1710-01/05/FR

WP 112

04/09/12

Avis 3/2005

sur l'application du règlement (CE) n° 2252/2004 du Conseil 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 États membres

(*Journal officiel L 385 du 29 décembre 2004 p. 1 - 6*)

Adopté le 30 septembre 2005

Table des matières

Avis 3/2005

sur l'application du règlement (CE) n° 2252/2004 du Conseil 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 États membres

(*Journal officiel L 385 du 29 décembre 2004 p. 1 - 6*)

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

institué en vertu de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995[1] ,

vu l'article 29, l'article 30, paragraphe 1, point c), et l'article 30, paragraphe 3, de la directive susmentionnée,

vu son règlement intérieur et notamment ses articles 12 et 14,

A ADOPTÉ L'AVIS SUIVANT:

1. Introduction

1.1. Question générale

Dans son «**Document de travail sur la biométrie[2]**», le groupe de travail a souligné que «les progrès rapides des technologies biométriques et la généralisation de leur application ces dernières années nécessitent un examen minutieux sous l'angle de la protection des données. Leur utilisation incontrôlée suscite des inquiétudes en ce qui concerne la protection des libertés et des droits fondamentaux des individus. Les données de ce type sont d'une nature

[1] Journal officiel L 281 du 23.11.1995, p. 31, disponible à l'adresse suivante: http://europa.eu.int/comm/justice_home/fsj/privacy/law/index_fr.htm

particulière parce qu'elles ont trait aux caractéristiques comportementales et physiologiques d'une personne et qu'elles peuvent permettre de l'identifier sans ambiguïté».

Depuis ces remarques fondamentales sur la biométrie, les développements législatifs ont progressé rapidement. Le Conseil européen de Thessalonique, les 19 et 20 juin 2003, a confirmé la nécessité de dégager au sein de l'Union européenne une approche cohérente en ce qui concerne les identificateurs ou les données biométriques pour les documents des ressortissantes de pays tiers, les passeports des citoyens de l'Union et les systèmes d'information (VIS et SIS II). À l'automne 2003, la Commission a présenté une proposition de règlement du Conseil modifiant les règlements 1683/95 et 1030/2002, établissant respectivement un modèle type de visa et un modèle uniforme de titre de séjour pour les ressortissants de pays tiers.

1.2. Historique du règlement (CE) n° 2252/2004 du Conseil

Le 18 février 2004, la Commission a présenté une proposition de règlement établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports des citoyens de l'UE[3]. L'objectif de cette proposition était de rendre les passeports plus sûrs en instaurant un instrument juridiquement obligatoire relatif aux normes concernant les dispositifs de sécurité harmonisés et, en même temps, de créer un lien fiable entre le document et son véritable titulaire, en insérant des éléments d'identification biométriques. De plus, cela devait permettre aux États membres de l'UE de satisfaire aux exigences du programme américain d'exemption de visa, conformément aux normes internationales. Dans cette proposition, la Commission européenne proposait que les passeports et autres documents de voyage comportent obligatoirement un support de stockage avec une photo faciale. Les États membres étaient autorisés à intégrer des empreintes digitales dans les passeports. En outre, la Commission européenne proposait que les identifiants biométriques soient stockés sur un support doté d'une capacité suffisante. Il pouvait s'agir d'une puce sans contact, mais également d'un autre support offrant la capacité voulue, la décision revenant aux experts du comité compétent. La proposition de règlement offrait également la possibilité de stocker les empreintes digitales dans une base de données nationale en vue de la création d'un futur registre européen des documents délivrés.

---

2 MARKT/10595/03/FR – WP 80, adopté le 1er août 2003.

3 Document C(2004) 116-final, publié au Journal officiel n° C 98 du 23 avril 2004, p. 39.

À l'été 2004, le groupe de travail sur les visas a examiné la proposition. Le 6 octobre 2004, le groupe de travail CSIFA (Comité stratégique sur l'immigration, les frontières et l'asile) a finalement discuté la proposition et l'a soumise au Parlement européen. La proposition finale imposait la photo faciale numérisée comme premier élément biométrique obligatoire, et les empreintes digitales comme second élément biométrique facultatif.

À l'issue du Conseil JAI (Justice et affaires intérieures) des 25 et 26 octobre 2004, le texte de la proposition a été modifié afin de rendre les deux éléments biométriques obligatoires[4].

