



Doc. 12522

16 février 2011

La nécessité de mener une réflexion mondiale sur les implications de la biométrie pour les droits de l'homme

Rapport¹

Commission des questions juridiques et des droits de l'homme

Rapporteur: M. Holger HAIBACH, Allemagne, Groupe du Parti populaire européen (PPE/DC)

Résumé

Depuis les attentats du 11 septembre 2001, la question de la sécurité, et par conséquent celle de l'identification et de la vérification des individus, est devenue une priorité mondiale. Ainsi, le recours à la biométrie devient de plus en plus fréquent. La commission des questions juridiques et des droits de l'homme est de plus en plus préoccupée par le développement rapide et non contrôlé des technologies biométriques. Elle souligne qu'il faut assurer correctement un équilibre entre la sécurité et la protection des droits de l'homme et des libertés fondamentales, notamment le droit à la vie privée.

Etant donné qu'au niveau européen le cadre juridique concernant l'utilisation des données biométriques reste imprécis, les Etats membres du Conseil de l'Europe devraient prendre davantage de mesures pour l'améliorer. Ils devraient notamment adopter une législation spécifique portant sur ce domaine, formuler une définition uniforme de la notion de «données biométriques», mettre en place des organes de contrôle et promouvoir une recherche multidisciplinaire.

Le Comité des Ministres pourrait notamment réviser la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel afin de l'adapter aux défis liés au développement des technologies biométriques.

1. 2011 - Commission permanente de mars



Sommaire

Page

A. Projet de résolution	3
B. Projet de recommandation	5
C. Exposé des motifs, par M. Haibach, rapporteur	6
1. Introduction	6
2. Que recouvre la notion de «biométrie»?	6
3. Quelles sont les différentes applications des données biométriques?	7
4. Risques de fraude et de falsification	8
5. Principales préoccupations en matière de biométrie vis-à-vis des droits de l'homme	8
5.1. La dignité humaine	9
5.2. Le droit au respect de la vie privée (article 8 de la Convention européenne des droits de l'homme)	9
5.3. L'interdiction de toute discrimination (article 14 de la Convention)	9
5.4. Le droit à un procès équitable (article 6 de la Convention)	10
5.5. La liberté de circulation (article 2 du Protocole no 4 à la Convention)	11
6. Dispositions juridiques	11
6.1. Au niveau mondial: les Nations Unies	11
6.2. Au niveau régional (européen)	11
6.3. Au niveau national	15
7. Conclusions	16

A. Projet de résolution²

1. Depuis les événements du 11 septembre 2001, la question de la sécurité est devenue une priorité mondiale. Depuis lors, on assiste à une recherche permanente de méthodes sûres et fiables d'identification et de vérification des données personnelles intrinsèques de chaque individu par le recours à la biométrie. Grâce à leur évolution rapide, les technologies biométriques offrent des solutions possibles à divers problèmes sécuritaires, mais peuvent également porter atteinte à un certain nombre de droits de l'homme, tels que le droit au respect de la vie privée, le droit à un procès équitable et à la présomption d'innocence, ou encore le droit à la liberté de circulation et à la non-discrimination – autant de droits inscrits dans la Convention européenne des droits de l'homme (STE no 5).
2. L'Assemblée parlementaire note qu'il y a un besoin d'assurer correctement un équilibre entre la sécurité et la protection des droits de l'homme et des libertés fondamentales, y inclus le droit à la vie privée. La large portée technique de la biométrie, son évolution rapide et la volonté des Etats membres d'y recourir à des fins multiples peuvent ne pas être reflétées de manière appropriée dans la législation des Etats membres pour sauvegarder les droits de l'homme. Lorsqu'une nouvelle technologie est utilisée au quotidien, il devient plus difficile de mettre en œuvre, voire d'adopter, un cadre juridique approprié. Ainsi, les Etats membres devraient traiter des questions juridiques concernant la biométrie dans les meilleurs délais.
3. Au niveau européen, le cadre juridique existant reste imprécis, car il n'existe aucune définition communément acceptée de la notion de «données biométriques». Ainsi, l'Assemblée est convaincue que le Conseil de l'Europe lui-même devrait prendre des mesures visant à améliorer et moderniser ce cadre juridique.
4. L'Assemblée invite, par conséquent, les Etats membres:
 - 4.1. à adopter une législation spécifique sur l'utilisation des technologies biométriques, afin de protéger les individus de toute violation des droits inscrits dans la Convention européenne des droits de l'homme et autres instruments de protection des droits de l'homme, plus particulièrement en vue:
 - 4.1.1. de formuler une définition uniforme de la notion de «données biométriques»;
 - 4.1.2. de réviser les règles en matière de protection générale des données à caractère personnel, en vue de les adapter aux applications actuelles de technologies biométriques renforcées;
 - 4.2. à réexaminer en permanence leur législation afin de pouvoir répondre aux défis du développement des technologies biométriques, y compris la biométrie dite «de deuxième génération»;
 - 4.3. à promouvoir le principe de proportionnalité en matière d'utilisation de données biométriques, notamment:
 - 4.3.1. en limitant au strict nécessaire l'évaluation, le traitement et le stockage de ces données, en d'autres termes, en limitant ces processus aux cas où le gain en termes de sécurité serait plus important qu'une éventuelle ingérence dans les droits de l'homme, et si le recours à d'autres techniques moins intrusives est insuffisant;
 - 4.3.2. en proposant d'autres modes d'identification et de vérification à toutes les personnes qui sont dans l'incapacité ou refusent de fournir des données biométriques;
 - 4.3.3. en travaillant sur des données formatées plutôt que sur des données biométriques à l'état brut, dans la mesure du possible;
 - 4.3.4. en renforçant la transparence et en faisant une condition préalable au consentement des personnes, et, le cas échéant, en facilitant la révocation de ce consentement;
 - 4.3.5. en permettant à tout individu d'accéder à ses données personnelles et/ou d'en demander l'effacement;
 - 4.3.6. en prévoyant des systèmes de stockage appropriés, notamment en réduisant au strict minimum la possibilité d'un regroupement central des données;
 - 4.3.7. en faisant en sorte que les données biométriques ne soient utilisées que pour les objectifs pour lesquels elles ont été collectées conformément à la loi, et en empêchant leur diffusion ou tout accès non autorisés;

2. Projet de résolution adopté à l'unanimité par la commission le 16 décembre 2010.

- 4.4. à mettre en place, en fonction des besoins, des organes de contrôle de l'application de la législation pertinente, et à garantir, pour tout individu, des recours effectifs en cas de violation de ses droits et libertés fondamentales;
- 4.5. à renforcer le respect, par le secteur privé, de la législation en vigueur en matière de protection des données personnelles en cas d'application des technologies biométriques, notamment:
 - 4.5.1. en garantissant la responsabilité des contrôleurs de données;
 - 4.5.2. en promouvant la formation des acteurs concernés à un traitement approprié des données personnelles;
- 4.6. à promouvoir une recherche multidisciplinaire dans le domaine des nouvelles technologies biométriques, afin de garantir un équilibre entre la nécessité de renforcer la sécurité, d'une part, et le respect de la vie privée et de la dignité des êtres humains, ainsi que de la transparence, d'autre part;
- 4.7. à évaluer les risques potentiels, vis-à-vis des droits de l'homme et des libertés fondamentales, de l'utilisation de la biométrie, et à échanger les résultats obtenus dans chaque Etat membre.
5. L'Assemblée demande également aux Etats membres de développer la coopération internationale, notamment avec les Nations Unies, l'Organisation de coopération et de développement économiques et l'Union européenne, afin d'harmoniser les normes en matière de biométrie, en conformité avec les normes internationales dans le domaine des droits de l'homme.

