour la recherche et a acquis une maturité suffisante pour un examen de politique publique plus large, pour le développement de prototypes et pour l'examen d'applications.

- *Mécanismes d'effacement automatique des données*

Afin d'empêcher que les données biométriques soient stockées plus longtemps que nécessaire pour les finalités pour lesquelles elles ont été collectées et traitées ultérieurement, des mécanismes d'effacement automatique des données doivent être appliqués, même lorsque la période de conservation peut être légalement prolongée, ce qui garantit la suppression opportune de données à caractère personnel qui deviennent inutiles pour le fonctionnement du système biométrique.

Lorsqu'ils utilisent le stockage intégré dans le lecteur, les fabricants peuvent également stocker les modèles biométriques sur une mémoire volatile qui garantit que les données seront effacées lorsque le lecteur sera débranché. Partant, aucune base de données biométrique ne subsiste lorsque le lecteur est vendu ou désinstallé. Des interrupteurs anti-tirage peuvent également être utilisés pour effacer automatiquement les données si quelqu'un essaie de voler le lecteur.

---

[19] http://www.ipc.on.ca/images/resources/bio-encryp.pdf (en anglais).

- *Vastes bases de données biométriques et bases de données «à faible connexion»*

Certains pays utilisent de vastes bases de données biométriques, principalement pour deux finalités: contribuer aux enquêtes pénales et sécuriser la délivrance de documents d'identité (passeports, cartes d'identité, permis de conduire). Les bases de données utilisées pour les enquêtes pénales rassemblent généralement des informations sur les criminels et les suspects et doivent être conçues pour identifier une personne grâce aux données biométriques. À l'opposé, les bases de données utilisées pour lutter contre l'usurpation d'identité contiennent des données biométriques de toute la population et ne doivent pas être utilisées pour authentifier la personne (par exemple, si la personne a perdu ses documents ou a détruit la puce de sécurité de son passeport sur laquelle les données biométriques sont stockées).

Lorsqu'une base de données centrale est utilisée pour lutter contre l'usurpation d'identité, le groupe de travail considère que des mesures techniques doivent être mises en œuvre pour éviter tout détournement de finalité. Tout d'abord, le principe de minimisation des données requiert que seules les données nécessaires à l'authentification d'une personne soient collectées. Par exemple, on considère que la comparaison des empreintes digitales de deux doigts est suffisamment précise pour authentifier une personne.

En outre, les responsables du traitement peuvent utiliser des bases de données «à faible connexion» où l'identité d'une personne n'est pas reliée à une seule donnée biométrique mais plutôt à un groupe de données biométriques. La conception de la base de données doit garantir l'authentification de la personne avec un taux de probabilité très élevé (par exemple 99,9 %, ce qui suffit à dissuader les usurpateurs) et veiller à ce que la base de données ne puisse être utilisée à des fins d'identification (car un ensemble de données biométriques correspond à un grand nombre de personnes).

Le groupe de travail est favorable à l'utilisation de ce type de système lorsque de vastes bases de données biométriques sont utilisées pour lutter contre l'usurpation d'identité.

Exemple: mesures techniques pour systèmes d'authentification
La source de données biométriques est unique et peut être associée à la personne concernée toute sa vie. Si elle est utilisée comme base pour des systèmes d'authentification, il faut garder à l'esprit qu'elle ne peut être changée, tandis qu'avec les technologies d'authentification communes qui requièrent en général «de connaître ou d'avoir» un justificatif (par ex., nom d'utilisateur, mot de passe), un changement de ce justificatif est toujours possible. Partant, les systèmes utilisant l'authentification biométrique doivent mettre en œuvre des garanties spéciales pour protéger le lien entre des données biométriques et d'autres données d'identité:
- les données de modèle ne doivent pas être stockées au niveau central étant donné que la sécurité du stockage de données biométriques est essentielle par rapport à la sécurité globale du système biométrique. Un stockage distribué (par ex., sur une carte à puce) doit être préféré. Le cas échéant, la source des données et le modèle sont portés par la personne concernée;
- le stockage et la transmission de données biométriques doivent être protégés contre l'interception, la divulgation non autorisée et la modification par l'utilisation de technologies cryptographiques appropriées;

- certains types de données biométriques ne sont pas secrets (par ex., le visage) et ne peuvent être verrouillés, bloqués ou modifiés à la suite une violation de données, une communication ou une mauvaise utilisation. En conséquence, l'authentification doit être associée à d'autres justificatifs qui peuvent être verrouillés ou modifiés.

5.4.2. Mesures organisationnelles

Pour garantir la protection des données, il est nécessaire de planifier et d'appliquer des mesures organisationnelles. Par exemple, le responsable du traitement doit établir une procédure claire pour savoir qui peut accéder aux informations dans le système, si l'accès est partiel ou non, et pour quelles raisons. Il convient d'assurer un suivi de toutes les actions.

Le groupe de travail signale que la sous-traitance à des fournisseurs de services externes est possible, y compris pour des demandes de visa (sections 13 et 43 du règlement (CE) n° 810/2009 du 13 juillet 2009 établissant un code communautaire des visas) et devient plus populaire du fait de l'utilisation plus fréquente du stockage en nuage.

Le cas échéant, le responsable du traitement doit établir une politique détaillée sur la manière de contrôler ses entrepreneurs, comme des inspections à l'improviste, et demander des garanties concernant les employés, une procédure concernant les droits des personnes, etc.

Fait à Bruxelles, le 27 avril 2012

Pour le groupe de travail
Le président
Jacob KOHNSTAMM