Le 2 décembre 2004[5], la résolution législative à caractère non contraignant du Parlement européen sur la proposition, présentée par la Commission, de règlement du Conseil établissant des normes pour les dispositifs de sécurité et les éléments biométriques intégrés dans les passeports des citoyens de l'UE a été adoptée par 471 voix pour, 118 voix contre et 6 abstentions. Le Parlement soutient l'introduction de passeports contenant une photo faciale au motif que cet élément biométrique rend les passeports plus difficiles à falsifier et assure que la personne présentant le passeport est effectivement la personne à qui il a été délivré. Il a cependant rejeté l'inclusion obligatoire des empreintes digitales et la création d'une base de données sur les passeports et les documents de voyage de l'UE, au motif que l'insertion d'éléments biométriques ne doit pas porter atteinte aux droits à la vie privée et à la protection des données. La résolution législative du 2 décembre 2004 déclare que les données biométriques intégrées dans les passeports ne seront utilisées que pour vérifier l'authenticité du document et l'identité du titulaire et qu'elles seront stockées sur «un support de stockage hautement sécurisé, doté d'une capacité suffisante et qui est à même de préserver l'intégrité, l'authenticité et la confidentialité des données stockées». Elle précise également que seules les autorités des États membres compétentes pour lire, stocker, modifier et effacer les données biométriques doivent y avoir accès. De plus, le Parlement a introduit un amendement au projet de règlement, lequel stipule que «il n'est établi aucune base de données centralisée des passeports et documents de voyage de l'Union européenne contenant les données biométriques et autres de tous les titulaires d'un passeport au sein de l'UE ». Selon le rapport de la Commission des libertés civiles, de la justice et des affaires intérieures

---

4 Document du Conseil n° 15139/2004.

5 Résolution législative du Parlement européen sur la proposition, présentée par la Commission, de règlement du Conseil établissant des normes pour les dispositifs de sécurité et les éléments biométriques intégrés dans les passeports des citoyens de l'UE (COM(2004)0116 – C5-0101/2004 – 2004/0039(CNS)), http://www2.europarl.eu.int/omk/sipade2?PUBREF=-//EP//TEXT+TA+P6-TA-2004-0073+0+DOC+XML+V0//EN&LEVEL=2&NAV=X.

du 25 octobre 2004, «la création d'une base de données centralisée violerait les principes de finalité et de proportionnalité. Elle accroîtrait le risque d'abus et de dérapages. Enfin, elle augmenterait également le risque d'utilisation des éléments d'identification biométrique comme «clés d'accès» à diverses bases de données, mettant ainsi en connexion différents fichiers».

Le 13 décembre 2004, le Conseil a adopté le règlement (CE) n° 2252/2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, sur la base du projet rédigé par le Conseil JAI des 25 et 26 octobre 2004[6]. Le règlement du Conseil impose la photo faciale numérisée comme premier élément biométrique obligatoire et les empreintes digitales comme second élément biométrique, également obligatoire. Le Conseil n'a pas tenu compte des suggestions et demandes de modification du Parlement. En vertu de son article 6, le règlement est entré en vigueur le 18 janvier 2005. Ce même article du règlement dispose que les États membres appliquent le règlement:

«a) en ce qui concerne la photo faciale: au plus tard 18 mois

b) en ce qui concerne les empreintes digitales: au plus tard 36 mois

après l'adoption des mesures visées à l'article 2.»

Le 28 février 2005, la Commission européenne a adopté la «décision établissant les spécificités techniques concernant les normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres[7]» laquelle fait référence à l'article 2 du règlement (CE) n° 2252/2004 du Conseil.

1.3. Avis précédent du groupe de travail

Le 18 août 2004, le président du groupe de travail «Article 29» a adressé une lettre au président du Parlement européen, au président de la commission LIBE, au secrétaire général du Conseil de l'Union européenne, au président de la Commission européenne, au directeur

---

6 Journal officiel L 385, p. 1-6, publié le 29 décembre 2004.

7 C(2005) 409 final, (non encore publié au Journal officiel).

de la DG Entreprises et au directeur général de la DG Justice et affaires intérieures. Il formulait les propositions concrètes suivantes[8].

«1. Le groupe de travail s'oppose fermement au stockage des données biométriques et autres de tous le titulaires d'un passeport au sein de l'UE dans une base de données centralisée des passeports et documents de voyages européens.