B. Projet de recommandation³

1. L'Assemblée parlementaire fait observer que le Conseil de l'Europe a déjà manifesté son engagement en matière de protection des droits de l'homme dans le contexte de la protection des données, notamment par l'adoption de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE no 108), et grâce à l'action du comité consultatif de cette convention. Par conséquent, le Conseil de l'Europe est bien placé pour promouvoir l'adoption, au niveau européen, de règles d'utilisation de la biométrie.
2. Se référant à sa Résolution ... (2011), l'Assemblée invite le Comité des Ministres:
 - 2.1. à réviser la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, afin d'adapter cet instrument aux défis liés à l'émergence de nouvelles technologies, y compris les technologies biométriques, notamment par une définition de la notion de «données biométriques»;
 - 2.2. à élaborer des lignes directrices à l'intention des Etats membres, au sujet de cadres législatifs qui permettraient de trouver un juste équilibre entre les intérêts des différentes parties concernées, notamment la sécurité et le respect de la vie privée;
 - 2.3. à suivre l'évolution des technologies biométriques et à étudier leurs effets éventuels sur les droits de l'homme et les libertés fondamentales inscrits dans la Convention européenne des droits de l'homme et autres instruments du Conseil de l'Europe relatifs à la défense des droits de l'homme.
3. L'Assemblée recommande également que le Comité des Ministres développe sa coopération avec les Nations Unies, l'Organisation de coopération et de développement économiques et l'Union européenne, afin de comparer les règles en vigueur en matière de biométrie et de promouvoir des principes cohérents en ce qui concerne son utilisation.

3. Projet de recommandation adopté à l'unanimité par la commission le 16 décembre 2010.

C. Exposé des motifs, par M. Haibach, rapporteur

1. Introduction

1. Le 5 octobre 2006, l'Assemblée parlementaire a décidé de renvoyer pour rapport à la commission des questions juridiques et des droits de l'homme la proposition de recommandation sur la nécessité de mener une réflexion mondiale sur les implications de la biométrie pour les droits de l'homme (Doc. 11066). A sa réunion du 27 janvier 2009, la commission m'a nommé rapporteur.

2. A la suite des événements du 11 septembre 2001 et autres attaques terroristes, la question de la sécurité est devenue l'une des priorités mondiales et a mené à une recherche permanente de méthodes sûres et fiables d'identification et de vérification, en utilisant les traits intrinsèques de chaque individu tels que les images d'empreintes digitales et de la rétine, de l'ADN, ou encore l'enregistrement vocal, et, plus récemment, les scanners corporels. En l'absence de tout cadre juridique dans ce domaine, le développement rapide des technologies biométriques suscite certaines préoccupations en ce qui concerne la protection des droits de l'homme et des libertés fondamentales.

3. La «biométrie» est un système qui se fonde sur des caractéristiques individuelles mesurables – physiques ou physiologiques – ou des modes de comportement personnels, en vue de déterminer l'identité d'une personne ou de vérifier ses déclarations identitaires⁴. Par rapport à d'autres moyens d'authentification, tels que les badges et les mots de passe, les données biométriques réduisent les risques d'utilisation frauduleuse, dans la mesure où l'on peut difficilement les transmettre à des tiers, et où ce type de données ne repose guère sur les processus de vérification ou d'identification opérés par les personnels de sécurité, ces processus étant précisément le point faible des systèmes sécuritaires actuels. Par conséquent, les technologies utilisant les données biométriques pour confirmer l'identité alléguée d'un individu permettent à la fois d'améliorer la sécurité globale et de réduire le risque de fraude. Bien que les avantages de la biométrie en termes de sécurité soient indéniables, la multiplication des techniques biométriques soulève des problèmes sur le plan des droits de l'homme les plus fondamentaux, notamment celui de la protection des données en question. En soi, la collecte et l'évaluation des données biométriques ne constituent pas de véritable menace pour les droits des personnes, étant donné qu'aujourd'hui les opérations de photographie, de reproduction des empreintes digitales et autres techniques sont rapides et ne sont pas intrusives. En revanche, le traitement en masse et la centralisation de données à caractère personnel – tels qu'ils sont opérés, par exemple, dans le cadre de la base de données Eurodac en liaison avec les demandes d'asile dans les Etats membres de l'Union européenne⁵ – peuvent être une menace pour la vie privée, car l'intégrité du corps humain et la manière dont ce dernier est utilisé pour la collecte de données biométriques concernent la dignité de l'être humain.

4. Le présent rapport a pour but d'exposer les problèmes essentiels liés à la biométrie, tels que le sens même de la notion de biométrie, la collecte et la conservation concrètes des données biométriques, ainsi que les préoccupations que ces pratiques peuvent faire naître⁶. Le présent rapport se réfère également aux règles européennes en vigueur en matière de protection des données; enfin, le présent document envisage un certain nombre de recommandations en vue de combler les lacunes du cadre législatif actuel.

2. Que recouvre la notion de «biométrie»?

5. Les données biométriques sont des caractéristiques physiques ou comportementales individuelles et uniques, différentes chez chaque être humain et qui, dans la plupart des cas, restent inchangées tout au long de la vie. Il peut s'agir, par exemple, d'échantillons d'ADN, d'images d'empreintes digitales, de l'iris ou de la rétine, ou encore d'un enregistrement vocal, de la démarche de l'individu, ou du rythme dactylographique lors de la frappe d'un mot de passe.

4. Glossaire du Contrôleur européen de la protection des données, disponible sur:

www.edps.europa.eu/EDPSWEB/edps/lang/fr/EDPS/Dataprotection/Glossary/pid/72.

5. Le système «Eurodac» est issu du Règlement (CE) no 2725/2000 du Conseil européen, aux fins d'application de la Convention de Dublin. La base de données «Eurodac» contient un ensemble d'empreintes digitales de demandeurs d'asile et de ressortissants étrangers ayant traversé des frontières de manière illégale. Pour de plus amples informations sur Eurodac, consulter le site:

http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/133081_fr.htm.

6. Dans ce contexte, je voudrais remercier tout particulièrement, pour son aide, le professeur Paul de Hert, de la Vrije Universiteit de Bruxelles et de l'université de Tilburg. Le document d'information qu'il a élaboré a été la base de travail essentielle du présent rapport.

6. Les systèmes biométriques sont un moyen d'authentification très fiable, car ils permettent d'établir un lien étroit entre un individu et sa prétendue identité par la vérification de ses données biométriques physiques, qui sont uniques. En outre, ce type de système a des avantages sur le plan pratique et c'est ce qui le rend plus acceptable que d'autres techniques. En effet, par rapport aux longues opérations d'identification et de vérification effectuées par les personnels de sécurité, le scanning de l'iris ou du visage et les analyses comportementales sont des opérations rapides, même si les vérifications portent sur un nombre de personnes considérable. En dépit d'investissements de départ importants dans les équipements les plus récents, les technologies biométriques sont très rentables (elles évitent, par exemple, les frais dus aux oublis de mots de passe).

