Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques (2005)

AVANT-PROPOS

1. Le rapport d'étape sur l'application des principes de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE No 108, ci-après la Convention 108) à la collecte et au traitement de données biométriques représente l'aboutissement de travaux entrepris en 2003 par le Groupe de Projet sur la Protection des Données (CJ-PD) sous l'égide du Comité européen de Coopération Juridique (CDCJ) et, suite à la restructuration des comités de protection des données, poursuivis en 2004 et 2005 par le Comité Consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD).

2. Le CJ-PD a reçu mandat du Comité des Ministres pour élaborer en priorité à l'attention du CDCJ ou son bureau, un rapport sur l'incidence des principes de protection des données sur l'utilisation des données biométriques (empreintes digitales, identification par l'iris, identification du visage, géométrie de la main, etc.) dans différents domaines. » Inspiré par cet objectif, le CJ-PD a donné mandat à un expert scientifique, M. Marcel YON, Directeur Général de l'entreprise allemande de biométrie Viisage Technologies AG, pour préparer une étude sur la biométrie, mettant en relief ses aspects techniques, afin de donner au CJ-PD les éléments nécessaires à sa tâche. L'étude technique devrait être lue en relation avec le présent rapport, car elle explique certains des concepts qui y sont employés.

3. Après la fusion du CJ-PD et du T-PD à la fin de 2003, le T-PD renouvelé a accepté de reprendre l'activité sur la biométrie. Il était très conscient à la fois de la nature complexe de la biométrie et de la nécessité d'adopter de façon urgente une position sur l'application des principes de protection des données à ce domaine, afin de contribuer aux débats et aux projets biométriques en cours au niveau national et international. Pour ces raisons, le T-PD a décidé de préparer un rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques.

4. Un projet de rapport d'étape a été préparé par un expert scientifique, M. Alexander PATIJN, Conseiller juridique principal auprès du Ministère néerlandais de la Justice. Le T-PD et son Bureau ont ensuite travaillé en collaboration avec l'expert scientifique afin de réviser et de finaliser le rapport d'étape. Le T-PD a décidé, lors de sa 21e réunion du 2 au 4 février 2005, sous la présidence de Charlotte Marie Pitrat, de rendre ce rapport d'étape public, afin de contribuer aux débats et projets en cours en matière de biométrie dans plusieurs Etats membres du Conseil de l'Europe et instances internationales, comme l'OCDE (Organisation pour la Coopération et le Développement Economique) et l'OACI (Organisation de l'Aviation Civile Internationale). A son tour, le T-PD serait heureux de recevoir des contributions et réactions sur le contenu de ce rapport de la part des Etats membres ou autres organisations ou entités internationales intéressés. Une approche concertée revêt en effet une importance particulière dans le domaine de la biométrie, du fait de la complexité du sujet et de ses implications pour la personne humaine.

5. Le T-PD souhaite également attirer l'attention sur les instruments et rapports suivants du Conseil de l'Europe, dont certains éléments sont pertinents concernant la biométrie :

- Recommandation N° R (87) 15 du Comité des Ministres aux Etats membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police et ses trois rapports d'évaluation (17 septembre 1987)
- Recommandation No.R(89) 2 sur la protection des données à caractère personnel utilisées à des fins d'emploi (18 janvier 1989) et exposé des motifs
- Recommandation N° R (91) 10 sur la communication à des tierces personnes de données à caractère personnel détenues par des organismes publics (9 septembre 1991) et exposé des motifs
- Recommandation N° R (97) 5 sur la protection des données médicales (13 février 1997) et Exposé des motifs
- Rapport contenant des principes directeurs pour la protection des personnes par rapport a la collecte et au traitement de données au moyen de la vidéo-surveillance (2003)
- Principes directeurs sur la protection des données à caractère personnel à l'égard des cartes à puce (2004)
- Etude sur les numéros personnels d'identification: leur mise en œuvre, leur utilisation et la protection des données (1991)

6. Le rapport d'étape a été établi sur la base de l'état des connaissances relatives à la biométrie au moment de sa rédaction. Si le T-PD le juge nécessaire compte tenu de développements ultérieurs dans le domaine de la biométrie, il pourra être complété ou d'autres rapports d'étape pourront être rédigés à l'avenir.

7. Le rapport d'étape contient quatre parties :

- Une partie introductive
- Une seconde partie s'attache à identifier les spécificités de la biométrie
- Une troisième partie propose des critères pour le choix de l'architecture des systèmes biométriques
- Une quatrième partie prend appui sur les parties II et III afin d'éclairer l'application de la Convention 108 aux données biométriques. Pour cette raison, il est fait référence à certaines notions à la fois dans les parties II ou III et dans la partie IV.

I. Introduction

8. La biométrie est une méthode traditionnelle d'identification des individus : les empreintes digitales, par exemple, sont utilisées depuis des décennies. Toutefois, deux récents développements convergents favorisent grandement le recours de la biométrie. Tout d'abord, il existe un besoin croissant d'identification sans équivoque d'individus à la fois dans le secteur privé et le secteur public. Les menaces terroristes actuelles à l'échelle mondiale poussent à l'identification de personnes, partant du fait que les terroristes font usage d'identités multiples. Dans le secteur privé, l'usurpation d'identité est un problème croissant, permettant par exemple aux contrevenants de détourner de larges sommes d'argents des victimes dont ils ont frauduleusement pris l'identité. Ensuite, la nouvelle technologie et son développement rapide semblent répondre à ce besoin en permettant d'utiliser la biométrie de façon automatisée pour des vérifications massives d'identité en quelques secondes dans un endroit donné avec un degré suffisant de fiabilité.

9. Dans de nombreux pays, les pouvoirs publics envisagent ou sont déjà en train d'inclure les données biométriques dans les pièces d'identité, par exemple les passeports[1]. L'utilisation des empreintes digitales ou les techniques d'identification par l'iris et par la reconnaissance faciale sont à l'heure actuelle les méthodes les plus vraisemblables. Des sociétés privées, comme les banques par exemple, envisagent l'émission de cartes à puces contenant des données biométriques pour leurs clients dans le but d'effectuer des transactions. Dans le même temps, les écoles elles-mêmes commencent à identifier leurs élèves afin d'empêcher les jeunes non autorisés à pénétrer dans leurs cantines. Dans un avenir proche, des applications domestiques arriveront sur le marché. Il conviendra alors d'observer et analyser ces applications au fur et à mesure de leur apparition.

10. L'application de la biométrie soulève d'importantes questions en matière de droits de l'homme. L'intégrité du corps humain et la manière dont il est utilisé par la biométrie constituent un aspect de la dignité humaine. En conséquence, en choisissant de faire appel ou non à la biométrie pour résoudre un problème particulier, les responsables de traitement devraient faire preuve d'un sens éthique particulier. La biométrie n'en est qu'à ses premiers pas et l'on sait peu de choses sur ses possibles inconvénients. Une fois que cette technique aura été adoptée à grande échelle, un développement irréversible, porteur d'effets imprévisibles, pourrait être amorcé. C'est pour cela qu'il convient d'appliquer le principe de précaution, qui, selon les circonstances , impose une certaine retenue. L'article 8 de la Convention européenne des Droits de l'Homme (ci-après CEDH) est particulièrement pertinent pour le domaine de la biométrie. D'une part, le droit au respect de la vie privée implique le respect du corps humain. La dignité humaine doit être pleinement respectée pendant le processus de collecte et d'utilisation des caractéristiques du corps humain. Les questions posées par les personnes handicapées et celles dont les caractéristiques physiques ne correspondent pas aux normes techniques doivent trouver une réponse. Des procédures de secours devraient être prévues en cas de panne du système si les caractéristiques physiques ne correspondent pas aux normes techniques. D'autre part, la collecte de données à caractère personnel en prévision de leur traitement automatisé pose le problème de la protection des données, en particulier si ces données biométriques révèlent inutilement, mais de manière inévitable des données sensibles comme par exemple une information sur un type de maladie ou un handicap physique.

11. De nombreux rapports sur la protection des données et la biométrie ont été récemment publiés[2]. *La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe* (Convention 108, ci-après dénommée «la Convention») a créé un Comité consultatif, ci-après dénommé «le Comité», dont l'une des fonctions est de donner des avis sur la pertinence de la Convention dans des domaines particuliers. La Convention donne effet à l'article 8 de la CEDH à l'égard du traitement automatisé des données à caractère personnel. Elle établit les principes généraux visant à éviter toute interférence avec la vie privée ou, lorsque celle-ci est inévitable, à l'entourer de garanties. Ces principes n'indiquent pas précisément quels types de traitement des données sont autorisés ou non. Ils exigent donc d'être interprétés dans le cas d'applications concrètes. La biométrie n'échappe pas à cette règle générale. Le Comité est d'avis que les principes de la Convention ont été formulés avec succès d'une manière indépendante de la technologie. Ils peuvent être appliqués même si les techniques de

[1] Le règlement du Conseil de l'Union européenne 15152/04, adopté en décembre 2004, prescrit l'introduction de données biométriques dans les passeports.

[2] Le Groupe de protection des données, créé par l'article 29 de la Directive de l'Union Européenne sur la protection des données, a publié le 1er août 2003 un document de travail sur la biométrie concernant les aspects relatifs à la Directive (www.europa.eu.int/comm/privacy).

traitement des données biométriques à caractère personnel n'étaient pas encore connues lors de la rédaction de la Convention.

12. À l'évidence, nous vivons à une époque où les personnes ne seront bientôt plus reconnues et identifiées à l'intérieur de communautés relativement restreintes qui délivreront les pièces attestant leur identité. La récente internationalisation et anonymisation de la société, ainsi que la montée des menaces sécuritaires et le développement rapide et constant de la technologie de l'information, ont fait naître d'énormes espoirs dans l'utilisation de la biométrie en matière de vérification (l'authentification) et l'identification des personnes. D'autre part, beaucoup craignent que, sans une réglementation appropriée, des atteintes aux droits relatifs à la protection de la vie privée auront lieu sans justification suffisante.