2. L'objectif de l'insertion d'éléments biométriques dans les passeports et documents de voyage, conformément au règlement, doit être explicite, approprié, proportionné et clair.

3. Les États membres doivent garantir d'une manière techniquement appropriée que les passeports contiennent un support de stockage doté d'une capacité suffisante et qui est à même de préserver l'intégrité, l'authenticité et la confidentialité des données stockées.

4. Le règlement doit définir qui peut avoir accès au support de stockage et dans quel but (lire, stocker, modifier ou effacer des données).

5. Les États membres devront tenir un registre des autorités compétentes»

Le président faisait observer que les éléments de sécurité intégrés dans les passeports et documents de voyage doivent être valides et garantis pendant toute la durée de validité du document. Les autorités délivrant ces documents sont responsables des normes de sécurité et des infrastructures nécessaires. Les défaillances dans ce domaine survenant lors de l'édition ou de la délivrance du document, ou durant sa période de validité, ne peuvent être imputées aux citoyens.

Enfin, il attirait l'attention sur l'avis relatif aux données biométriques (WP 80), adopté par le groupe de travail le 1er août 2003[9], et sur l'avis sur l'insertion d'éléments biométriques dans les visas et titres de séjour (WP 96), adopté le 11 août 2004[10].

Dans une autre lettre, adressée le 30 novembre 2004 au président de la commission LIBE et au président du Conseil de l'Union européenne, le président du groupe de travail «Article 29»

---

8 Lettre du 18 août 2004 adressée par le président du groupe de travail « Article 29 » au président du Parlement européen, au président de la commission LIBE, au secrétaire général du Conseil de l'Union européenne, au président de la Commission européenne, au directeur de la DG Entreprises et au directeur général de la DG Justice et affaires intérieures (non publiée).

9 MARKT/10595/03/FR – WP 80, adopté le 1er août 2003.

10 MARKT/11224/04/FR – WP 96, adopté le 11 août 2004.

se déclarait défavorable à un second élément biométrique obligatoire. Il soulignait que l'introduction d'un élément biométrique supplémentaire rendait d'autant plus nécessaire la création d'un système sûr et étanche afin d'assurer que le droit fondamental à la vie privée n'était pas menacé.

À cet égard, il importe de prendre également en considération le récent avis du groupe de travail «Article 29» (WP110) du 23 juin 2005 sur la proposition de règlement du Parlement européen et du Conseil concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour[11]. Cet avis rappelle la position du groupe de travail «Article 29» sur la biométrie et demande la mise en place de garanties appropriées pour le traitement des données biométriques dans les VIS.

1.4. Résolution de la Conférence internationale des commissaires à la protection des données et à la vie privée

Le 16 septembre 2005, la 27ème conférence internationale des commissaires à la protection des données et à la vie privée de Montreux a adopté la **Résolution sur l'utilisation de la biométrie dans les passeports, cartes d'identité et documents de voyage**[12]. Dans cette résolution, la conférence internationale souligne que l'utilisation sur une grande échelle de la biométrie aura un impact considérable sur la société et devrait donc être précédée d'un débat ouvert au niveau mondial. La conférence internationale appelle à

1. la mise en place, à un stade précoce, de garanties efficaces en vue de limiter les risques inhérents à la nature de la biométrie,

2. une distinction stricte entre les données biométriques collectées et conservées à des fins publiques (par exemple, contrôles aux frontières) sur la base d'obligations légales, et celles qui sont collectées à des fins contractuelles sur la base du consentement,

3. la limitation, par des mesures techniques, de l'utilisation des données biométriques intégrées dans les passeports et les cartes d'identité à des fins de vérification, par comparaison des données figurant dans le document avec celles fournies par son titulaire lorsqu'il le présente.

---

[11] MARKT/1022/05/FR.

[12] http://www.privacyconference2005.org (non encore publié).

2. *Insertion d'éléments biométriques dans les passeports, les autres documents de voyage et les cartes d'identité*

L'article 1er, paragraphe 2, du règlement (CE) n° 2252/2004 dispose que les passeports des citoyens de l'UE contiennent obligatoirement une photo faciale numérisée et les empreintes digitales. Conformément à son article 6, et en vertu de la décision C (2005) 409 du 28 février 2005 de la Commission européenne, les États membres doivent intégrer la photo faciale numérisée au plus tard le 28 août 2006 et les empreintes digitales au plus tard le 28 février 2008 dans les passeports de leurs citoyens. Les premiers États membres devront commencer à délivrer des «ePasseports» contenant une photo faciale numérisée stockée sur une étiquette intelligente à l'automne 2005. Pour les États membres délivrant des cartes d'identité, on envisage d'y intégrer des éléments biométriques.