7. La biométrie dite de «première génération» (par exemple, empreintes digitales et lecture de l'iris) n'a suscité que peu de polémiques concernant le respect des droits de l'homme et, en particulier, les conditions de collecte des données et leur finalité. L'apparition ultérieure de données biométriques non techniques («*soft biometrics*»), qui incluent le sexe, le poids, la taille, l'âge et l'origine ethnique à des fins de classification automatisée, s'est révélée plus problématique, les critiques y voyant un risque de profilage social discriminatoire. La biométrie dite de «deuxième génération» vise à identifier une personne sur la base de son comportement ou de ses activités. Elle englobe des mesures de la fréquence cardiaque, de la température corporelle, de l'activité cérébrale et de la dilatation des pupilles – d'où la nécessité de nous interroger sur ce que nous entendons par «données à caractère personnel». Peut-être faudra-t-il également déterminer s'il y a lieu – et si oui, dans quelle mesure – de traiter ici la question des «scanners corporels» et de leur utilisation (éventuellement abusive). Le fait que ce type de données puisse être recueilli à l'insu d'un individu ne fait qu'ajouter à la controverse. Aujourd'hui, la vidéosurveillance permet de repérer des individus à distance et d'établir des profils individuels sans l'accord des personnes en question.

3. Quelles sont les différentes applications des données biométriques?

8. L'usage qui est fait de la biométrie varie selon les Etats membres du Conseil de l'Europe. Les systèmes biométriques ont l'un des deux objectifs suivants, ou les deux à la fois: l'identification d'une personne, exclusivement fondée sur les données biométriques, ou la vérification de l'identité d'une personne, processus consistant à soumettre le sujet à un ensemble d'éléments formatés. L'identification demande de nombreuses opérations de comparaison d'un élément avec plusieurs autres, tandis que le processus de vérification se limite à la comparaison d'un élément avec un autre. On peut opter pour divers types de stockage de données en fonction de l'objectif global du système. D'une manière générale, le processus d'identification risque bien plus de porter atteinte aux droits de l'homme que l'utilisation directe des données biométriques, car dans le processus d'identification ces données ne sont jamais sous le contrôle strict et entier de l'individu concerné.

9. Les applications les plus courantes de la biométrie se situent dans le domaine du contrôle de l'immigration: en l'occurrence, les techniques biométriques sont utilisées pour les passeports, le contrôle des frontières, les demandes de visa et la vérification de l'identité des demandeurs d'asile. En Europe, ces données sont centralisées et conservées dans de vastes bases de données telles que le Système d'information sur les visas de l'Union européenne et le Système d'information Schengen.

10. De plus, la plupart – sinon l'ensemble – des Etats membres du Conseil de l'Europe autorisent le prélèvement obligatoire d'empreintes digitales et d'échantillons de cellules dans le cadre de procédures pénales. Vingt Etats membres au moins ont pris des dispositions en vue du prélèvement de données ADN et de leur stockage dans des bases de données nationales ou sous d'autres formes (Allemagne, Autriche, Belgique, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Italie, Lettonie, Luxembourg, Norvège, Pays-Bas, Pologne, République tchèque, Suède et Suisse). Le nombre d'Etats prenant ce type de mesures est en constante augmentation.

11. Etant donné l'utilité du système biométrique, le secteur privé y a également recours et contribue à son expansion. Ainsi, les données biométriques sont utilisées pour contrôler l'accès à des établissements privés, tels que les casinos, les discothèques ou les clubs de sport et de remise en forme. Les compagnies d'assurances portent également un grand intérêt à la biométrie, car toute information concernant l'état de santé de leurs clients peut les renseigner sur le coût du risque. D'autre part, l'usage important qui est fait, aujourd'hui, des «cartes de fidélité» montre que les consommateurs sont tout à fait disposés à révéler leurs préférences personnelles, même s'ils ne sont pas toujours conscients que cela revient, dans une certaine mesure, à dévoiler des données personnelles.

12. A l'heure actuelle, la nécessité d'identifier très précisément les personnes, aussi bien dans la sphère publique que dans le secteur privé, rend inévitable le développement de ces nouvelles technologies. Dans la sphère publique, la biométrie est désormais un élément central des politiques nationales et internationales en

matière de sécurité et d'immigration. La lutte contre le terrorisme et contre la criminalité organisée englobe également l'utilisation des techniques scientifiques modernes d'investigation et d'identification. Dès lors, parallèlement à l'utilisation de systèmes biométriques pour le contrôle des frontières, les Etats créent de plus en plus d'importantes bases de données centralisées, contenant des données biométriques telles que des photographies faciales lisibles sur ordinateur, des empreintes digitales ou encore des profils ADN⁷. D'autre part, les systèmes biométriques gagnent également du terrain dans la sphère privée, car les fraudes liées à l'identité sont de plus en plus fréquentes dans le secteur croissant du commerce en ligne.

4. Risques de fraude et de falsification

13. Les données biométriques sont considérées comme très fiables; en ce qui concerne la plupart des systèmes biométriques visant à l'identification des personnes, il y a de fortes chances que, grâce à ce processus, on identifie effectivement la bonne personne.

14. Cependant, des erreurs dans l'un ou l'autre sens (identification positive ou négative erronée) sont toujours possibles, en raison des imperfections techniques de la biométrie. Le taux d'erreur est généralement de l'ordre de 0,5 à 1 %; en d'autres termes, il n'existe pas de résultat totalement positif ou totalement négatif en matière d'identification d'un individu. Il y a un risque d'identification ou de vérification erronée, par exemple dans de mauvaises conditions de lumière ou en cas de formation insuffisante des opérateurs. Enfin, des manipulations intentionnelles sont également possibles.

15. En principe, les caractéristiques biométriques restent inchangées pendant toute la durée d'une vie. Elles peuvent toutefois changer à la suite d'une intervention chirurgicale, d'un accident ou, tout simplement, en raison du vieillissement. Des études sur la viabilité à long terme des données biométriques ont montré que les empreintes digitales pouvaient évoluer avec le temps.

16. Les caractéristiques biométriques se modifient avec le développement corporel d'une personne et ne sont en fait pleinement développées qu'au début de l'âge adulte. De ce fait, la prise d'empreintes digitales d'un enfant pour l'établissement d'un passeport, ou pour contrôler l'accès à un établissement scolaire (comme cela se fait d'ores et déjà dans certaines écoles), augmente les risques d'erreur. Les enfants ne devraient pas être soumis à un contrôle biométrique tant que leurs caractéristiques biométriques ne sont pas pleinement développées et afin d'éviter une catégorisation prématurée, voire un processus discriminatoire à leur égard.

17. Enfin, se pose la question importante de la sécurité des données biométriques conservées. Les systèmes biométriques sont, entre autres, exposés au piratage, à la modification ou à la destruction non autorisées, à la falsification, à la perte involontaire et à la divulgation illicite de données. Il a été démontré que la falsification des données biométriques, et en particulier des empreintes digitales, était parfaitement possible. En outre, le recours à la biométrie n'exclut pas une falsification ou une usurpation d'identité, comme cela a été démontré dans le cas des nouveaux passeports électroniques mis en place dans un certain nombre d'Etats membres de l'Union européenne.

5. Principales préoccupations en matière de biométrie vis-à-vis des droits de l'homme

18. En matière de traitement de données personnelles, il importe de définir des garanties de protection des droits de l'homme. Certes, en principe, les techniques biométriques permettent de renforcer la sécurité tout en protégeant les droits de l'homme. Mais ce qui est plus préoccupant, c'est l'usage généralisé, inutile et non protégé qui peut être fait des données personnelles.

