CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

Avis du contrôleur européen de la protection des données sur la proposition de règlement du Parlement européen et du Conseil concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (COM(2004) 835 final)

(2005/C 181/06)

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité instituant la Communauté européenne, et notamment son article 286,

vu la Charte des droits fondamentaux de l'Union européenne, et notamment son article 8,

vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,

vu le règlement (CE) n° 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, et notamment son article 41,

vu la demande d'avis formulée par la Commission conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001, reçue le 25 janvier 2005,

A ADOPTÉ L'AVIS SUIVANT:

1. **INTRODUCTION**

1.1. **Remarques préliminaires**

La mise en place du système d'information sur les visas (VIS) constitue un élément important de la politique commune de l'UE en matière de visas et a fait l'objet de plusieurs instruments étroitement liés.

— En avril 2003 a été présentée une étude de faisabilité ([1]) sur le VIS, commandée par la Commission.

— En septembre 2003, la Commission a proposé une modification ([2]) d'un règlement antérieur établissant un modèle type de visa. L'objectif principal était d'intégrer dans ce nouveau modèle de visa des données biométriques (images du visage et de deux empreintes digitales), qui seraient stockées sur une puce.

([1]) Système d'information sur les visas, rapport final, commandé par la CE à Trasys, avril 2003.
([2]) COM(2003) 558 final - 2003/0217 (CNS) et 2003/0218 (CNS).

— En juin 2004, une décision du Conseil ([1]) a lancé le processus de mise en place du système d'information sur les visas en fournissant la base juridique pour permettre son inscription au budget de l'UE. Cette décision proposait la création d'une base de données centrale comprenant des informations sur les demandes de visas et envisageait le recours à la procédure de comitologie pour gérer le développement technique du VIS.

En décembre 2004, la Commission a adopté une proposition de règlement concernant le VIS et l'échange de données entre les États membres sur les visas de court séjour ([2]) (ci-après dénommée «la proposition»), sur laquelle porte le présent avis. La proposition est accompagnée d'une analyse d'impact approfondie ([3]) (ci-après dénommée «l'AIA»).

Néanmoins, ainsi qu'il est précisé dans l'exposé des motifs de la proposition, d'autres instruments seront nécessaires pour compléter ce règlement, en particulier pour:

— modifier les Instructions consulaires communes adressées aux représentations diplomatiques et consulaires de carrière des parties contractantes de la Convention de Schengen (ci-après dénommées «les instructions consulaires communes») en ce qui concerne l'introduction de données biométriques dans les procédures,

— mettre en place un nouveau mécanisme d'échange de données avec l'Irlande et le Royaume-Uni,

— échanger des données sur les visas de long séjour.

Ainsi qu'il a été décidé lors de la session du Conseil «Justice et affaires intérieures» tenue les 5 et 6 juin 2003 et conformément aux dispositions de l'article 1er, paragraphe 2, de la décision susmentionnée du Conseil de juin 2004, le VIS reposera sur une architecture centralisée comprenant une base de données dans laquelle les dossiers de demande de visas seront stockés, appelée «système central d'information sur les visas» (CS-VIS), ainsi qu'une «interface nationale» (NI-VIS) située dans les différents États membres. Chaque État membre désignera ([4]) une autorité centrale nationale reliée à l'interface nationale, qui autorisera l'accès des différentes autorités nationales compétentes au CS-VIS.

1.2. **Principaux éléments de la proposition du point de vue de la protection des données**

La proposition vise à améliorer la mise en œuvre de la politique commune en matière de visas en facilitant l'échange de données entre les États membres grâce à la création d'une base de données centrale. Le règlement envisage d'enregistrer des données biométriques (photographies et empreintes digitales) pendant la procédure de demande de visa et de les stocker dans la base de données centrale.

Des données biométriques pourraient également être introduites dans les vignettes-visas, conformément au règlement modificatif établissant un modèle type de visa, proposé par la Commission, qui prévoit d'intégrer dans ce modèle une photographie et des empreintes digitales, stockées sur une puce (dans l'attente, à ce jour, d'une décision du Conseil sur la base des résultats de l'analyse en cours).