2.1. Considérations générales

L'introduction d'éléments biométriques dans les passeports aura de lourdes conséquences pour les titulaires de ceux-ci. De ce fait, elle ne peut se faire sans que l'on procède à une évaluation appropriée de ses conséquences sur la vie privée. Jusqu'à présent, une description de certains éléments biométriques dans les passeports ou autres documents de voyage, tels qu'une photo, le sexe, la taille ou la couleur des yeux, suffisait. Après la mise en oeuvre du règlement (CE) n° 2252/2004 du Conseil, les citoyens européens devront fournir des éléments biométriques numérisés. Ces données peuvent être stockées dans des bases de données et peuvent être mises à disposition à des fins non prévisibles.

2.2. Risques éthiques liés à l'usage d'éléments biométriques intégrés dans les passeports, les autres documents de voyage et les cartes d'identité

L'intégration d'éléments biométriques dans les passeports, documents de voyage et cartes d'identité comporte de nombreux risques éthiques. Financé par la CE dans le cadre du sixième programme-cadre de recherche et de développement technologique (6e PC), le projet ETIB (Éthique des technologies d'identification biométrique)[13] a été lancé en octobre 2004. Il a pour but de lancer la recherche et d'ouvrir un débat public sur l'éthique de la biométrie. Une consultation publique sera organisée en juin 2006. Un autre projet soutenu par l'Union

[13] http://www.biteproject.org/

européenne dans le cadre du 6e PC est le projet FIDIS[14] (L'avenir de l'identité dans la société de l'information), qui est dirigé par un consortium rassemblant des universités et des entreprises européennes, ainsi que d'autres institutions publiques et privées. Le but de FIDIS est de définir les conditions auxquelles devra satisfaire la future gestion de l'identité dans la société européenne de l'information et de contribuer en développement des technologies et infrastructures nécessaires[15].

D'après une étude prospective[16] commandée par la commission LIBE du Parlement européen, des procédures de secours devraient être disponible afin de constituer une garantie essentielle pour l'introduction de la biométrie, du fait qu'elle n'est ni accessible à tous ni tout à fait exacte. De telles procédures devraient être mises en place et utilisées afin de respecter la dignité de personnes n'ayant pu suivre la procédure d'inscription avec succès et éviter de leur imputer la responsabilité des imperfections du système[17].

Un des aspects de la discussion est que les institutions gouvernementales et autres autorités publiques pourront collecter et stocker un nombre considérable d'informations sensibles sur leurs citoyens. Dans ce contexte, il devrait être particulièrement souligné que la collecte d'éléments biométriques concerne la collecte d'informations concernant le *corps* d'une personne.

Un autre aspect est que, jusqu'à présent, les éléments biométriques tels que les empreintes digitales étaient collectés principalement dans des affaires pénales. La question est: les citoyens européens sont-ils prêts à donner leurs empreintes digitales pour d'autres raisons?

D'autres préoccupations sont de nature différente: les personnes pour qui il peut être plus difficile de prouver leur identité, comme les immigrants, pourraient être injustement visées par un tel système; les personnes handicapées qui ne peuvent pas se soumettre à des examens biométriques pourraient être stigmatisées; et des informations médicales sensibles pourraient être obtenues. À un niveau pratique, les lois sur la vie privée varient d'un pays à l'autre, ce qui aura des répercussions dans le partage des données et l'interaction des bases de données.

---

[14] http://www.fidis.net

[15] Deux autre projets, BIOSEC et BIOSECURE, également financés par le 6e PC, étudient aussi cette question dans une certaine mesure. http://www.biosec.org et http://www.biosecure.info

[16] Biometrics at the frontiers: assessing the impact on Society, February 2005, Institute for Prospective Technological Studies, DG Joint Research Centre, European Commission.