19. La possibilité de réunir des données biométriques collectées par des organismes publics et d'en faire bénéficier des entreprises privées pose un réel problème en matière de droits de l'homme⁸. Les entreprises privées portent aujourd'hui un grand intérêt à ce type de données, car celles-ci les renseignent de manière approfondie sur le profil physique et comportemental de leurs clients: c'est le cas, par exemple, des

7. Par exemple, en octobre 2009, les autorités françaises ont mis en place une base de données baptisée OSCAR («Outil simplifié de contrôle des aides au retour»), contenant des données biométriques relatives à des ressortissants étrangers ayant perçu une aide financière pour leur retour dans leur pays d'origine. Ce processus a été contesté par plusieurs ONG – sans succès. Voir www.ldh-toulon.net/spip.php?article4049.

8. Comité consultatif national d'éthique pour les sciences de la vie et de la santé. Avis no 98 – «Biométrie, données identifiantes et droits de l'homme», 20 juin 2007. Voir www.ccne-ethique.fr/docs/en/avis098.pdf.

On en trouve notamment un exemple au Royaume-Uni, où les données informatiques réunies par l'Etat pour le contrôle aux frontières sont liées au système informatique des compagnies aériennes concernant leurs passagers. Voir le site: www.computing.co.uk/ctg/news/1814880/leak-reveals-details-eborders-trial-routes.

compagnies d'assurances, qui peuvent utiliser ces données pour déterminer le coût du risque ou, d'une manière plus générale, à des fins de marketing, pour toute entreprise. Dès lors, les données personnelles deviennent des éléments très appréciables sur le plan commercial.

20. En ce qui concerne les droits de chaque individu, le principal danger est celui de la collecte et du regroupement de données personnelles sans l'accord des personnes directement concernées – voire sans même qu'elles en soient informées –, ainsi que le fait d'accéder à davantage de données qu'il n'en faut pour l'opération en question⁹. Des organismes publics en mal de crédits peuvent être tentés de vendre des données personnelles à des entreprises privées qui offrent des sommes d'argent importantes pour l'obtention de ce type d'informations. Etant donné la grande complexité, sur le plan juridique, de la question d'une atteinte éventuelle aux droits de l'homme (*«Drittwirkung»*), nous nous permettons de ne pas analyser ici, dans le détail, tous les aspects du processus d'utilisation des données biométriques¹⁰.

5.1. La dignité humaine

21. Les données biométriques étant collectées à partir du corps humain ou provenant de ce dernier, la question se pose de savoir si cela peut porter atteinte à la dignité humaine. Certaines personnes y seront indifférentes, tandis que d'autres pourront ressentir une certaine gêne à l'idée que leur corps soit ainsi «analysé» et s'opposer à la collecte de leurs données biométriques, pour des motifs religieux, socioculturels ou personnels. Cette notion de «dignité humaine» est le fondement même des droits de l'homme et détermine, par conséquent, tout ce qui peut constituer une violation de ces droits.

5.2. Le droit au respect de la vie privée (article 8 de la Convention européenne des droits de l'homme)

22. De toute évidence, l'évaluation – et, plus encore, la collecte et le stockage de données à caractère personnel – concernent le droit au respect de la vie privée, tel qu'il est garanti à l'article 8 de la Convention européenne des droits de l'homme («la Convention»). Etant donné que toute information sur une personne est susceptible de révéler dans une large mesure l'identité de l'individu en question, il convient d'être très prudent dans le traitement de ce type d'informations.

23. Certaines données doivent être collectées si l'on veut ménager un juste équilibre entre la sécurité et la vie privée des personnes. Mais, dans ce domaine, les techniques actuelles permettent non seulement de réunir des données nécessaires à l'identification d'une personne, mais aussi de révéler les origines ethniques, l'état de santé ou toute autre information génétique sur la personne en question. La lecture numérique de l'iris peut révéler certaines pathologies connues – ou, au contraire, totalement ignorées – de la personne concernée. Si l'on associe ces techniques à la technologie actuelle concernant l'ADN – technologie qui, certes, n'est pas considérée comme biométrique au sens strictement technique du terme –, il y a un risque très important d'exposer au grand jour l'identité d'une personne.

24. Cela pose un problème très sérieux en ce qui concerne les personnes atteintes de maladies ou handicapées – notamment en termes de possibilités d'emploi, de prise en charge par les assurances, etc.; et le problème se pose également vis-à-vis de l'identité sexuelle de la personne. Tous ces processus sont en totale contradiction avec le droit au respect de la vie privée, qui englobe le droit de choisir la manière de s'exposer et d'être reconnu dans la sphère publique. Ainsi, un individu ayant changé de sexe ne sera pas reconnu sur la base de son choix personnel, mais à partir de données biométriques. Cela peut provoquer des discriminations et un certain ostracisme.

5.3. L'interdiction de toute discrimination (article 14 de la Convention)

25. Le recours à la biométrie peut également engendrer certaines préoccupations quant au respect du principe de non-discrimination, tel qu'il est inscrit à l'article 14 de la Convention (ainsi qu'à l'article 1er du Protocole no 12 à cette Convention¹¹). Dans ce contexte, il faut tout particulièrement réfléchir aux incidences

9. Citons l'exemple de la Commission nationale pour la protection des données, au Luxembourg, qui a rejeté la demande d'un opérateur de station thermale – lequel souhaitait utiliser des données biométriques pour contrôler l'accès à l'établissement: le refus des autorités luxembourgeoises a été motivé par le non-respect du principe de proportionnalité. La Commission luxembourgeoise n'a finalement accédé à cette demande que lorsque l'opérateur commercial en question a accepté de stocker les données concernées au niveau local et non pas en liaison avec une base centrale.

Voir www.cnpd.public.lu/fr/decisions-avis/2006/04/decision-traitement-biometrique/deliberation_33_2006.pdf.

10. Pour de plus amples informations à ce sujet et sur les actes liés à cette question, voir mon rapport sur les droits de l'homme et les entreprises, Doc. 12361, du 27 septembre 2010.

11. Protocole qui, à ce jour, a été ratifié par seulement 18 Etats membres du Conseil de l'Europe.

que peuvent avoir les systèmes biométriques sur la vie des personnes physiquement handicapées ou de celles dont les caractéristiques physiques ne correspondent pas aux exigences techniques. En soi, cette situation peut susciter des préoccupations quant à la protection des données, car le seul fait, pour ces personnes, d'être «traitées» dans le cadre d'un système différent révèle déjà des données «sensibles» à leur sujet. Le fait de se renseigner ainsi sur ces personnes, par le biais de données biométriques, peut dépasser les objectifs acceptables de la collecte de données personnelles. En un mot, l'usage croissant de la biométrie pourrait conduire à une stigmatisation et à l'exclusion sociale des personnes handicapées et de celles dont les caractéristiques physiques ne sont pas facilement mesurables. Certaines études ont d'ores et déjà indiqué que, lors de l'utilisation de la plupart des méthodes biométriques, il fallait y consacrer davantage de temps et limiter le nombre de techniques dans le cas de personnes handicapées¹².

26. Chaque individu peut s'interroger: les données biométriques sont-elles utilisées à des fins autres que les objectifs déclarés a priori ou acceptés par la personne en question avant la collecte des données (c'est ce que l'on appelle en anglais «*function creep*», c'est-à-dire un «détournement d'usage»). Dans ce domaine, l'un des exemples les plus connus est l'ouverture de la base de données Eurodac à la police et à d'autres organismes chargés de faire respecter la loi. L'ouverture de bases de données aussi importantes qu'Eurodac peut permettre aux Etats de surveiller secrètement l'activité de chaque individu. Plus encore, un tel détournement d'usage peut aussi permettre des investigations à caractère discriminatoire, ou des classifications de personnes en groupes ou catégories particuliers – et ce, pour des motifs douteux. Par exemple, l'utilisation de données biométriques en vue d'identifier des minorités ethniques à des fins politiques serait particulièrement préoccupante.