13. Le Comité juge nécessaire d'attirer l'attention sur certaines questions relatives aux rapports entre la Convention et l'usage de la biométrie. La Convention permet l'extension de ses règles au traitement manuel de données personnelles. On pourrait prendre l'exemple de la traditionnelle comparaison manuelle de la photographie sur un passeport avec la personne qui le présente au contrôle d'identité ou celui pas si ancien de la fastidieuse comparaison d'empreintes digitales relevées sur le lieu d'un crime avec celles de criminels connus. Le Comité n'a pas étudié spécifiquement ce traitement manuel. Il se focalise sur le nouveau développement consistant à la vérification d'une prétendue identité ou à l'identification sur place et en quelques secondes de groupes importants de personnes par le traitement automatisé de données biométriques. En effet, nous n'avons que peu d'expérience de telles applications, et elles comportent des risques d'abus. Bien que les données elles-mêmes ne révèlent en général aucune information concernant les personnes soumises au contrôle, ces données biométriques, mises en relation avec les circonstances par rapport auxquelles elles sont collectées apportent une connaissance sur ces individus qui pourrait, d'une part ne pas être nécessaire à la finalité de la collecte et, d'autre part, ne pas avoir de base légale adéquate.

14. Le Comité n'a pas souhaité traiter davantage des questions liées aux autorités de contrôle et au transfert des données biométriques vers des pays qui n'offrent pas un niveau de protection adéquat. Ces aspects sont traités dans le protocole additionnel de la Convention 108 sur les autorités de contrôle et les flux transfrontières de données (STE No 181), récemment entré en vigueur. Les règles générales exposées dans cet instrument valent également pour les données biométriques. Des problèmes spécifiques aux données biométriques dans le contexte des flux transfrontières de données ne sont pas encore apparus, mais il pourrait s'avérer nécessaire d'examiner à nouveau cette question à l'avenir.

15. Ce rapport est conçu comme un guide pour tous ceux qui sont amenés à décider s'il faut faire usage de la biométrie et, dans ce cas, quelles conditions et garanties pourraient être envisagées. Il est encore trop tôt pour émettre un jugement définitif. Les incertitudes sont encore nombreuses. En effet, les avantages apparents peuvent être source d'inconvénients dont on ne mesure pas encore pleinement les conséquences. Certaines de ces craintes peuvent se révéler infondées. C'est pourquoi le Comité a choisi de se limiter à un rapport d'étape. Celui-ci ne tire pas de conclusions définitives, mais vise à contribuer au débat sur le traitement des données biométriques et la protection des données. Il appelle à des précautions afin d'éviter de possibles développements irréversibles non souhaités mais comportant des inconvénients considérables et inutiles pour la protection des données à caractère personnel. Le Comité se propose d'actualiser le présent rapport ou de publier d'autres rapports si des faits nouveaux le rendent nécessaire, voire de rédiger de nouveaux instruments juridiques .

II. En quoi la biométrie est-elle spécifique ?

Description des technicités

16. Le terme « biométrie » fait référence à des systèmes qui utilisent des caractéristiques physiques, physiologiques ou des éléments de comportement personnel mesurables afin de déterminer l'identité ou de vérifier l'identité alléguée d'un individu. Le système est basé sur les étapes suivantes. Un échantillon biométrique est prélevé sur un individu, par exemple le relevé d'une empreinte digitale ou un balayage de l'iris. Cette caractéristique physique peut être représentée au moyen d'une image. Il arrive souvent toutefois que des données soient extraites de cet échantillon. Ces données extraites constituent le gabarit biométrique. Les données biométriques, qu'il s'agisse de l'image ou du gabarit, sont alors conservées sur un support de stockage. Ces phases préparatoires sont connues sous le nom de processus d'enrôlement. La personne dont les données sont ainsi stockées est appelée l'enrôlé.

17. La finalité elle-même du système biométrique n'intervient qu'à un stade ultérieur. Lorsqu'une personne se présente au système, celui-ci va lui demander de présenter ses caractéristiques biométriques. Le système procédera alors à une comparaison entre l'image des données présentées (ou le gabarit extrait de ses données) et les données biométriques de l'enrôlé. Si la comparaison est positive, la personne sera reconnue et « acceptée » par le système. Si elle ne l'est pas, la personne ne sera pas reconnue et sera « rejetée ».

18. L'image ou le gabarit des données enrôlées ne sera que rarement identique à l'image ou au gabarit des données biométriques qui seront ensuite présentées au système. La caractéristique change souvent quelque peu ou est présentée d'une autre manière qu'au cours de l'enrôlement. La comparaison comporte inévitablement un certain élément de probabilité. L'absence d'une correspondance parfaite n'empêche pas d'établir avec un degré suffisant de certitude pour de nombreuses finalités que la personne qui présente ses caractéristiques biométriques au système est la même personne que la personne enrôlée.

Vérification et identification

19. Aux fins de remplir une finalité donnée, un choix doit être opéré entre les deux fonctions de la biométrie, dont l'une est la vérification et l'autre l'identification.

20. La vérification consiste à comparer un échantillon biométrique présenté avec les données biométriques enrôlées appartenant à une seule personne. Il est envisagé, dans le but de renforcer la sécurité, de vérifier plus d'une caractéristique biométrique d'un individu, par exemple ses empreintes digitales et son iris. Dans ce cas, le système ne reconnaîtrait la personne uniquement dans le cas d'un résultat positif d'une vérification cumulée des deux données. Le résultat est positif ou négatif, la comparaison est acceptée ou rejetée.Le fait que les données enrôlées soient conservées sur un support de stockage individuel (par exemple la carte à puce) dans une base de données, ou dans les deux est neutre. L'élément décisif est que, dans le cas d'un contrôle d'identité, les données relatives à une seule personne concernée fassent l'objet d'un traitement automatisé.

21. Lors de l'identification, les données présentées ne sont pas seulement comparées aux données enrôlées appartenant prétendument à la même personne, mais également avec les données biométriques d'autres personnes concernées contenues dans la même base de données ou dans des bases de données qui y sont reliées. Ceci exclut la possibilité de conserver les données enrôlées uniquement sur un support de stockage individuel. Il faut

effectuer une recherche pour établir une concordance possible entre l'échantillon présenté par un individu et les données enrôlées de (plusieurs) autres individus. Il peut donc arriver que la même donnée biométrique semble attachée à d'autres individus ou que la même personne semble reliée avec différentes caractéristiques enrôlées dans la base de données. Cela pourrait signifier soit qu'une personne utilise plusieurs identités, soit que quelqu'un essaie de cacher sa vraie identité sous le nom de quelqu'un d'autre. Dans ce cas, il s'agirait d'un cas d'usurpation d'identité.

22. Le choix d'une fonction de vérification ou d'identification dépend hautement de la finalité envisagée du système biométrique et des circonstances dans lesquelles il sera employé. L'instrument doit servir la finalité pour laquelle les données ont été collectées et ne pas être inutilement surdimensionné. Soit, exprimé en termes juridiques : l'instrument ne doit pas être disproportionné par rapport à la finalité première qu'il doit remplir. Le choix d'un système d'identification, alors qu'un système de vérification apparaît également possible, exige une justification particulière. Le rapport technique insiste sur ce point essentiel : les problèmes de vérification ne doivent pas être résolus par des solutions d'identification.

23. La délivrance d'un passeport, d'une carte d'identité ou d'un visa a pour but d'établir que la personne concernée n'a pas déjà fait une demande sous un autre nom. La caractéristique qui est introduite pendant le procédé d'enrôlement doit être comparée à la liste des caractéristiques déjà enregistrées dans le système, ce qui permet d'éviter les doubles saisies. Cette finalité ne peut pas être assurée sans l'aide d'un système d'identification. Cependant, après l'enrôlement, pour déterminer le détenteur légitime, il suffit de vérifier que la caractéristique biométrique incorporée dans le document correspond à la caractéristique présentée par la suite par le détenteur du document.

24. Le Comité convient que la vérification des passeports peut avoir d'autres finalités légitimes. Si la finalité n'est pas uniquement de vérifier que l'utilisateur du passeport est le détenteur légitime mais également, par exemple, de contrôler que la personne concernée n'est pas sur une liste de personnes recherchées, la simple vérification n'est pas suffisante. Vérifier sur la base de données biométriques que quelqu'un figure dans une liste suppose le recours à l'identification. cette finalité supplémentaire doit être explicitée pour qu'il soit possible de juger si le système d'identification choisi est nécessaire à cette finalité supplémentaire.

25. Un autre exemple est celui de l'émission d'une carte bancaire. Dans des circonstances normales, il est possible d'identifier une personne en vérifiant son passeport ou toute autre pièce d'identité. En supposant que les documents présentés sont fiables, il n'est pas nécessaire d'établir l'identité de cette personne d'une autre manière. La carte bancaire pourrait contenir les caractéristiques biométriques d'une personne pour qu'il soit possible de vérifier si la carte est bien utilisée par le propriétaire légitime. La vérification consisterait, dans ce cas, à contrôler que la caractéristique biométrique de l'utilisateur correspond à la caractéristique biométrique stockée dans la carte. Pour cette finalité, il n'est pas nécessaire que la banque stocke des données biométriques supplémentaires sur la carte bancaire. Il n'est pas nécessaire à cette fin de stocker d'autres données biométriques dans une base de données en plus de celles déjà contenues sur la carte bancaire.