Dans le cas du stockage des empreintes digitales, il faudra être attentif au fait que diverses corrélations entre certaines caractéristiques papillaires et des maladies correspondantes sont en cours de discussion. Par exemple, certaines caractéristiques papillaires dépendraient de la nutrition de la mère (et donc du fœtus) pendant le troisième mois de grossesse[18]. La leucémie et le cancer du sein semblent être statistiquement liés à certaines caractéristiques papillaires. On n'a pas encore établi de corrélation directe ou précise dans ce domaine, mais un débat scientifique est en cours et on ne peut l'ignorer.

2.3. Aspects législatifs de l'utilisation des éléments biométriques

a) Réserves à l'égard d'une base de données nationale ou européenne sur les éléments biométriques

Dans la décision législative du 2 décembre 2004, le Parlement européen a demandé l'interdiction d'une base de données centralisée des passeports et documents de voyage de l'Union européenne contenant les données biométriques et autres de tous les titulaires d'un passeport au sein de l'UE. Le groupe de travail soutient cette demande et déclare que les objections à l'égard d'une base de données centralisée des passeports et documents de voyage de l'Union européenne sont les mêmes que celles qui sont formulées à l'égard des bases de données centralisées des passeports et documents de voyage et des cartes d'identité au niveau national.

La création d'une base de données centralisée contenant les données personnelles et en particulier les données biométriques de tous les citoyens (européens) risquerait de violer le principe de base de proportionnalité. Toute base de données centralisée accroîtrait les risques d'utilisation abusive et d'appropriation frauduleuse. Elle accroîtrait également le risque d'abus et de dérapages. Enfin, elle augmenterait également le risque d'utilisation des éléments d'identification biométrique comme «clés d'accès» à diverses bases de données, et partant d'interconnexion de différents fichiers.

---

[17] Rapport d'étape sur l'application des principes de la convention 108 relative à la collecte et au traitement des données biométriques, Conseil de l'Europe, 2005, page 11

[18] FIDIS, étude sur l'ICP et la biométrie, p. 68.

b) Accès aux éléments biométriques réservé aux autorités compétentes

Les éléments biométriques intégrés dans les passeports, les autres documents de voyage ou les cartes d'identité sont d'une grande sensibilité. Il faut donc garantir que seules les autorités compétentes peuvent avoir accès aux données stockées sur la puce. Tout accès non autorisé est inacceptable. C'est pour cette raison que le groupe de travail soutient les demandes du Parlement européen que chaque État membre tienne un registre des autorités compétentes et des organismes autorisés visés à l'article 3, du règlement (CE) n° 2252/2004. Les États membres doivent communiquer ce registre et, au besoin, les mises à jour de celui-ci à la Commission, laquelle tiendra un registre en ligne à jour et publiera chaque année une compilation des registres nationaux.

En cas de rejet lors d'un contrôle aux frontières ou de tout autre contrôle effectué par les autorités compétentes, les personnes concernées doivent être informées des raisons de ce rejet, des moyens par lesquels elles peuvent faire valoir leur point de vue et des autorités de recours compétentes.

2.4. Aspects techniques

Les risques techniques sont d'une autre nature. Ils concernent l'intégration d'une puce sans contact (étiquette intelligente) et les éléments biométriques contenus dans cette puce.

Dans sa décision législative du 2 décembre 2004, le Parlement européen a demandé que les passeports comportent un support de stockage doté d'une capacité suffisante et qui est à même de préserver l'intégrité, l'authenticité et la confidentialité des données stockées. Le groupe de travail a soutenu cette demande[19], mais celle-ci n'a pas été prise en compte par le Conseil. L'étiquette intelligente conforme à la norme ISO 14443 visée dans le règlement du 13 décembre 2004 entraîne de nombreux risques pour le droit à la vie privée des citoyens européens. La décision de la Commission du 28 février 2005[20] n'est pas appropriée pour protéger les droits des citoyens étant donné que le contact entre la puce et le lecteur peut être intercepté et que l'information peut être écrémée.

---

[19] Lettre du 18 août 2004 adressée par le président du groupe de travail « Article 29 » au président du Parlement européen, au président de la commission LIBE, au secrétaire général du Conseil de l'Union européenne, au président de la Commission européenne, au directeur de la DG Entreprises et au directeur général de la DG Justice et affaires intérieures (non publiée).

[20] C(2005) 409 final.