27. En ce qui concerne le secteur public, ces détournements d'usage peuvent être liés à la tentation récente des Etats de privilégier les missions de surveillance, de contrôle et de détection des fraudes; cette attitude est nourrie par la crainte mondiale du terrorisme, depuis les événements du 11 septembre 2001. L'accent qui est mis sur le «contrôle» des individus va désormais au-delà de la volonté de réduire au minimum la collecte de données et les risques liés à ces opérations.

5.4. Le droit à un procès équitable (article 6 de la Convention)

28. Etant donné les risques de faux (voir la section 4, ci-dessus), l'usage de données biométriques peut également porter atteinte au droit de toute personne à un procès équitable (tel qu'il est garanti au paragraphe 1er de l'article 6 de la Convention) et, en particulier, au droit à la présomption d'innocence (paragraphe 2 de l'article 6 de la Convention)¹³. Toute erreur ou manipulation concernant les données collectées peut avoir de graves conséquences pour la personne concernée: c'est le cas, par exemple, d'une personne «reconnue» à tort comme faisant partie d'une liste de criminels recherchés. Dans la pratique, cela peut avoir pour conséquence l'obligation, pour la personne en question, de prouver son innocence. Au sujet des données biométriques, il est donc essentiel de garder à l'esprit le fait qu'elles ne renvoient qu'à une probabilité, et il importe tout autant de respecter le principe de la présomption d'innocence: ce principe, qui est l'un des fondements de la démocratie, ne doit en aucun cas et à aucun moment s'inverser.

29. La prise d'empreintes digitales se fait généralement dans le cadre d'une procédure pénale contre un individu, et l'utilisation de longue date de cette technique est ainsi comprise. D'autre part, dans le cas des demandeurs d'asile, bon nombre d'entre eux ayant été victimes de persécution, le processus d'évaluation par des données biométriques peut constituer un nouveau traumatisme. Comme l'a montré l'affaire *S. et Marper c. le Royaume-Uni*, l'utilisation de données biométriques peut constituer une violation du droit à un procès équitable dans la mesure où il n'est pas clairement établi de distinction entre des personnes condamnées et celles qui n'ont pas fait l'objet d'une quelconque condamnation¹⁴. Une telle stigmatisation peut être une atteinte au principe de présomption d'innocence.

12. Voir l'étude des Services de passeports du Royaume-Uni (UK Passport Service): *Biometrics Enrolment Trial*, 2005, p. 8 – texte disponible sur:

http://hornbeam.cs.ucl.ac.uk/hcs/teaching/GA10/lec3extra/UKPSBiometrics_Enrolment_Trial_Report.pdf.

13. Paragraphe 2 de l'article 6: «Toute personne accusée d'une infraction est présumée innocente jusqu'à ce que sa culpabilité ait été légalement établie».

14. Cour européenne des droits de l'homme: Affaire *S. et Marper c. Royaume-Uni*, Requêtes nos 30562/04 et 30566/04, arrêt du 4 décembre 2008, paragraphe 122.

5.5. La liberté de circulation (article 2 du Protocole no 4 à la Convention)

30. Au niveau européen, la liberté de circulation est garantie – dans une certaine mesure¹⁵ – au paragraphe 1er de l'article 2 du Protocole no 4 à la Convention, et le paragraphe 2 de ce même article dit que toute personne est libre de quitter n'importe quel pays, y compris le sien. De plus, les ressortissants des Etats membres de l'Union européenne ont le droit de circuler librement et de rester sur le territoire de leur Etat, aux termes de l'article 21 du Traité sur le fonctionnement de l'Union européenne¹⁶. Les techniques biométriques étant souvent utilisées aux fins de contrôle aux frontières, on peut craindre que telle ou telle personne ne fasse l'objet d'un refoulement pour des motifs illégitimes ou en raison d'une erreur du système informatique. Et, si la personne en question est mal informée des procédures d'usage, elle ne sera pas en mesure de faire réparer l'erreur.

6. Dispositions juridiques

31. A l'heure actuelle, il n'existe pas d'instrument international traitant de la biométrie. Les législations en vigueur en la matière traitent uniquement de la notion générale de «données personnelles», et ne précisent que très rarement ce qu'est la «biométrie». Compte tenu de l'évolution rapide des technologies ces dernières années, il convient d'adapter les dispositions juridiques existantes afin de trouver un juste équilibre entre le souci de sécurité et la protection des droits de l'homme. Certes, on pourrait appliquer à la biométrie les dispositions générales sur les «données personnelles»; mais, en vérité, la biométrie «de deuxième génération» est porteuse de risques plus importants que ne l'étaient les technologies précédentes.

6.1. Au niveau mondial: les Nations Unies

32. L'article 17 du Pacte international relatif aux droits civils et politiques garantit le droit au respect de la vie privée. En 1990, les Nations Unies ont défini des Principes directeurs pour la réglementation des fichiers personnels informatisés¹⁷. Ce texte vise à empêcher un traitement et une évaluation des données personnelles qui soient non protégés, inexacts, discriminatoires et contraires à la loi. Ces principes soulignent l'importance d'un traitement régulé et de l'accord de la personne concernée. Dans ce contexte, un organe de contrôle indépendant doit surveiller la collecte et le traitement des données en question. De plus, le principe de proportionnalité doit être respecté, et le processus de transmission transfrontalière de données personnelles doit faire l'objet de garanties de sécurité.

33. Toutefois, il faut souligner que les principes directeurs ainsi définis par les Nations Unies ne concernent pas spécifiquement les données biométriques: ils ne visent que les données personnelles d'ordre général – ce en quoi ce texte est d'ores et déjà en partie obsolète.

6.2. Au niveau régional (européen)

6.2.1. L'Organisation de coopération et de développement économiques

34. En 1980, l'Organisation de coopération et de développement économiques (OCDE) a défini des Lignes directrices sur la protection de la vie privée et les flux transfrontières de données de caractère personnel¹⁸. Bien que ces recommandations ne concernent que les données et les informations d'ordre général, elles indiquent également ce que l'OCDE entend par «données de caractère personnel». De plus, dans un rapport datant de 2004, le Groupe de travail sur la sécurité et le caractère privé de certaines informations donne une définition précise de la «biométrie»¹⁹.

15. Cette disposition stipule que «quiconque se trouve régulièrement sur le territoire d'un Etat a le droit d'y circuler librement et d'y choisir librement sa résidence». D'autre part, les paragraphes 3 et 4 de l'article 2 du Protocole no 4 fixent d'autres restrictions dans ce contexte.

16. On en trouvera la version consolidée sur:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0047:0200:FR:PDF>.

17. United Nations Guidelines for the regulation of computerized personal data files. A/RES/45/95. Texte consultable sur: www.un.org/documents/ga/res/45/a45r095.htm.

18. OCDE: «Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel» (1980). Texte accessible sur:

www.oecd.org/document/18/0,3746,fr_2649_34255_1815225_1_1_1_1,00.html.

19. OCDE, Groupe de travail sur la sécurité et le caractère privé de certaines informations: «Biometric-based Technologies», 2004. Texte accessible sur:

[www.oecd.org/officialdocuments/displaydocumentpdf?cote=dsti/iccp/reg\(2003\)2/final&doclanguage=en](http://www.oecd.org/officialdocuments/displaydocumentpdf?cote=dsti/iccp/reg(2003)2/final&doclanguage=en).