La dignité humaine

26. Les données biométriques sont collectées à partir ou proviennent du corps humain. Rien n'est plus personnel, affirment certains, que son propre corps. En effet, la collecte de

ces données pourrait être ressentie comme une atteinte à la dignité humaine. Certaines personnes y seront indifférentes, d'autres éprouveront une résistance psychologique à l'idée que le corps humain soit utilisé comme une source d'information. D'autres encore n'accepteront pas qu'une partie de leur corps, ne serait-ce qu'un doigt, soit « analysée » par une machine. D'autres, peuvent exprimer leur inquiétude face à la banalisation sans considération du corps humain. La résistance peut dépendre de facteurs socioculturels, religieux ou propres à chaque individu. L'attitude à l'égard de l'utilisation du corps humain par la biométrie pourrait également évoluer avec le temps.

27. Ces arguments ne signifient pas que l'usage de la biométrie est inutile ou injustifié, mais ils posent les limites aux domaines auxquels elle s'applique. Un responsable de traitement doit évaluer les avantages et les inconvénients de l'utilisation des données biométriques dans un but précis avant de décider d'employer la biométrie ou des solutions de substitution. Cette évaluation devrait avoir lieu avant de procéder aux choix. La biométrie ne devrait pas être choisie uniquement parce qu'elle est pratique à utiliser. C'est la finalité de cet instrument qui devrait justifier son utilisation, et l'usage des données biométriques ne devrait pas trop s'écarter de cette finalité, compte tenu de tous les intérêts correspondants et des valeurs en jeu. Le but de ce rapport est de mettre en lumière certains de ces intérêts.

Un caractère unique et permanent

28. La caractéristique qui identifie une personne de manière unique n'est pas donnée par l'homme mais par la nature et elle est en principe inaltérable tout au long de sa vie. Quels que soient les moyens employés par une personne pour dissimuler son identité, légitimes (par exemple les repentis qui cherchent à se protéger des malfaiteurs) ou illégitimes (par exemple des criminels cherchant à échapper aux forces de l'ordre) la biométrie permettra souvent une identification permanente. À l'avenir, il n'est pas exclu que la biométrie puisse être utilisée de manière généralisée pour identifier les individus pendant toute leur vie. Il existe cependant des exceptions qui peuvent poser problème quant à l'identification permanente. Les caractéristiques biométriques d'un individu peuvent changer au cours de son existence, par exemple suite au vieillissement, à une intervention chirurgicale ou à un accident. Un système biométrique pourrait alors ne plus le reconnaître.

Probabilité

29. En ce qui concerne la biométrie, deux moments devraient être distingués. Le premier est le moment de l'enrôlement, au cours duquel la donnée biométrique d'une personne est introduite dans le système ; le second est constitué par toute collecte subséquente de données biométriques aux fins de comparaison avec les premières données. Une correspondance absolument parfaite entre les données enrôlées et celles présentées ensuite au système est techniquement impossible. L'utilisation d'un système basé sur des données biométriques repose inévitablement sur des probabilités d'ordre statistique. Il n'existe pas de système infaillible. Si les deux caractéristiques correspondent avec un degré suffisant de probabilité, la personne concernée sera « reconnue » par le système. Les systèmes biométriques sont donc intrinsèquement faillibles.

30. Le risque d'une fausse reconnaissance ou d'une fausse non reconnaissance peut avoir de fâcheuses conséquences pour la personne concernée. Par exemple, si elle est « reconnue » à tort comme apparaissant sur une liste de criminels ou délinquants recherchés, la conséquence pratique pourrait être qu'elle aura à démontrer son innocence. Le taux de fausse reconnaissance et de faux rejets dépend de plusieurs propriétés du système, comme sa qualité

et sa fiabilité, le processus d'enrôlement etc. Les taux peuvent être ajustés de manière à obtenir le niveau de sécurité requis pour la finalité du système. Les efforts visant à prévenir des résultats erronés devraient être proportionnels à la finalité du système.

31. Le principe d'un traitement loyal des données à caractère personnel suppose que la personne concernée soit informée des aspects du traitement qui sont pertinents pour elle. Les propriétés du système qui reposent de façon inhérente sur des probabilités et donc sont faillibles, constituent un tel aspect pertinent. Aussi, il revient au responsable de traitement d'informer la personne concernée sur ce fait et sur ce qu'elle peut faire si elle est victime de ce système. Toute présomption d'infaillibilité est erronée.

32. Le caractère probabiliste des systèmes biométriques peut avoir des effets contraires pour la personne concernée ou le responsable de traitement, selon la façon dont le système est établi. Quatre situations peuvent être distinguées :

(a) Un système filtre des individus indésirables, par exemple un stade de football désire empêcher l'entrée d'hooligans figurant sur une liste avec leurs données biométriques. Une erreur du système tournera à l'avantage de la personne concernée. Elle ne sera pas reconnue et donc ne sera pas filtrée. Le hooligan entrera dans le stade.
(b) Le même système « reconnaît » à tort la personne concernée. Cette dernière aura des problèmes à prouver qu'elle a été faussement cataloguée comme hooligan.
(c) Un système permet uniquement à des personnes reconnues utilisant par exemple une carte à puce servant de clé pour pénétrer dans des locaux sécurisés. Une non-reconnaissance à tort de la personne autorisée se retournera contre elle s'il n'existe pas de procédure alternative pour permettre à la personne d'accéder par un autre moyen.
(d) Le même système « reconnaît » à tort une personne qui en réalité n'est pas autorisée. Le responsable de traitement fait face à une menace concernant la sécurité. En pratique cette menace peut être réduite à un minimum acceptable, mais elle ne peut pas être supprimée.

33. Il revient au responsable de traitement d'assumer le caractère faillible inhérent au système biométrique pour lequel il a opté. C'est à lui d'établir le degré adéquat de probabilité par rapport à la finalité du système, est-il par exemple adéquat d'accepter un taux erreur d'un sur dix mille ou d'un sur dix millions ? Ceci sera particulièrement important pour des applications à grande échelle. C'est à lui de tester régulièrement que le système est toujours en accord avec le degré de fiabilité exigé pour la finalité qu'il doit servir.

34. Des questions peuvent se poser quant à la précision à l'égard d'une éventuelle finalité secondaire incompatible avec la finalité du système. Il serait en effet contraire au principe de proportionnalité d'exiger qu'un système employant des données biométriques soit plus précis que ne le requiert la finalité initiale de ce système, pour l'unique raison que dans des cas exceptionnels les données pourraient être requises pour une finalité secondaire, comme par exemple la répression d'infractions pénales conformément à l'article 9 de la Convention. Si, dans des cas exceptionnels, les données sont utilisées à de telles finalités secondaires, leur fiabilité devrait être évaluée par rapport à la finalité pour laquelle elles ont été initialement obtenues. Prenons l'exemple d'un cas de système biométrique conçu pour une finalité spécifique où il serait suffisant d'enrôler un gabarit comportant douze éléments extraits de l'échantillon biométrique original. Pour une finalité secondaire incompatible, un gabarit comprenant au moins cinquante éléments semble

nécessaire. Mais cette utilisation incompatible exceptionnelle ne peut justifier le stockage de ces cinquante éléments. Si, dans des cas exceptionnels, les données devaient être utilisées à de telles finalités secondaires, il faudrait alors prendre en compte le caractère limité de leur fiabilité.

35. Les données biométriques ont la réputation d'être extrêmement fiables car elles paraissent liées à la présence physique et réelle d'une personne et, à ce titre, seraient donc inaliénables. Il existe réellement une forte probabilité que l'usage des données biométriques permette d'être assuré d'avoir affaire à la bonne personne. Néanmoins, des falsifications sont toujours possibles. Les empreintes digitales relevées sur un verre peuvent par exemple servir à créer avec de la cire une empreinte analogue sur un support de stockage. Il est plus difficile de programmer un ordinateur pour qu'il génère artificiellement autant d'images nécessaires à la reproduction du gabarit enregistré sur un support de stockage de données volées. Cette image (par exemple imprimée dans la cire) peut servir à se faire passer pour le propriétaire légitime du support volé. Cette procédure de falsification n'est pas affectée par un cryptage du gabarit préalable à son enregistrement sur le support de stockage.

36. Même si les systèmes biométriques paraissent fiables, il est néanmoins dangereux de leur faire trop confiance. Les applications impliquant un large groupe d'individus sont encore rares. Le caractère faillible inhérent de ces systèmes implique que des erreurs se produiront nécessairement, même si le système fonctionne parfaitement. Il y a encore peu de recul quant à leur efficacité, fiabilité et leurs effets sur la vie privée. Les effets sur la société d'une introduction plus générale de toutes sortes de systèmes biométriques à la fois dans les sphères privées et publiques sont encore moins connus. Ceci milite en faveur d'une installation graduelle et prudente de ces systèmes. Une introduction trop rapide et trop enthousiaste pourrait produire des effets imprévus qui seraient très difficiles à renverser.

37. En fonction des circonstances, l'on pourrait envisager d'utiliser simultanément une ou deux caractéristiques biométriques. En théorie, l'augmentation ou la diminution du risque d'erreur semblerait dépendre de l'architecture du système. S'il existe un double contrôle de l'identité d'un individu (par exemple une combinaison des empreintes digitales et de l'iris), a priori cela rendrait le système plus fiable. Cependant, les erreurs étant inévitables, la procédure comporterait un double risque d'erreurs. Le Comité désire mettre ces questions en avant sans en donner les réponses. On peut penser que des réponses définitives à ces questions ne seront possibles qu'au travers d'expériences concrètes.

Interopérabilité

38. Il existe une tendance que l'on peut comprendre à collecter les caractéristiques biométriques conformément à des procédures standardisées, pour permettre à différents systèmes de fonctionner entre eux. Les systèmes qui permettent la compatibilité peuvent reconnaître les personnes en fonction de leurs données biométriques, indépendamment du responsable de traitement qui a mis au point le système et de la finalité pour laquelle les données ont été collectées. Cette évolution a cependant pour effet d'élargir le fossé entre des intérêts antagonistes : l'utilité des systèmes employant des données biométriques est accrue, mais il en va de même des risques d'utilisation pour des finalités incompatibles.