Les risques liés à l'intégration d'étiquettes intelligentes dans les passeports, autres documents de voyage ou cartes d'identité, ainsi que les risques générés par l'intégration d'éléments biométriques dans la puce nécessitent une architecture de sécurité qui renforce la confiance et qui favorise ainsi l'échange d'informations. Pleinement conscient des problèmes qui se posent, le groupe de travail constate donc un besoin d'une infrastructure à clé publique (ICP) mondiale. Les certificats associés aux clés publiques contiennent des informations sur le titulaire. Chaque certificat numérique assure une traçabilité exclusivement jusqu'à la personne à qui il a été délivré. Les certificats numériques sont aussi uniques que les numéros de sécurité sociale, de carte de crédit ou d'assurance maladie. Mais les certificats numériques peuvent être utilisés de façon abusive pour refuser au titulaire l'accès à des services. De plus, les données générées par des transactions effectuées avec des certificats cibles peuvent être filtrées par des instruments de surveillance et transmises électroniquement à des tiers, à la police ou d'autres autorités.

Compte tenu de ces risques, il est impératif de créer un Profil de Protection (PP) sur la base des Critères communs d'évaluation de la sécurité des technologies de l'information (Critères Communs - CC) vers. 2.1 (norme ISO 15408). Ces profils proposent une solution généralement acceptée aux problèmes de sécurité informatique. Ils décrivent un concept de sécurité informatique qui doit être complet, constant et cohérent. Le Profil de Protection devrait être présenté par le comité institué par l'article 5 du règlement (CE) n° 2252/2004. Conformément aux amendements proposés par le Parlement européen dans sa résolution législative du 2 décembre 2004, le groupe de travail propose que le comité soit assisté par des experts désignés par le groupe de travail.

a) Insertion d'une photo faciale numérisée

En vertu de la décision de la Commission européenne du 28 février 2005, les États membres sont tenus d'intégrer une photo faciale numérisée dans les passeports de leurs citoyens au plus tard le 28 août 2006. En vertu de l'article 1er et du point 5.2 de l'annexe de la décision, les États membres doivent assurer l'accès aux données de la puce par un élément de sécurité appelé Basic Access Control – BAC (contrôle d'accès de base). Le BAC est une recommandation de l'Organisation de l'Aviation Civile Internationale (ICAO), mais il n'est

pas obligatoire[21]. Le but du BAC est d'empêcher l'écrémage et l'interception. Il doit garantir que l'accès aux données et aux données biométriques en particulier n'est possible que lorsqu'une «Document Basic Access Key» (clé d'accès de base au document) a été créée avant la lecture des données de la puce à partir de la zone lisible par machine (ZLM) du passeport par un contact optique entre le passeport et le lecteur. La «Document Basic Access Key» est calculée à partir du numéro du passeport, de la date de naissance et de la date d'expiration. Après avoir créé cette clé, le lecteur est en mesure de lire les données stockées sur l'étiquette intelligente. Pour des raisons de sécurité, la transmission des données se fait de manière cryptée. Cela implique une puce sécurisée certifiée possédant un coprocesseur crypté[22].

Cependant, le BAC ne constitue pas un élément de sécurité suffisant. Il se base sur la zone MRZ (lisible par machine) du passeport, mais les données contenues dans cette zone ne sont pas traitées de manière strictement confidentielle. Par exemple, si un citoyen européen souhaite acheter un billet pour un évènement exceptionnel comme la «Coupe du Monde FIFA 2006» en Allemagne ou l' «Euro UEFA 2008» en Autriche et en Suisse, il doit donner sur un formulaire Internet son nom, sa date de naissance, son numéro de passeport ou de carte d'identité ainsi que la date de délivrance du document. De telles procédures pour l'achat d'un billet ont déjà été appliquées pour l'«Euro UEFA 2004» au Portugal. Elles seront appliquées également lors d'autres évènements, tels que des concerts ou de grands évènements sportifs comme les Jeux olympiques ou le championnat du monde d'athlétisme. Comme, dans certains États membres, les entreprises privées copient les passeports ou les cartes d'identité à titre de garantie du montant dû, les éléments constitutifs de la «Document Basic Access Key» ne sont pas secrets et l'on peut craindre que l'algorithme du BAC ne soit un jour consultable sur Internet.

---

[21] ICAO Technical Report: PKI for Machine Readable Travel Documents offering ICC Read-Only Access (Rapport technique OACI: ICP sur les documents de voyage lisibles à la machine offrant un accès CPI en lecture seule), Version 1.1, publié le 1er octobre 2004, page 16.