35. L'OCDE recommande de limiter la collecte de données – y compris pour des motifs légitimes. De la même manière que les Nations Unies, l'OCDE souligne l'importance de l'accord de la personne concernée, et la nécessité d'un mécanisme de contrôle indépendant et suffisamment solide. Dans le rapport de 2004 précité, les experts de l'OCDE déclarent que, même si la biométrie peut contribuer au renforcement de la sécurité – si les techniques en question sont bien utilisées –²⁰, on peut craindre un risque d'erreur important²¹.

6.2.2. Le Conseil de l'Europe

6.2.2.1. Article 8 de la Convention et jurisprudence de la Cour européenne des droits de l'homme

36. La Convention européenne des droits de l'homme et ses protocoles additionnels garantissent plusieurs droits et libertés qui peuvent être directement affectés par l'utilisation de données biométriques: il s'agit du droit au respect de la vie privée, du droit à un procès équitable, de la présomption d'innocence, de l'interdiction de toute discrimination et de la liberté de circulation. Dans ce contexte, le droit au respect de la vie privée, tel qu'il est inscrit à l'article 8 de la Convention, est tout particulièrement important; il est à l'origine d'une riche jurisprudence de la Cour européenne des droits de l'homme («la Cour»). Toutefois, le droit au respect de la vie privée n'est pas absolu, car il peut être sujet au type d'ingérences justifiables aux termes du paragraphe 2 de l'article 8 de la Convention. Mais ces restrictions doivent être «prévues par la loi» et «nécessaires dans une société démocratique».

37. Conformément à l'article 8 de la Convention, la Cour européenne des droits de l'homme a traité de nombreuses affaires touchant à la protection des données. Mais, même si les technologies biométriques ne sont plus totalement nouvelles, on ne compte encore que de très rares affaires relatives à la biométrie. En réalité, cela s'explique par le fait que ces technologies ne font partie de la vie quotidienne que depuis peu.

38. Le principe de «proportionnalité» tient une place centrale dans les arrêts de la Cour. Les affaires *Kinnunen c. Finlande*²², *Van der Velden c. Pays-Bas*²³, *Rotaru c. Roumanie*²⁴ et *W. c. Pays-Bas*²⁵ montrent bien que la question des violations de la vie privée doit être traitée au cas par cas.

39. L'arrêt de la Cour de 2008 concernant l'affaire *S. et Marper c. Royaume-Uni*²⁶ a fait jurisprudence en matière de recours à la biométrie. Cette affaire portait sur le fait que des empreintes digitales et des échantillons d'ADN collectés à la suite de l'arrestation des futurs requérants avaient été conservés après la libération des deux individus, et alors que ces derniers avaient expressément demandé la destruction de ces éléments. La Cour a fait valoir que la conservation durable des éléments en question constituait une atteinte à la vie privée des deux requérants, et, par conséquent, une violation de l'article 8 de la Convention. Désormais, cet arrêt devrait pouvoir s'appliquer à d'autres types de données biométriques; l'affaire en question a également montré l'importance de l'accord des personnes faisant l'objet d'une utilisation de données biométriques, ainsi que le caractère sensible des données²⁷.

40. Cet arrêt allait également dans la même direction que certains arrêts antérieurs de la Cour au sujet d'informations personnelles conservées dans des registres secrets de la police²⁸, et du prélèvement, de la conservation et de la classification d'échantillons d'ADN²⁹. Les données biométriques recueillies dans le cadre d'enquêtes criminelles sont généralement légitimes dès lors que l'individu concerné fait l'objet de

20. *Ibid.*, p. 13.

21. *Ibid.*, p. 38.

22. *Kinnunen c. Finlande*, Requête no 24950/94, décision du 15 mai 1996. La Cour a établi que la prise d'empreintes digitales et de photographies à la suite d'une arrestation n'était pas une infraction à l'article 8 de la Convention, en raison de l'absence d'éléments susceptibles de s'opposer à ces pratiques.

23. *Van der Velden c. Pays-Bas*, Requête no 29514/05, décision du 7 décembre 2006. La Cour a jugé que le stockage systématique d'éléments d'ADN pour un éventuel usage a posteriori était une ingérence suffisamment importante pour être considérée comme une violation de l'article 8 de la Convention.

24. *Rotaru c. Roumanie*, Requête no 28341/95, arrêt du 4 mai 2000. La Cour a conclu à une violation du droit du requérant au respect de sa vie privée, du fait que le mode de collecte, de stockage et d'utilisation des informations par les services de renseignements roumains n'était pas assorti de garanties juridiques suffisantes.

25. *W. c. Pays-Bas*, Requête no 20689/08, décision du 20 janvier 2009. Le prélèvement d'échantillons d'ADN sur un mineur, à la suite d'une condamnation, ne constitue pas une violation de l'article 8 de la Convention si, indépendamment de l'âge du prévenu, toutes les règles concernant le prélèvement d'ADN sont respectées.

26. *S. et Marper c. Royaume-Uni*, Requêtes nos 30562/04 et 30566/04, arrêt du 4 décembre 2008.

27. *Ibid.*, paragraphe 34.

28. *Leander c. Suède*, Requête no 9248/81, arrêt du 26 mars 1987, paragraphe 48.

29. *Van der Velden c. Pays-Bas*, voir note 23 ci-dessus.

soupçons plausibles. C'est la raison pour laquelle, en règle générale, la législation doit être précise et non seulement définir la nature des données requises, mais aussi justifier les objectifs de la collecte, de l'évaluation et du traitement de telles données.

6.2.2.2. *La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*

41. Le principal instrument juridique du Conseil de l'Europe qui soit pertinent en matière de données biométriques est la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, qui date de 1981 (STE no 108) («la Convention relative à la protection des données») et son protocole additionnel (STE no 181), qui concerne les autorités de contrôle et les flux de données transfrontaliers.

42. A ce jour, cette convention a été ratifiée par 43 des 47 Etats membres du Conseil de l'Europe. Elle vise à mieux définir les normes de protection de la vie privée, et à harmoniser et renforcer cette protection dans les Etats membres. Ce texte a été le premier instrument contraignant au niveau international, dans ce domaine. Il définit la notion de «données personnelles», ainsi que les concepts de «contrôleur» et de «traitement automatisé» – ce en quoi il est conforme aux règles que l'OCDE avait établies un an auparavant. La convention concerne à la fois le secteur public et le secteur privé.

43. L'article 5 de la convention établit les principes d'évaluation et de traitement des données personnelles (obtention loyale, enregistrement et utilisation pour des finalités déterminées et légitimes, et exactitude). Concernant la sécurité des données (articles 7 et 8), les dispositions de la convention ont un caractère plutôt général («mesures appropriées») et laissent une grande part de liberté aux Etats membres pour légiférer sur le sujet. Il en est de même des données dites «sensibles», telles que celles concernant la santé, la vie sexuelle et les convictions politiques et religieuses. Ce type de données ne peut faire l'objet d'un traitement automatisé, excepté si les législations nationales prévoient des garanties appropriées (article 6 de la convention).

44. Le paragraphe c de l'article 5 exige que les données utilisées soient «adéquates, pertinentes et non excessives» – traduction du principe de proportionnalité, qui devrait encore être renforcé face aux nouveaux défis.