39. On ne peut exclure que l'interopérabilité technologique en cours pourrait avoir à long terme comme conséquence pratique l'assimilation de l'utilisation de certaines données

biométriques à un identifiant unique d'application générale[3]. Un exemple d'un tel identifiant est le numéro d'identification personnel (PIN)[4]. Un facteur aggravant pourrait venir du fait que, contrairement au numéro PIN qui peut être changé au cours d'une vie (par exemple à la suite d'une émigration), un tel changement n'est pas nécessairement envisageable pour les données biométriques.

40. Les recommandations de l'OACI qui visent à assurer la compatibilité des systèmes au niveau mondial afin de renforcer la sécurité des transports dans l'aviation civile, ajoutent une dimension supplémentaire. Sans règles précises, elles pourraient facilement avoir pour effet une dissémination générale des données biométriques car certains pays ne disposent pas d'une législation dans le domaine de la protection des données ou appliquent une telle législation uniquement à leurs propres citoyens. Le Comité est conscient de l'étroite coopération entre le Conseil de l'Europe, l'OACI, l'OCDE et l'Union Européenne afin d'aborder certains de ces problèmes. Il espère beaucoup du résultat de ces travaux.

L'utilisation de la biométrie comme outil de protection de la vie privée (PET)

41. La biométrie peut être utilisée comme outil de protection de la vie privée (PET). Une caractéristique biométrique dans une carte bancaire empêche celle-ci d'être utilisée par quelqu'un qui n'en est pas le détenteur légitime. La biométrie peut également servir à protéger les bases de données contenant des données à caractère personnel contre un accès abusif. Si la personne qui accède aux données stockées dans une base de données est identifiée par une caractéristique biométrique, il est probable que ce n'est pas une personne non autorisée qui demande d'y accéder.

III. Critères de sélection de l'architecture du système

42. L'utilisation de la biométrie est possible dans différentes architectures du système. Les systèmes peuvent être distingués en vue de leur pertinence pour la protection des données à caractère personnel. D'un point de vue de la protection des données, plusieurs critères semble être pertinents. On peut citer actuellement dans ce cadre l'approche consistant à privilégier l'image ou le gabarit et la manière dont les données sont stockées et peuvent être consultées. Cependant, l'évolution de la technologie dans un avenir proche pourrait mener à des systèmes ou des critères auxquels on ne pense pas encore.

43. Le choix entre l'enrôlement de l'image complète d'une caractéristique biométrique ou d'un extrait sous la forme d'un gabarit se réfère au principe selon lequel il ne faut pas collecter plus de données que celles nécessaires à la finalité pour laquelle ces données sont collectées. Traditionnellement, les empreintes digitales et la photographie des délinquants arrêtés sont stockées afin de les retrouver plus facilement en cas de récidive après leur condamnation. Ils peuvent ensuite laisser des empreintes digitales sur le lieu du crime ou être reconnus par des témoins sur les photographies de la police. L'enrôlement de l'image complète est nécessaire, puisqu'on ne sait pas par avance quelle partie de l'empreinte digitale pourra être recueillie sur le lieu du crime. Cette image peut révéler des données sensibles, comme certaines forme de maladies ou handicaps physiques. Ces données peuvent ne pas être nécessaires à la finalité, leur conservation n'en est pas moins indispensable.

[3] Voir à ce sujet l'article 8 paragraphe 7 de la Directive 95/46/CE

[4] Se reporter également au rapport du Conseil de l'Europe sur *Les numéros personnels d'identification : leur mise en oeuvre, leur utilisation et la protection des données* (1991).

44. Il est moins évident qu'il soit nécessaire de conserver dans un système une image complète dans le cas où la reconnaissance à l'aide de données biométriques s'effectue en demandant la coopération de la personne concernée afin qu'elle soumette l'échantillon biométrique pertinent lors de la collecte secondaire. Un degré suffisant de probabilité pour de nombreuses finalités sera atteint en extrayant un gabarit des caractéristiques soumises et en les comparant avec celles qui ont été enrôlées.

45. Un autre point pertinent est la façon dont les données enrôlées, qu'il s'agisse d'images ou de gabarits, sont conservés puisque ceci a des conséquences sur leur accessibilité et leur possible dissémination. L'architecture d'un système biométrique peut être conçue de différentes manières. La première possibilité est que la donnée enrôlée soit stockée uniquement sur un support de stockage individuel sécurisé, par exemple une carte à puce[5]. Cela pourrait suffire à des fins de vérification. Les données nécessaires sont disponibles uniquement sur la carte. Si la personne concernée perd sa carte, toutes les données sont perdues. La carte est comparable à une clé. Jusqu'à récemment, il était acquis que, ce faisant, la personne concernée gardait le contrôle de l'utilisation des données la concernant. On pensait que nul ne pouvait avoir accès aux données tant que la personne concernée n'utilisait pas sa carte. Le responsable de traitement qui établit la finalité du système, ses moyens et la catégorie de données à traiter n'aurait aucun accès aux données tant que la personne concernée elle-même ne les soumettrait pas volontairement et en toute connaissance de cause. Une nouvelle technologie permet d'équiper une carte à puce de façon à permettre la lecture sans contact direct de la donnée enrôlée et stockée sur cette carte *(RFID)*. La personne concernée perd ainsi le contrôle exclusif de l'utilisation de ses données. Ceci pourrait être compensé par des mesures de sécurité supplémentaires. Par exemple, on pourrait donner effet au principe du traitement loyal en prévenant le détenteur chaque fois qu'il y a lecture des données sur sa carte. La lecture secrète de données, si elle est nécessaire, devrait être spécifiquement prévue par la loi en incluant des garanties adéquates contre les abus. Toutefois, si la personne concernée n'est pas dans le champ d'un lecteur, le responsable de traitement n'a pas accès aux données.

46. Une autre architecture possible du système consiste à stocker les données enrôlées dans une base de données locale ou régionale par exemple sous le contrôle exclusif des autorités municipales responsables de la délivrance d'un passeport. Il n'importe donc pas de savoir si oui ou non les données sont stockées en plus sur un support individuel de stockage pour la personne concernée. Grâce à sa base de données, le responsable de traitement peut vérifier si les données biométriques d'un requérant existent déjà dans le système. Dans le cas d'un passeport, les autorités municipales peuvent vérifier si un résident local a déjà demandé un passeport sous un autre nom. Accompagné d'autres garanties, cette architecture pourrait être considérée comme adéquate pour empêcher toute acquisition d'une double identité. Ainsi, la législation allemande sur les passeports ne permet pas la création d'une base de données fédérale comprenant des données biométriques, provenant des autorités locales de délivrance des passeports. De même, ses autorités fédérales n'ont pas un accès automatique aux données[6]. Pour certaines finalités, il

[5] Voir les *« principes directeurs du Conseil de l'Europe pour la protection des données à caractère personnel à l'égard des cartes à puces. » (2004)*

[6] Le Parlement Européen a plaidé pour une solution similaire dans son opinion sur la proposition de la Commission Européenne d'introduire des données biométriques dans les passeports des citoyens de l'UE. En octobre 2004, la Commission des Libertés, de la Justice et des Affaires Intérieures a publié un projet de programme s'opposant à des projets d'établissement d'une base de données centralisées des passeports émis au niveau de l'UE dans la mesure ou cela augmenterait le risque d'utilisations incompatibles.

sera nécessaire de stocker les données enrôlées dans une base de données centrale ou de les rendre accessibles à travers une interconnexion d'un groupe de responsables de traitement[7].

47. Le Comité note que des expérimentations sont en cours dans différents pays afin de tester l'architecture conciliant au mieux les besoins de l'établissement de l'identité d'un individu par la vérification ou l'identification avec les exigences légales de protection des données biométriques en accord avec les principes de protection des données. Le Comité ne pense pas pouvoir exclure que d'autres caractéristiques de l'architecture du système sont ou pourraient devenir légalement pertinentes du point de vue de la protection des données.

48. La distinction entre un support de stockage individuel et une base de données n'est pas liée à la distinction entre les fonctions de vérification et d'identification. Un système qui utilise la fonction de vérification peut s'appuyer soit sur le simple support de stockage individuel ou sur une base de données. En cas de support de stockage individuel, seule une comparaison *avec* l'individu qui est en possession du support est possible. Bien qu'une base de donnée puisse être organisée pour procéder uniquement à cette sorte de comparaison, la possibilité existe de comparer l'échantillon soumis lors de la collecte secondaire avec les données biométriques enrôlées d'autres personnes concernées. Les fonctions de la base de données peuvent changer du jour au lendemain. Un système d'identification par contre suppose nécessairement le choix d'une base de données afin de permettre la comparaison d'une donnée soumise avec les données biométriques de plus d'une personne. Toutefois, le choix d'une base de données pour la fonction de vérification requiert une justification particulière.

49. Dans certains cas exceptionnels, le changement ad hoc de fonction ou l'interconnexion ad hoc de différentes bases de données biométriques peut s'avérer nécessaire et déroger à la finalité pour laquelle le système a été établi à l'origine. En l'espèce, l'article 9 de la Convention 108 exige que la loi décrive ces cas au préalable et avec précision. Une procédure doit ensuite décrire qui décide de l'application de ces cas particuliers. Elle pourrait également prévoir des conditions supplémentaires, par exemple définir la finalité précise de l'interconnexion et prévoir une révision périodique. Certaines circonstances spéciales peuvent justifier l'exigence d'une architecture spécifique qui incorporerait des fonctions techniques permettant de répondre à de telles demandes juridiques exceptionnelles. Une fois encore, la loi devrait explicitement prévoir un tel cas. Le Comité a débattu de la question de savoir s'il peut y avoir des cas dans lesquels il pourrait être justifié d'exiger que l'architecture du système incorpore la facilité technique permettant de collecter plus de données biométriques ou de données associées ou encore un gabarit plus détaillé que ne l'exige la finalité du système. Le Comité a estimé qu'il n'était pas en mesure de répondre à cette question. Toutefois, il souligne que si une telle collecte de données supplémentaires, incompatible avec la finalité du système est considérée comme nécessaire, elle doit se fonder sur une loi spécifique remplissant toutes les conditions de l'article 8 paragraphe 2 de la Convention européenne des Droits de l'Homme et de la jurisprudence de la Cour européenne des droits de l'homme y afférente, en particulier en ce qui concerne l'exigence de proportionnalité.