[22] Aux fins de transmission sécurisée, le «groupe Essen» a développé un logiciel spécial appelé Golden Reader Tool. Le groupe Essen Group est constitué d'autorités publiques, d'entreprises de sécurité informatique et d'entreprises produisant des documents de voyage d'Allemagne, des Pays-Bas et du Royaume-Uni.

b) Introduction d'éléments biométriques supplémentaires, notamment concernant les empreintes digitales

Les circonstances dans lesquelles les empreintes digitales sont collectées doivent garantir une fiabilité parfaite. L'ICAO, qui ne considère pas la photo faciale numérisée comme sensible – parce qu'il y a toujours une photo du titulaire dans le passeport – reconnaît que l'intégration d'empreintes digitales et d'autres éléments biométriques dans le passeport est en revanche extrêmement sensible. Elle recommande donc un mécanisme de sécurité spécial appelé Extended Acces Control (Contrôle d'Accès Étendu)[23]. Ce mécanisme fonctionne de manière similaire au BAC, comme décrit précédemment. Cependant, pour cet Extended Acces Control, on utilise une série de «Document Extended Access Keys» au lieu des «Document Basic Access Keys». Il appartient à chaque État de définir la série de «Document Extended Access Keys» (propre à chaque puce). La série de «Document Extended Access Keys» peut consister soit en des clés symétriques (par exemple dérivées d'une MRZ et d'une «clé universelle nationale»), soit en une paire de clés asymétriques avec un certificat de carte correspondant. Mais beaucoup de détails de ces mécanismes de sécurité demeurent imprécis.

Le «Extended Access Control» représente un progrès en ce qui concerne les mesures de sécurité, mais ce mécanisme n'est qu'une option, comme le BAC[24]. On peut, de plus, se demander si les pays tiers mettront en place ce «Extended Access Control». La Commission européenne et les États membres devraient garantir que les passeports intégrant des données d'empreintes digitales ne peuvent être lus par des lecteurs qui ne sont pas compatibles avec le «Extended Access Control».

3. Conclusions

L'intégration d'éléments biométriques dans les passeports, autres documents de voyage et cartes d'identité soulève de nombreuses questions éthiques, juridiques et techniques. Aussi, le groupe de travail souligne-t-il les aspects suivants:

---

[23] ICAO Technical Report: PKI for Machine Readable Travel Documents offering ICC Read-Only Access (Rapport technique OACI: ICP sur les documents de voyage lisibles à la machine offrant un accès CPI en lecture seule), Version 1.1, publié le 1er octobre 2004, page 17.

[24] ICAO Technical Report: PKI for Machine Readable Travel Documents offering ICC Read-Only Access (Rapport technique OACI: ICP sur les documents de voyage lisibles à la machine offrant un accès CPI en lecture seule), Version 1.1, publié le 1er octobre 2004, pages 17, 21 et 22.

1. Avant d'intégrer des éléments biométriques dans les passeports, autres documents de voyage ou cartes d'identité, un débat approfondi au sein de la société est nécessaire. Pour cela, il faut attendre les conclusions du projet ETIB.

2. Afin de limiter les risques inhérents à la nature de la biométrie, des garanties effectives doivent être mises en place à un stade précoce. Dans ce but, le comité institué par l'article 5 du règlement (CE) n° 2252/2004, qui devrait être assisté par des experts nommés par le groupe de travail «Article 29», devra présenter un Profil de Protection.

3. Une nette distinction doit être garantie entre les données biométriques collectées et stockées à des fins publiques (par exemple, pour le contrôle aux frontières) sur la base d'obligations légales, d'une part, et celles qui sont collectées à des fins contractuelles sur la base du consentement, d'autre part.

4. L'utilisation de la biométrie dans les passeports et cartes d'identité doit être techniquement limitée à des fins de vérification, pour comparer les données du document et celles produites par le titulaire lorsqu'il présente le document.

5. La Commission européenne et les États membres devraient garantir que les passeports intégrant des données d'empreintes digitales ne peuvent être lus par des lecteurs qui ne sont pas compatibles avec le «Extended Access Control».

6. Il devrait être garanti que seules les autorités compétentes peuvent avoir accès aux données stockées sur la puce. Les États membres tiendront un registre des autorités compétentes.

Fait à Bruxelles, le 30 septembre 2005

Pour le groupe de travail
Le président
Peter Schaar