45. Du fait que les données à caractère personnel définissent un individu en ce qui concerne les événements potentiels de sa vie, le «droit à l'autodétermination» doit occuper une place centrale dans toute réglementation juridique en la matière. Par «autodétermination», il faut entendre notamment le consentement de la personne en question. Si la Convention relative à la protection des données établit effectivement le droit de l'individu concerné à obtenir la destruction des données collectées (article 8.c), il n'est pas dit clairement, en revanche, si la personne est propriétaire des données en question et, dès lors, si elle peut trancher au sujet du traitement des données. On peut dire, par conséquent, que l'article 8.c révèle une certaine faiblesse de la convention à cet égard et que ce texte prévoit, certes, des instruments d'application adéquats, mais aussi de trop nombreuses dérogations. Naturellement, il convient de se rappeler que cette convention ne fait qu'établir des principes applicables par les Etats membres; mais, en fait, la convention devrait inciter les Etats à faire preuve d'une plus grande fermeté en la matière.

6.2.2.3. *Le Protocole additionnel à la Convention relative à la protection des données*

46. En 2001, un protocole additionnel à la convention – concernant la mise en place d'autorités de contrôle – était ouvert à la signature. A ce jour, il a été ratifié par 30 Etats membres. Aux termes de ce protocole, les Etats membres du Conseil de l'Europe ont l'obligation de créer des autorités de contrôle indépendantes.

6.2.2.4. *Le rapport d'étape*

47. En 2005, le Conseil de l'Europe publiait un «Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement de données biométriques». Ce rapport a été élaboré par le Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe. Il contient une analyse des spécificités de la biométrie, un examen des critères de sélection des structures du système, ainsi que des orientations concernant l'application de la convention à la biométrie. En premier lieu, il s'agissait de déterminer si la convention pouvait s'appliquer aux données biométriques en tant que telles³⁰ – étant donné que la convention ne concernait, a priori, que les «données à caractère personnel». On peut effectivement se poser

30. Voir le site www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Biometrie_2005.pdf.

la question de l'applicabilité de cette convention en la matière, car les processus d'identification et de vérification ne portent pas exclusivement sur les données biométriques en elles-mêmes puisque, pour identifier et vérifier, il faut toujours un élément de référence³¹.

48. Cependant, étant donné que, dans ce type de processus, on note toujours des caractéristiques biométriques particulières à l'individu concerné, pourquoi ne pas les considérer comme des «données à caractère personnel»? Si l'on considère le nom et la date de naissance d'une personne comme des données qui lui sont effectivement «personnelles», on pourrait également établir, par extension, que les caractéristiques corporelles et le comportement sont aussi des «données personnelles» puisque ces éléments ne sont pas acquis a posteriori par l'individu, et constituent plutôt des caractéristiques naturelles ou inhérentes à la personne en question. Par conséquent, il n'y a pas lieu d'envisager l'applicabilité de la convention uniquement en liaison avec le concept de «traitement automatisé» – comme le suggère le rapport³²; parallèlement à ce concept, on peut également fonder la notion d'applicabilité de la convention sur le fait que les données biométriques sont aussi des «données à caractère personnel».

49. Reconnaisant le fait que de nombreux aspects de la biométrie ne sont pas encore totalement connus, le rapport ne propose pas de conclusions définitives et n'exclut pas la nécessité d'une révision de la Convention relative à la protection des données sur ce point. Les technologies biométriques permettent de renforcer considérablement la sécurité, certes; mais la ligne jaune de la violation des droits de l'homme peut être facilement franchie. Bon nombre de personnes ne sont pas suffisamment conscientes du risque d'atteinte à la vie privée, car elles n'ont pour souci que de disposer d'instruments pratiques et utilisent ces nouvelles technologies sans réfléchir à leurs conséquences. Le consentement d'un individu n'a aucune valeur si la personne en question n'est pas consciente des conséquences que peut avoir l'opération proposée; donc, il faut absolument poser la question des effets de l'utilisation de données biométriques.

6.2.3. L'Union européenne

6.2.3.1. La Charte des droits fondamentaux

50. Tout en ne modifiant pas fondamentalement la nature des concepts de «droit au respect de la vie privée» et de «protection des données à caractère personnel», l'entrée en vigueur du Traité de Lisbonne a apporté des changements considérables au statut de ces notions: aux termes du Traité de Lisbonne, de l'article 6, paragraphe 1, du Traité de l'Union européenne³³, et par la référence qui est faite à la protection des données à l'article 16 du Traité sur le fonctionnement de l'Union européenne, la Charte des droits fondamentaux de l'Union européenne a désormais un caractère contraignant. Non seulement la Charte protège la vie privée en son article 7³⁴, mais elle garantit également, en son article 8, la protection des données à caractère personnel³⁵. Le statut des droits établis par la Charte montre bien l'importance de la nécessité de protéger ce type d'informations.

6.2.3.2. La Directive 95/46/CE

51. En 1995, le Parlement européen et le Conseil de l'Union européenne ont adopté la Directive 95/46/CE³⁶, qui concerne la protection des personnes physiques à l'égard du traitement des données à caractère personnel et la libre circulation de ces données. La directive développe le contenu de l'article 8 de la Convention et les dispositions de la Convention relative à la protection des données. Mais, de même que la plupart des législations en vigueur, la directive ne concerne pas explicitement les «données biométriques»; elle porte, d'une manière plus générale, sur les «données à caractère personnel». C'est sur cette directive que les Etats membres de l'Union européenne ont fondé leurs systèmes respectifs de protection des données. Il faut noter encore que l'Union européenne a également adopté d'autres instruments en ce qui concerne la protection des données à caractère personnel³⁷.

31. Voir le paragraphe 8 ci-dessus.

32. *Ibid.*

33. Consulter la version intégrale sur:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0013:0046:FR:PDF>.

34. «Toute personne a le droit au respect de sa vie privée et familiale, de son domicile et de ses communications.»

35. Article 8 – Protection des données à caractère personnel:

1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante.

36. Texte disponible sur: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:fr:HTML>.

52. La Directive 95/46/CE oblige les Etats membres de l'Union européenne à adopter une législation établissant un juste équilibre entre sécurité et respect de la vie privée. Il est évident que cette directive ne concerne pas la protection des données dans les Etats non membres de l'Union.

53. En raison de la mondialisation et des développements récents en matière technologique, la Commission européenne a proposé, le 4 novembre 2010, une stratégie de renforcement des règles de l'Union européenne en matière de protection des données – et notamment une révision de la Directive 95/46/CE. La Commission européenne envisage de proposer, en 2011, un nouveau cadre juridique général pour la protection des données à caractère personnel dans l'Union européenne³⁸; entre autres éléments, ce nouveau cadre renforcera les droits des personnes en matière de collecte de données.

6.2.3.3. Le Règlement (CE) no 2252/2004

54. Le Règlement (CE) no 2252/2004³⁹ traite explicitement des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les Etats membres de l'Union européenne. Ce règlement vise à renforcer la sécurité par une harmonisation et une offre de normes minimales de sécurité en matière de biométrie, dans les documents de voyage, afin d'éviter toute fraude ou falsification.

55. Cependant, ce règlement ne traite guère des questions de vie privée, en raison de l'obligation de respecter le principe de proportionnalité et de définir les objectifs de l'évaluation et du traitement des données biométriques. La question d'un stockage correct des données n'est pas non plus réglementée: cet élément est laissé à l'initiative des Etats membres. Enfin, le Règlement no 2252/2004 ne contient pas non plus de définition des «caractéristiques biométriques» ou des «identifiants biométriques».

6.2.3.4. Le Groupe de travail «Article 29» sur la protection des données et le Contrôleur européen de la protection des données

56. En outre, à la suite de la Directive 95/46/CE, un Groupe de travail sur l'article 29 a été créé, en tant qu'organe de contrôle, composé de représentants de tous les Etats membres de l'Union européenne et du Contrôleur européen de la protection des données – celui-ci ayant rejoint le groupe dans un deuxième temps. Ce groupe de travail est un organe consultatif qui aide les Etats membres à mettre correctement en place le cadre établi par la directive et à œuvrer à une législation commune.