50. Toute base de données court le risque d'être piratée ou que les données qu'elle contient soient mises en danger, quelles que soient les mesures techniques, organisationnelles ou réglementaires prises. Il peut arriver qu'un pirate informatique trompe la sécurité d'un système. Dans le passé, maintes mesures de sécurité réputées

[7] Un exemple est Eurodac, système visant à identifier au moyen de leurs empreintes digitales les personnes réfugiées ou supposées telles qui ont demandé l'asile dans l'un des pays de l'UE.

adéquates n'en ont pas moins été contournées. Le cryptage des données traitées aide à accroître la sécurité mais ne peut garantir une sécurité absolue. Le personnel ayant accès aux données peut en faire mauvais usage, quels que soient les règlements et le contrôle en place. Enfin, l'histoire a montré qu'à des régimes respectant l'Etat de droit, peuvent succéder d'autres qui ne le respectent pas.

IV. Comment les principes de la Convention 108 s'appliquent-ils aux données biométriques?

A quel moment la Convention 108 s'applique-t-elle aux données biométriques ?

51. La Convention 108 s'applique au traitement automatisé des données à caractère personnel (article 1). Dans la définition de l'article 2, lettre a, de la Convention 108, les données à caractère personnel désignent toute information concernant une personne physique identifiée ou identifiable. Différents points de vue existent quant à savoir si les données biométriques constituent toujours des données à caractère personnel. Certains arguent du fait qu'il pourrait s'avérer impossible d'identifier quelqu'un sur la base par exemple d'une empreinte digitale incomplète. En outre, l'on pourrait soutenir que les données biométriques en elles-mêmes ne fournissent aucune information sur l'individu. D'autres au contraire défendent l'idée que les données biométriques permettent par leur nature même l'identification d'un individu, puisque ces données peuvent être rattachées de manière unique et permanente à une personne. Des technologies à venir pourraient permettre d'effectuer facilement une identification qui pourrait sembler impossible à l'heure actuelle. L'argument selon lequel les données biométriques ne fourniraient aucune information sur la personne peut être contredite, puisqu'il ne s'agit que d'un argument purement théorique. En effet, la collecte de données biométriques ne peut se produire qu'en certaines circonstances relatives par exemple au lieu et au moment de la collecte. Or ces circonstances offrent toujours certaines informations sur la personne concernée qui est la source des données biométriques.

52. Le Comité est d'avis qu'il n'est pas nécessaire de décider si les données biométriques sont des données personnelles ou si c'est le cas seulement dans certaines circonstances. Il pense que, dès que les données biométriques sont collectées en vue d'un traitement automatisé, la possibilité existe que ces données soient rattachées à une personne identifiable. Dans ce cas, la Convention s'applique.

Qui est le responsable de traitement ?

53. Le responsable de traitement est la personne qui décide quelle sera la finalité des données, quelles catégories de données seront collectées et quelles opérations leur seront appliquées (article 2, lettre d). Lorsque la Convention s'applique, il doit exister une personne responsable de la conformité avec les règles de protection des données. Cette personne est considérée comme responsable de traitement, même dans les cas où sa responsabilité consiste seulement à éviter toute identification réelle. Dans le cas de systèmes biométriques, le responsable de traitement n'est pas toujours facile à déterminer de prime abord. Prenons l'exemple de bases de données contenant les données biométriques des titulaires de passeport : il se peut que seules les autorités locales délivrant les passeports aient accès aux données, bien que la finalité, les catégories de données

devant être stockées et leur utilisation soient toutes établies par le législateur. Dans ces cas, la législation devrait stipuler qui doit assumer les responsabilités en question.

54. De multiples responsables de traitement peuvent, comme par exemple pour les bases de données décentralisées, assumer les responsabilités qui leur sont conférées par la Convention. Il peut exister une situation encore plus complexe, dans laquelle, bien qu'un responsable de traitement définisse le système, sa finalité etc…, les données ne sont accessibles qu'à la personne concernée, puisqu'elles sont stockées uniquement sur une carte à puce en sa possession.

55. Parfois, ce sont des sous contractants qui traitent les données pour le compte du responsable de traitement, sans pour autant que la pleine responsabilité de ce dernier n'en soit réduite. Dans la Directive 95/46 de l'UE, de tels sous-contractants sont définis dans l'article 2, lettre e comme « *sous-traitants* ».

56. Dans toutes ces situations complexes, il est nécessaire d'établir clairement qui est le responsable de traitement et de rendre cette information transparente pour la personne concernée. Celle-ci a en effet le droit de savoir sans recherches compliquées à qui s'adresser en cas de non respect supposé des règles de protection des données. Ce n'est pas à elle de rechercher, dans des situations complexes, qui accepte ou qui - au terme de poursuites - est contraint d'assumer la responsabilité de ce non respect.

Traitement loyal et licite

57. Les données à caractère personnel doivent être obtenues et traitées loyalement et licitement (article 5, lettre a). La loyauté est un large concept. Appliqué aux données biométriques, il implique en particulier le fait d'informer la personne concernée qu'elle est l'objet d'une collecte de données, à moins qu'elle ne soit déjà en possession de cette information. La personne concernée doit connaître précisément la finalité de la collecte et l'identité du responsable de traitement.

58. En théorie, la première collecte de données biométriques sera soit rendue obligatoire par une loi, soit volontaire. La délivrance par une autorité publique d'une pièce d'identité est un exemple de collecte obligatoire. S'il existe dans un pays l'obligation de présenter une pièce d'identité à un agent de l'Etat qui la demande (par exemple un passeport) et s'il est prévu que ce document contienne des caractéristiques biométriques, la personne concernée n'a pas le choix de refuser. Dans le domaine du droit privé, on considère souvent que les données biométriques sont collectées sur la base du volontariat. La personne concernée est sensée avoir le libre choix d'opter par exemple pour une carte bancaire en vue de faire des retraits d'argent. Le Comité note que des systèmes similaires ont été créés dans le passé sur la base d'un libre choix pour le client, mais au travers d'une application à d'importants groupes de personnes et de l'acceptation de contrats d'adhésion[8] ou de clauses standards non négociables, ils ont évolué vers une situation ou *de facto* les personnes concernées qui désirent mener une vie normale n'ont plus de libre choix.

59. Le second temps du traitement des données biométriques a lieu lorsque le système est utilisé, par la présentation d'une caractéristique biométrique qui est comparée avec les données enrôlées précédemment. Si les deux correspondent, la personne est acceptée par le système. Beaucoup de systèmes biométriques sont conçus pour conserver des données

[8] En anglais « standard contracts »

concernant l'utilisation du système. On se réfère à ces données sous les noms de « données virtuelles », « données de trafic » ou « données associées ». Elles indiquent en général quand et à quel endroit un individu a été en contact avec le système. C'est le terme « données associées » qui sera utilisé aux fins du présent rapport .

60. Une finalité légitime du traitement de données associées est par exemple de s'assurer du bon fonctionnement du système biométrique. Elles ont cependant pour effet secondaire de révéler des informations concrètes sur le comportement d'une personne. À chaque fois que la personne concernée soumet ses caractéristiques biométriques, elle laisse des traces plus ou moins précises sur son comportement : où elle était, quand, pendant combien de temps, avec qui, etc. Selon le principe de traitement loyal, la personne concernée doit être informée de chaque collecte ultérieure de données biométriques, soit parce que celle-ci lui est présentée de manière évidente et qu'elle introduit délibérément ses données biométriques, soit parce qu'elle est informée de la collecte à l'initiative du responsable de traitement. Dans certains contextes, il pourrait être suffisant de donner des informations à caractère général. Dans d'autres cas où il n'est pas évident que des données associées sont collectées, la « loyauté » impose de donner des informations à chaque fois que les données sont collectées. Les données associées ne devraient pas être utilisées à des finalités incompatibles avec celles pour lesquelles elles ont été collectées.

Définition de la finalité et choix d'une technique particulière

61. Les données à caractère personnel doivent être traitées pour des finalités déterminées et légitimes (article 5, lettre b). Choisir d'utiliser les données biométriques implique de déterminer et d'expliciter la finalité de leur traitement. L'utilisation de données biométriques afin de contrôler l'accès à un pays, une zone ou des locaux protégés peut être considérée comme un usage légitime de données biométriques. Un autre usage légitime de données biométriques pourrait être leur utilisation dans des passeports ou des visas pour empêcher l'utilisation d'identités frauduleuses, l'obtention d'un second passeport ou l'émission d'un passeport à une personne non autorisée. Il n'y a pas de liste exhaustive des finalités légitimes.

62. Dès que les finalités sont déterminées, le système technique ne devrait pas permettre la collecte et le traitement de plus de données personnelles que les finalités ne l'exigent, qu'il s'agisse de données biométriques ou associées. Il faut donc bien faire la distinction entre les différentes fonctions de vérification et d'identification[9]. Celles-ci sont les instruments au service de cette finalité. Ce sont les finalités du système qui déterminent le choix d'installation d'un système d'identification ou de vérification. Le Comité ne peut pas se prononcer de façon générale en faveur de l'un ou de l'autre système. Il doit se borner à rappeler que si un processus de vérification est suffisant aux fins de la finalité choisie, l'installation d'un système d'identification requiert une justification particulière.

Caractère non excessif

63. Les données biométriques ont ceci de particulier qu'elles contiennent souvent plus d'informations que celles qui sont nécessaires à la vérification ou l'identification des personnes (article 5, lettre c). Il est possible d'éviter le traitement des données en excès en limitant le stockage et l'utilisation des données biométriques, pendant la phase d'enrôlement et la collecte secondaire, à une extraction qui répond aussi bien à la finalité du système. Le

[9] Pour une description de la distinction entre vérification et identification, se reporter au paragraphe 2, description des technicités.

terme technique utilisé pour cette extraction est « gabarit ». Le gabarit doit être conçu de telle sorte que les données obtenues ne révèlent que les informations nécessaires à la finalité du système. En particulier, il doit éviter tout lien possible avec des données à caractère sensible. Un exemple peut être utilement cité : l'image de l'iris peut révéler certaines maladies, informations qui ne sont pas nécessaires à la reconnaissance d'un individu. Le gabarit doit être conçu de telle façon qu'il ne contienne pas ces informations superflues.

64. Un gabarit peut être comparé à une liste de mots-clés extraits d'un texte qui n'est lui-même pas conservé. Il suffit que les mots-clés correspondent à ceux produits après le traitement ultérieur du même texte. Ainsi, le gabarit extrait de l'image biométrique au cours de la collecte supplémentaire peut être comparé au gabarit enrôlé chaque fois que le système est utilisé. La notion de« données biométrique » englobe l'image biométrique et le gabarit qui en est extrait.

65. Du point de vue de la protection des données, l'autre avantage de ce gabarit est que l'image originale de la caractéristique biométrique ne peut pas être reconstruite, tout comme un texte ne peut pas être reconstruit à partir de mots-clés. Si l'on ne relève qu'une partie d'empreinte digitale et si cette partie ne contient pas toutes les caractéristiques extraites, la personne ne peut pas être identifiée au moyen du gabarit préalablement enrôlé. Il sera nécessaire, dans le but d'identifier de possibles malfaiteurs, de posséder une image biométrique complète. Pour de nombreuses autres finalités, un gabarit s'avère suffisant.

66. La notion de caractère non excessif intervient aussi pour la collecte et le stockage des données associées. Seules doivent être stockées - et pas plus longtemps que nécessaire - les données associées nécessaires à la finalité de la collecte. C'est pourquoi la finalité du traitement des données associées, faisant partie de l'architecture du système, doit être précisée dès le départ.

Exactitude et probabilité

67. Les données à caractère personnel doivent être exactes (article 5, lettre d). L'une des caractéristiques du traitement des données biométriques est qu'il recèle un élément de probabilité inévitable. En effet, le résultat du traitement peut être faux même si toutes les données stockées sont exactes. Ce paradoxe mérite une explication.

68. De temps en temps et même si le système fonctionne parfaitement, il est inévitable que les deux caractéristiques d'une même personne ne correspondent pas. Quelqu'un sera donc rejeté à tort. Dans le même ordre d'idée, le système pourrait accepter le degré de probabilité entre deux caractéristiques bien qu'elles appartiennent à différentes personnes. Quelqu'un sera dans ce cas accepté à tort.

69. Il a été dit que les données biométriques ont un caractère unique et permanent (cf. paragraphe 28). Des exceptions sont toutefois possibles. Les individus qui vieillissent peuvent changer de caractéristiques biométriques. Les maladies, les accidents ou la chirurgie peuvent affecter les caractéristiques biométriques en question et entraîner un dysfonctionnement du système biométrique par rapport à une personne donnée. On ne peut plus considérer les données enrôlées comme étant exactes aux vues de la finalité qu'elles doivent servir.

70. Si les données n'atteignent pas un degré adéquat d'exactitude ou de similarité, un droit de rectification devrait être accordé à la personne concernée à sa demande.

Conservation des données

71. Les données à caractère personnel ne doivent pas être conservées pendant une durée excédant celle nécessaire aux finalités pour lesquelles elles sont enregistrées (article 5, lettre e). En ce qui concerne les données biométriques, cette exigence semble peu problématique. Tant que le système remplit sa fonction, les données biométriques enrôlées seront conservées sur un support de stockage, quel qu'il soit. L'article 5, lettre e évoque en général la possibilité de conservation des données sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées. A l'égard des données biométriques, l'option consistant à anonymiser les données n'est pas valable étant donné que les données biométriques de part leur nature propre, sont un instrument d'identification des individus, particulièrement lorsqu'elles sont traitées automatiquement.

72. Les données obtenues lors de la collecte secondaire ne seront d'aucune utilité après qu'elles aient été comparées avec les données enrôlées. Elles ne seront en principe pas stockées, mais immédiatement effacées. Le stockage des données présentées pour une collecte secondaire ne pourra être justifié que dans des cas exceptionnels, lorsqu'il existe des raisons valables de soupçonner une fraude à l'identité.

73. Plus problématique pourrait être la question de la conservation des données associées (voir paragraphe 59), qui ont différentes fonctions. Pour protéger des zones à niveau de sécurité élevé, par exemple une centrale nucléaire, il pourrait sembler légitime que le système puisse détecter avec précision qui a pénétré dans certaines zones, quand et pendant combien de temps. Ces données ont cette fonction première. D'autres systèmes peuvent avoir une autre finalité, par exemple d'établir que le détenteur d'une pièce d'identité en est bien le titulaire légitime. Ces données peuvent être utiles pour vérifier que le système, dans son ensemble, fonctionne correctement. On pourrait imaginer un système capable de détecter si des données biométriques identiques sont utilisées pendant un laps de temps dans des zones géographiquement distantes. Si tel était le cas, il pourrait s'agir d'une duplication de données, voire d'une fraude. Une telle finalité secondaire pourrait être jugée compatible avec la finalité première. L'article 5, lettre b de la Convention 108 permet de conserver les données associées pour de telles finalités secondaires. Dans le cas d'une utilisation primaire et secondaire, le système doit pouvoir spécifier et expliciter la durée de la conservation des données associées par rapport à la finalité pour laquelle elles ont été enregistrées. La conservation de données associées à des fins incompatibles avec la finalité de la collecte est interdite. Une dérogation n'est possible que si les conditions de l'article 9 de la Convention sont remplies.

Données sensibles

74. Les données biométriques peuvent révéler des maladies ou une origine raciale. L'article 6 les classe dans les « catégories particulières de données » qui exigent des garanties appropriées. Dans la doctrine de la protection des données, elles sont désignées sous le nom de données sensibles. Le progrès technique pourrait également donner la possibilité d'extraire beaucoup plus d'informations des données biométriques que ce qu'on aurait pu imaginer. En général, ces nouvelles informations ne correspondent pas à la finalité pour laquelle les données ont été collectées. Le Comité reconnaît que dans de telles circonstances, le traitement des données biométriques implique le traitement inévitable de données qui ne sont pas nécessaires, une situation comparable à celle que l'on rencontre lorsqu'un nom révèle l'origine ethnique. De nombreux systèmes biométriques extraient des

données de l'image biométrique d'origine, pendant l'enrôlement et lors de la capture ultérieure des données. Seules ces données extraites font l'objet d'une comparaison. Le choix des données à extraire doit être effectué de manière à éviter la collecte de telles données sensibles car, en général, ces données ne permettront pas de vérifier l'identité de la personne concernée ou de l'identifier.

Sécurité des données

75. L'article 7 traite du devoir de prévoir des mesures de sécurité appropriées protégeant les données à caractère personnel. Les normes de qualité du logiciel et du matériel pourraient être définies par le secteur industriel, en particulier les applications à grande échelle et les systèmes qui exigent un niveau de sécurité élevé. Les autorités de protection des données devraient veiller à ce que les standards techniques englobent les aspects nécessaires relatifs à l'application de la Convention. La formation du personnel utilisant le système et les équipements est un autre facteur important à prendre en compte. Elle devrait inclure une sensibilisation du personnel au fonctionnement du système.

76. Par la suite, ces standards et les systèmes qui les appliquent devraient faire régulièrement l'objet d'un audit et d'une évaluation, le cas échéant par un organisme indépendant, en tenant compte de toutes les parties du système, comme l'enrôlement, les données conservées, le processus de comparaison des données enrôlées et des données présentées, le cryptage des différentes phases, le personnel affecté à son fonctionnement etc.

77. Une mesure de protection générale, applicable également aux données biométriques, consiste à utiliser des algorithmes fiables pour extraire un gabarit d'une image biométrique et comparer les données enrôlées avec celles soumises par la suite. La transparence de ces algorithmes fait actuellement l'objet d'un débat entre autres en vue de leur interopérabilité. L'utilisation du cryptage est recommandée pendant le processus d'enrôlement pour éviter que des personnes non autorisées puissent accéder aux données brutes et les utiliser pour usurper l'identité de l'utilisateur légitime. Le cryptage sophistiqué des données biométriques pendant le processus d'enrôlement, pour le stockage et la transmission sur des lignes de télécommunication renforce la sécurité et rend plus difficile l'usage non autorisé des données biométriques. Quiconque intercepterait le signal crypté et ne disposerait pas de la clé de cryptage ne pourrait pas reconstruire le signal de réponse du système biométrique.

Transparence

78. L'existence d'un système utilisant les données biométriques, la finalité du système et l'identité et la résidence du responsable de traitement doivent être communiquées sur demande, non seulement à la personne concernée, mais au public en général (article 8, lettre a). Des problèmes particuliers peuvent se poser quant à la notion de finalité. Dans certains cas, un système assurera d'autres finalités, certaines évidentes, d'autres non. Dans de telles circonstances, il serait recommandable que le responsable de traitement prenne l'initiative d'informer les personnes concernées et le public sur le système, les finalités pour lesquelles les données personnelles sont utilisées, la manière dont elles sont utilisées et les risques éventuels. Dans d'autres cas, le principe de transparence peut être satisfait en fournissant les informations sur demande.