57. Le poste de Contrôleur européen de la protection des données a été créé en 2001. Le mandat du contrôleur est semblable à celui du groupe de travail dans son ensemble: il consiste à superviser, à coopérer avec les organes de contrôle nationaux et à conseiller.

6.3. Au niveau national

58. Au niveau national, rares sont les pays ayant adopté une législation générale sur le traitement des données biométriques. Dans la plupart des Etats membres du Conseil de l'Europe, la législation nationale ne mentionne pas expressément la biométrie, ces questions étant généralement régies par la législation nationale en matière de protection des données.

59. Sur les 47 Etats membres du Conseil de l'Europe, 34 ont intégré dans leur Constitution une disposition relative à la protection des données. La plupart disposent également d'une législation nationale spécifique applicable à la protection des données à caractère personnel⁴⁰. Tandis que de nombreux Etats non européens ont adopté des lois distinctes traitant séparément du secteur public et du secteur privé (ou un même cadre législatif dans lequel les deux secteurs font l'objet de chapitres distincts), la plupart des Etats européens ont adopté une seule loi visant également le secteur public et le secteur privé.

37. Citons notamment la Directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, telle qu'elle a été modifiée par la Directive 2006/24/CE; le Règlement (CE) no 45/2001 du Parlement européen et du Conseil, du 18 décembre 2000, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données.

38. [http://europa.eu/rapid/pressReleasesAction.do?](http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1462&format=HTML&aged=0&language=EN&guiLanguage=fr)

[reference=IP/10/1462&format=HTML&aged=0&language=EN&guiLanguage=fr](http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1462&format=HTML&aged=0&language=EN&guiLanguage=fr).

39. Règlement (CE) no 2252/2004, du 13 décembre 2004, établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les Etats membres. Texte disponible sur: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R2252:FR:HTML>.

40. Pour un survol des législations nationales sur la protection des données, consulter: www.coe.int/t/dghl/standardsetting/dataprotection/National_laws_en.asp.

7. Conclusions

60. D'après le rapport d'étape de 2005 du Comité consultatif du Conseil de l'Europe de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, «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»⁴¹. Les principales questions de droits de l'homme posées par l'essor de la biométrie concernent le droit au respect de la vie privée, le droit à un procès équitable, la présomption d'innocence, la liberté de circulation et l'interdiction de la discrimination. La biométrie n'en est qu'à ses débuts, et l'on n'en connaît pas encore très bien les risques. Lorsque cette technique aura été adoptée à grande échelle, un développement irréversible, porteur d'effets imprévisibles, pourrait être amorcé. Dès lors, il convient d'appliquer le principe de précaution et de faire preuve d'une certaine prudence en l'état actuel des choses. Dans l'avenir, il se peut que l'on ne s'aperçoive même pas que les données sont collectées. Les programmes de surveillance par vidéo sont capables de suivre le comportement d'une personne à distance. Ainsi, chaque fois que l'on collecte des données biométriques il faut l'annoncer de manière claire et anticipée aux personnes concernées, par exemple en installant des panneaux d'information dans les endroits publics.

61. Cinq ans après l'adoption du rapport d'étape précité, le temps est venu de réexaminer la question de la biométrie, en tenant compte des progrès technologiques réalisés entre-temps. Il faut également se rappeler que la biométrie de deuxième génération a étendu la portée de ces technologies, accru leur précision et leur caractère intrusif. Enfin, il faut noter que les informations disponibles à ce sujet sont souvent contradictoires, notamment en raison des frontières imprécises entre les capacités potentielles (= futures) et actuelles des applications de la biométrie. On doit donc procéder à une analyse et à une évaluation systématiques, actualisées en permanence et prévoyant les effets sociaux, économiques et juridiques de l'utilisation croissante de la biométrie. Le perfectionnement des technologies biométriques devrait aller de pair avec une limitation des conséquences préjudiciables qu'elles pourraient avoir pour les droits de l'homme.

62. Plusieurs études ont souligné la nécessité de préciser le concept de «données biométriques», dans la mesure où la plupart des législations existantes n'abordent la notion de «données à caractère personnel» que de manière très générale⁴². En dépit d'une ouverture vers les nouvelles évolutions en la matière, les définitions d'ordre général augmentent les risques de défaut d'application des textes et de vides juridiques. Le Règlement no 2252/2004 du Conseil de l'Union européenne, qui préconise l'insertion de données biométriques dans les passeports, montre bien la nécessité de préciser clairement la terminologie et les concepts utilisés, et ce, dans les meilleurs délais.

63. L'une des actions majeures du Conseil de l'Europe doit être de sensibiliser davantage au droit au respect de la vie privée et à ce que cela recouvre – y compris les règles de protection des données. Si la plupart des citoyens européens savent qu'ils jouissent du droit au respect de leur vie privée – lequel est généralement garanti par la Constitution de leur pays –, bon nombre d'entre eux n'en connaissent pas la portée exacte. Très fréquemment, on ne se rend pas compte du caractère privé de tel ou tel élément – sauf si les conséquences de la révélation de certaines données privées sont tout à fait évidentes. Trop nombreux sont ceux qui sont prêts à divulguer des informations personnelles pour gagner un petit avantage pratique ou un peu de temps. Or, le fait que les bases de données soient facilement interconnectées et associées pour établir un profil identitaire très précis met en danger ce droit au respect de la vie privée. Des réglementations s'imposent également vis-à-vis de l'utilisation de la biométrie dans le secteur privé.

64. Par conséquent, le Conseil de l'Europe devrait actualiser le contenu de sa Convention relative à la protection des données, et suivre de très près le développement des technologies biométriques, afin de veiller à ce que les législations répondent correctement aux nouveaux défis. Nous devons définir très précisément les données biométriques, indiquer quelles législations traitent de ces données, et faire connaître le «contrôleur» des données. L'adoption de tout texte de loi sur la protection des données doit être guidée par les principes de transparence, de consentement des personnes et de proportionnalité, afin de satisfaire non seulement aux intérêts sécuritaires, mais aussi au respect de la vie privée et de la dignité des personnes.

65. On ne saurait assez souligner l'importance d'un juste équilibre entre ces deux dimensions. Mais, en réalité, on doit déplorer que les Etats aient tendance à collecter et à conserver davantage d'informations que nécessaire – et ce pour un usage à venir, éventuellement préventif, comme en a témoigné récemment la

41. Voir note 30 ci-dessus, paragraphe 10.

42. Korff, D. et Brown, I., *New Challenges to Data Protection*, 2010, p. 2. Texte accessible sur:
http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_summary_en.pdf.

plainte déposée par deux ONG contre la réglementation française sur les passeports biométriques⁴³. Par conséquent, on peut dire en conclusion qu'il reste encore beaucoup à faire sur le plan législatif et en termes de sensibilisation et de recherche scientifique.

43. Il s'agit d'une plainte d'IRIS («Imaginer un internet solidaire») et de la Ligue des droits de l'homme. On en trouvera le texte sur www.ines.sgdg.org/IMG/pdf/recours-passeport0708.pdf. La réglementation française va bien au-delà du Règlement de l'Union européenne, puisqu'elle exige huit empreintes digitales, à stocker dans une base de données centralisée. Cette affaire a été en attente de jugement pendant plus de deux ans; c'est la preuve du caractère sensible d'une telle question et de la difficulté de la justice et du législateur à trouver un juste équilibre.