79. Toute dérogation à la transparence concernant les finalités, quelles qu'elles soient, doit être, conformément à l'article 9 de la Convention 108, prévue par la loi et rendue

nécessaire dans une société démocratique, dans l'intérêt, par exemple, de la sûreté publique.

Droit d'accès

80. Toute personne peut accéder aux données biométriques qui la concernent (article 8, lettre b, Convention 108). Ce droit s'applique aussi bien aux données biométriques qu'aux données associées qui révèlent, intentionnellement ou non, des informations sur la personne concernée. Il pourrait être dans l'intérêt d'une personne concernée de vérifier les données biométriques que le système associe à son identité, car il n'est pas exclu qu'elles puissent avoir été détériorées ou falsifiées, entraînant de ce fait de faux rejets. Dans ce cas, à la demande de la personne concernée, une recherche doit être effectuée sur les données biométriques se rapportant à son nom.

81. La personne concernée peut faire valoir que les données biométriques ou les gabarits enregistrés ne correspondent pas ou plus aux données biométriques qu'elle introduit à chaque fois qu'elle utilise le système, et que cela entraîne un taux de faux rejets plus élevé que la moyenne. Ceci peut être la conséquence d'altérations des caractéristiques biométriques dues au vieillissement, à une intervention chirurgicale ou à un accident de la personne concernée, qui ont entraîné un changement durable de ses caractéristiques biométrique. Le Comité est d'avis que le droit d'accès implique la vérification d'une telle plainte. La personne concernée n'a pas besoin de justifier sa demande.

82. La personne concernée a le droit d'accéder à ses données sous une « forme intelligible ». Accorder le droit d'accès aux données biométriques supposera souvent qu'une machine capable de lire les données biométriques soit à disposition. De même cela pourrait nécessiter un expert pour interpréter et vérifier les données. Le Comité estime que le responsable de traitement ne devrait pas pouvoir refuser de telles demandes au seul motif qu'une machine ou un expert ne sont pas disponibles.

83. Le Comité a examiné la possibilité d'un recours abusif au droit d'accès. Dans une certaine mesure, l'article 8, lettre b, de la Convention 108 traite de ce sujet. Les demandes d'accès excessivement fréquentes peuvent être rejetées, car seules les demandes effectuées « à des intervalles raisonnables » doivent être accordées. On peut également imaginer d'autres formes de demandes abusives. Le Comité considère que les principes généraux du droit, qui ne se limitent pas au domaine de la protection des données, s'appliquent à la doctrine de l'abus de droits et de demande d'indemnités.

84. Dans certains cas, s'il a des raisons valables de suspecter une usurpation d'identité, le responsable de traitement devrait faire son possible pour faire des recherches sur le cas d'espèce.

85. Dans la pratique, cette recherche ne peut, bien entendu, aboutir que si le responsable de traitement a lui-même accès à ces données. Il est possible que ce ne soit pas le cas (se reporter au chapitre III concernant le stockage des données sur un support de stockage particulier). Mais la personne concernée peut tout de même présenter une demande de vérification, si elle a des raisons de croire que quelqu'un usurpe ses données biométriques dans le système. Le Comité estime alors que le responsable de traitement a l'obligation de prendre les mesures nécessaires pour garantir l'exactitude des données. Une piste possible à cette fin peut être l'utilisation des données associées pour détecter une éventuelle fraude.

Droit de rectification et d'effacement

86. Les données biométriques ou données associées peuvent s'avérer inexactes. Dans ce cas, la personne concernée peut demander leur rectification ou leur effacement (article 8, lettre c).

87. L'exactitude des données doit être jugée par rapport aux finalités pour lesquelles elles ont été collectées. Lorsque les données sont uniquement utilisées pour accorder l'accès à un bâtiment, sans stockage ultérieur des données associées liées aux individus, le responsable de traitement pourrait légitimement accepter un degré plus élevé de probabilité de fausse acceptation ou de faux rejet, par exemple pour éviter que le système ne devienne excessivement coûteux.

88. Le degré de probabilité joue un rôle à la fois dans la phase d'enrôlement et dans l'utilisation subséquente du système. Au cours de la phase d'enrôlement, l'algorithme servant à extraire le gabarit de la caractéristique biométrique peut être plus ou moins étendu selon la finalité du système. Un algorithme moins étendu va accroître la probabilité de fausses acceptations ou de faux rejets puisque le gabarit sera moins spécifique. Au cours des utilisations ultérieures, le système peut être réglé pour une comparaison plus ou moins approfondie entre l'image ou le gabarit enrôlé et la donnée biométrique présentée. Le Comité est d'avis que c'est en premier lieu le responsable de traitement qui décide du degré de probabilité que le système doit admettre compte tenu de ses finalités. La personne concernée ne peut exiger une certitude absolue – l'absolu étant irréalisable – mais approcher cette certitude autant que cela est rendu possible par la technique.

89. Le caractère par essence probabiliste de l'utilisation et de la correspondance des données biométriques a parfois pour conséquence inévitable de lier les données associées à une personne qui n'est pas concernée. Si c'est le cas, l'interprétation de ces données pour les besoins d'un individu doit prendre ce fait en compte. La correspondance (l'acceptation) ou la non correspondance (le rejet) n'étant jamais garanties à cent pour cent, il en va de même pour les données associées liées à une personne concernée particulière. Le degré de probabilité reste le même.

90. Ceci soulève des problèmes particuliers dans un système dans lequel les données sont utilisées pour contrôler systématiquement le comportement d'une personne, ce qui pourrait être justifié, par exemple, dans une zone très protégée où il est nécessaire de savoir qui était là, quand et pendant combien de temps. Le système doit donc fournir un degré de précision plus élevé. En ce qui concerne les données biométriques, il en découle que la probabilité d'une fausse acceptation ou d'un faux rejet est assez faible.

91. L'exactitude de la « reconnaissance » de la personne concernée de même, ne doit pas être tenue pour acquise. La personne concernée ne doit pas attendre qu'elle soit rigoureusement exacte. On pourrait ajouter en corollaire que le fait de trouver des données associées inexactes ne signifie pas que le responsable de traitement a agi illégalement, ce qui ouvrirait un droit à l'indemnisation.

92. Lié au droit de rectification est le droit d'effacement, qui intervient si les données biométriques sont stockées contrairement à la loi.

93. En ce qui concerne les données biométriques, il est possible qu'un conflit survienne entre le responsable de traitement et la personne concernée à propos du degré acceptable de

probabilité des faux rejets. Si la personne concernée demande un nouvel enrôlement alors que le responsable de traitement n'admet pas que les données sont inexactes, le droit à la rectification pourrait être interprété comme donnant droit en principe à un nouvel enrôlement par la personne concernée sans coûts excessifs. Il en va de même si des données enrôlées étaient correctes, mais que la caractéristique biométrique a été modifiée avec l'âge, un accident ou de la chirurgie. Au fil du temps, les données sont devenues graduellement incorrectes.

Recours effectif

94. Chacun a le droit à un recours effectif lorsque le droit à la transparence, à l'accès, à la rectification ou à l'effacement n'est pas respecté (article 8, lettre d, de la Convention 108). Pour ce qui est des données biométriques, on pourrait imaginer une définition plus complète de ce droit. Il a été plusieurs fois mentionné que la nature probabiliste de l'usage des données biométriques est la cause de problèmes spécifiques liés à la protection des données. Le choix d'utiliser un système biométrique est un risque assumé par le responsable de traitement. Ce n'est pas à la personne concernée de supporter les inconvénients possibles de tels systèmes. En fonction des circonstances, la personne concernée devrait soit avoir la possibilité de voir sa situation corrigée immédiatement, soit avoir accès à un recours dès que possible.

95. Un individu peut ne pas être « reconnu » par un système biométrique. Les causes peuvent être diverses, par exemple :

> (a) La personne n'est pas la même que celle dont les données biométriques sont enregistrées. Le résultat est exact. Les données ne correspondent pas et le système rejette la personne concernée.
> (b) Le système contient de fausses données biométriques. Les données doivent être rectifiées.
> (c) Les données sont exactes mais la collecte secondaire ne fonctionne pas correctement et la mise en correspondance des données biométriques n'aboutit pas. La machine doit être réglée.
> (d) Le système fonctionne parfaitement et les données sont exactes. Néanmoins, le système ne trouve pas de correspondance à cause de la nature probabiliste de l'opération de mise en correspondance.

96. On pourrait penser à bien d'autres cas. La comparaison des données soumises avec les données enrôlées peut à tort s'avérer être juste. La correspondance fait apparaître la personne concernée comme faisant partie d'une liste de personnes non autorisées alors que ce n'est pas le cas.

97. Dans toutes ces situations, un individu doit pouvoir demander un réexamen. Dans le cas (a), le rejet sera confirmé. Dans tous les autres cas, le résultat automatisé doit être corrigé. En dernier ressort, la personne concernée devrait pouvoir s'adresser à un être humain qui, au nom du responsable de traitement, décide si la personne concernée doit être rejetée ou acceptée[10]. La procédure de ce recours ne doit pas être excessivement contraignante pour la personne concernée. Le droit de recours doit également s'appliquer aux personnes qui ne peuvent pas utiliser le système à cause d'un handicap physique. Quelqu'un qui n'a pas de mains ne peut pas être accepté par un système qui fonctionne avec un lecteur

[10] Se reporter à l'article 15 de la directive 95/46 de l'UE sur la protection des données personnelles.

d'empreintes digitales. Le responsable de traitement doit veiller à ce que ces personnes disposent d'une autre solution sans compromettre le niveau de sécurité visé.

98. Dans l'éventualité où la personne concernée et le responsable de traitement auraient un désaccord durable, ils peuvent s'adresser à l'autorité de contrôle aux termes du Protocole additionnel à la Convention 108.

Pertinence de l'article 9 de la Convention sur les systèmes biométriques

99. L'article 9, paragraphe 2 de la Convention prévoit des dérogations aux principes mentionnés ci-dessus dans certaines limites. Ce paragraphe s'inspire de l'article 8, paragraphe 2 de la Convention Européenne des droits de l'Homme (CEDH).

100. La collecte de données à caractère personnel qu'elles soient biométriques ou associées et leur traitement ultérieur peuvent porter atteinte à la vie privée. Une telle interférence est interdite par l'article 8, paragraphe 1, de la CEDH, sauf si elle est justifiée conformément à l'article 8 paragraphe 2. Si des données biométriques sont traitées, les principes de la Convention 108 s'appliquent, que la vie privée soit en jeu ou non. Ces opérations ne sont possibles que si les critères et les procédures conformes au paragraphe 2 s'appliquent. Une dérogation aux principes de la Convention 108 est possible seulement si les critères de l'article 9, lettre 2 s'appliquent. Ces critères sont similaires à ceux de l'article 8, lettre 2 de la CEDH.

101. Dans l'arrêt Rotaru c. Roumanie de mai 2000, la Cour européenne des Droits de l'Homme estime que la collecte secrète de données à caractère personnel pour des raisons de sécurité d'Etat pouvaient interférer avec la vie privée. La Cour a ainsi appliqué les critères de l'article 8, lettre 2 de la CEDH. Dans son arrêt, la Cour estime que les catégories de personnes auxquelles ces atteintes à la vie privée s'appliquent et la nature des données qui peuvent être consignées doivent être définies au préalable d'une manière précise et prévisible en accord avec les critères légaux. La dérogation au droit général à la protection de la vie privée est donc rendue visible. Il a parfois été admis qu'aucune interférence avec la vie privée de la personne concernée n'avait eu lieu dans la mesure où cette dernière ne le remarquait pas. L'arrêt Rotaru c. Roumanie fait clairement apparaître le caractère non valable de cet argument.

102. L'arrêt Rotaru c. Roumanie à l'égard de l'article 8, lettre 2 de la CEDH pourrait avoir des implications dans l'interprétation de l'article 9, lettre 2 de la Convention 108. Le traitement des données biométriques et les différentes catégories de données à caractère personnel associées, la finalité de leur collecte et l'identité du responsable de traitement devraient en principe être des informations transparentes pour la personne concernée. De nouvelles technologies telles que la reconnaissance faciale permettent la recherche immédiate de malfaiteurs recherchés constituerait une forme de traitement sans stockage des données de toutes les personnes identifiées qui ne durerait que les quelques secondes nécessaires à effectuer la vérification. Néanmoins, cette forme de traitement serait couverte par la Convention 108. Le traitement secret de ces données serait en effet contraire au principe de traitement loyal des données et ne devrait donc être autorisé que si les critères de l'article 9 sont remplis.

103. Prenons un exemple pour illustrer ce point de vue. Malgré les essais infructueux à ce jour, il n'est pas exclu que, dans un avenir proche, la technique permette d'identifier les individus qui marchent dans le rue en comparant leurs visages avec une liste de personnes

recherchées. En effet, il sera bientôt possible d'extraire des informations numérisées à partir d'images, dans le but de les comparer avec des bases de données. L'enrôlement pourrait consister à prendre des photos d'un criminel après son arrestation. Celles-ci pourraient être comparées aux images produites par la vidéosurveillance des citoyens qui marchent dans la rue. Dans la pratique, cette vidéosurveillance pourrait être effectuée secrètement. Mais ceci constituant un traitement déloyal, elle ne devrait être permise que si les critères de l'article 9 de la Convention étaient remplis, rendant nécessaire l'adoption d'une loi décrivant précisément les exceptions admises à la règle général du traitement loyal.

104. Certains font valoir une utilisation secondaire de données associées venant de systèmes utilisant des données biométriques dont la compatibilité avec la finalité pour laquelle elles ont été collectées serait discutable. Par exemple, il pourrait être dans l'intérêt des services de renseignement de conserver ces données dans le but de surveiller des personnes qu'ils pensent capables de commettre des actes terroristes. Souvent, cette conservation sera incompatible avec la finalité d'origine, de collecte de ces données. L'article 9 de la Convention 108 donne la possibilité d'une telle conservation dans une société démocratique pour des raisons de sûreté publique. Si cela est nécessaire, des dérogations au critère de compatibilité peuvent être inscrites dans une loi qui définirait la manière dont de telles données peuvent être utilisées pour cette nouvelle finalité.

105. L'article 8, lettre 2 de la CEDH et l'article 9 de la Convention 108 sont des exceptions justifiant une interférence aux principes énoncés dans ces deux conventions. Une interférence limitée dans la vie privée ou une dérogation limitée aux règles de la Convention 108 ne créerait pas d'entorse à ces principes. Une surveillance secrète générale du public, même prévue par la loi, ne serait ni conforme aux dispositions de la Convention européenne des droits de l'homme, ni à celles de la Convention 108.

Conclusions du rapport d'étape

106. Le Comité a tenu des échanges préliminaires sur certaines questions posées par la biométrie dans son rapport avec les principes de la protection des données, tels qu'ils sont énoncés dans la Convention 108. De nombreuses questions restent ouvertes. Malgré les évolutions technologiques considérables qui ont vu le jour depuis la rédaction de la Convention, le Comité a estimé que ses principes demeurent pertinents et peuvent s'appliquer aux systèmes qui utilisent la biométrie. Le présent rapport traduit la pertinence des principes juridiques à l'égard de ces nouvelles techniques. Il vise à contribuer au débat sur la relation qui existe entre les droits de l'homme et la biométrie au niveau national et international. Le Comité se propose d'actualiser le présent rapport ou de publier d'autres rapports si des faits nouveaux le rendent nécessaire, voire de rédiger de nouveaux instruments juridiques

107. A ce stade, le Comité souligne en particulier les points suivants :

1. Les données biométriques doivent être considérées comme une catégorie spécifique des données dans la mesure où elles émanent du corps humain, restent les mêmes dans différents systèmes et sont inaltérables à vie. Toutefois, elles peuvent s'altérer par exemple par le vieillissement ou une intervention chirurgicale.

2. Avant de recourir à la biométrie, le responsable de traitement devrait évaluer, d'une part les avantages et inconvénients possibles pour la vie privée de la

personne concernée et d'autre part les finalités envisagées, et prendre en compte de possibles solutions alternatives, portant une atteinte moindre à la vie privée.

3. La biométrie ne devrait pas être choisie uniquement parce qu'elle est pratique à utiliser. En effet, l'utilisation de la biométrie peut porter atteinte à la dignité humaine. Il faut prendre en compte les aspects socio-culturels et les réticences possibles à l'égard de l'utilisation instrumentale du corps humain.

4. Les données biométriques et toutes données associées générées par le système doivent être utilisées à des fins déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités.

5. Les données devraient être adéquates, pertinentes et non excessives par rapport à la finalité du traitement. Un système de traitement des données devrait être configuré de façon à exclure la collecte et le traitement de plus de données biométriques ou associées que sa finalité ne l'exige. Si des gabarits sont suffisants, la collecte ou le stockage de l'image biométrique devrait être évité.

6. Dans le choix de l'architecture du système, le responsable de traitement devrait mettre en balance d'une part les avantages et les inconvénients pour la vie privée de la personne concernée et d'autre part les finalités envisagées. Un choix raisonné devrait être opéré entre le stockage uniquement sur un support de stockage individuel, dans une base de données décentralisée ou dans une base de données centralisée, tout en gardant à l'esprit les aspects de sécurité.

7. L'architecture d'un système biométrique ne devrait pas être disproportionnée par rapport à la finalité du traitement. Ainsi, si la vérification suffit, le responsable de traitement ne devrait pas développer une solution d'identification. Les données biométriques qui sont uniquement utilisées à des fins de vérification devraient être stockées de préférence sur un support individuel sécurisé de stockage, par exemple une carte à puce, que détiendrait uniquement la personne concernée.

8. La personne concernée devrait être informée de la finalité du système et de l'identité du responsable de traitement, ainsi que des données traitées et des catégories de personnes auxquelles ces données seront communiquées dans la mesure où ces informations sont nécessaires pour garantir la loyauté du traitement.

9. La personne concernée a un droit d'accès, de rectification, de blocage et d'effacement de ses données. Ces droits s'étendent aux données biométriques faisant l'objet d'un traitement automatisé et nominatif, aux possibles données associées (comme la date et localisation de l'utilisation du système), et aux personnes à qui elles ont été communiquées.

10. Le responsable de traitement doit prévoir des mesures techniques et organisationnelles appropriées afin de protéger les données biométriques et les autres données à caractère personnel qui y sont associées contre la destruction – accidentelle ou illicite – et la perte accidentelle, ainsi que contre l'accès, la modification, la communication non autorisés ou toute autre forme de traitement illicite.

11. Une procédure de certification et de contrôle devrait être développée, en particulier dans le cas des applications de masse, dans le but d'établir des normes de qualité pour les logiciels, le matériel et pour la formation du personnel responsable de l'enrôlement et de la vérification. Un audit régulier testant les performances du système est recommandé.

12. Si une personne concernée enrôlée dans un système biométrique est rejetée, le responsable de traitement devrait, à sa demande, réexaminer le cas et, si nécessaire, lui proposer des solutions de remplacement appropriées. Des procédures devraient être établies afin d'informer la personne concernée lors d'une prétendue non reconnaissance par le système.

T-PD, février 2005