La proposition décrit de manière détaillée les différentes opérations dont font l'objet les données (saisie, modification, effacement et consultation), ainsi que les différentes données à intégrer dans le VIS en fonction de la suite donnée à la demande (acceptation, refus, etc.).

La proposition prévoit que les données relatives à chaque demande sont conservées pendant cinq ans.

La proposition établit une liste limitative des autorités compétentes autres que les autorités chargées des visas qui auront accès au VIS, et définit les droits d'accès qui leur seront accordés:

— les autorités compétentes chargées des contrôles des visas aux frontières extérieures et sur le territoire de l'État membre,

— les autorités compétentes en matière d'immigration,

([1]) Décision 2004/512/CE, JO L 213 du 15.6.2004, p. 5.
([2]) COM(2004) 835 final - 2004/0287 (COD).
([3]) «*Study for the Extended Impact Assessment of the Visa Information System*» (Étude d'analyse d'impact approfondie du système d'information sur les visas), rapport final du EPEC, décembre 2004.
([4]) Article 24, paragraphe 2, de la proposition.

— les autorités compétentes en matière d'asile.

Dans sa description du fonctionnement du VIS et des responsabilités s'y rapportant, la proposition souligne que la Commission traite les données du VIS au nom des États membres. Elle indique qu'il est nécessaire d'établir des relevés des opérations de traitement des données pour assurer la sécurité des données et détaille les responsabilités de chaque partie pour garantir de ce niveau de sécurité.

La proposition contient un chapitre consacré à la protection des données, qui détaille le rôle des autorités nationales ainsi que celui du contrôleur européen de la protection des données (ci-après dénommé «le CEPD»).

Elle prévoit qu'un comité institué par l'article 5, paragraphe 1, du règlement (CE) nº 2424/2001 relatif au développement du système d'information de Schengen de deuxième génération (SIS II) soit chargé de la mise en œuvre technique du VIS et de l'identification des technologies nécessaires à cette mise en œuvre.

Une analyse d'impact approfondie du VIS, commandée par la Commission à l'EPEC, est jointe à la proposition. Elle conclut que la meilleure manière d'améliorer la politique commune en matière de visas consiste à opter pour un VIS qui s'appuie sur l'utilisation de données biométriques.

2. **CADRE JURIDIQUE APPLICABLE**

La proposition aura une incidence majeure sur le respect de la vie privée et d'autres droits fondamentaux des personnes physiques. C'est pourquoi nous l'examinons au regard des principes régissant la protection des données. Notre examen se fonde principalement sur les textes suivants:

— Le respect de la vie privée est garanti en Europe depuis l'adoption par le Conseil de l'Europe, en 1950, de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (ci-après «CEDH»). L'article 8 de la CEDH consacre le «droit au respect de la vie privée et familiale».

  Aux termes de l'article 8, paragraphe 2, de la CEDH, il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est «prévue par la loi» et qu'elle constitue une mesure qui, «dans une société démocratique, est nécessaire» à la protection d'intérêts majeurs. Dans la jurisprudence de la Cour européenne des droits de l'homme, le respect de ces conditions implique des exigences supplémentaires relatives à la qualité de la base juridique de l'ingérence, la proportionnalité des mesures et la nécessité de garanties adéquates contre les abus.

  La convention sur la protection des données élaborée par le Conseil de l'Europe et adoptée en 1981 énonce des principes fondamentaux en matière de protection des personnes à l'égard du traitement des données à caractère personnel.

— Le droit au respect de la vie privée et la protection des données à caractère personnel ont été consacrés plus récemment dans les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, qui doit constituer la partie II de la nouvelle Constitution de l'UE.

  L'article 52 de la Charte prévoit que ces droits peuvent faire l'objet de limitations, étant entendu que des conditions similaires à celles qui sont prévues à l'article 8 de la CEDH doivent être remplies. Ces conditions doivent être prises en compte chaque fois qu'une proposition prévoyant une éventuelle ingérence est examinée.

À ce jour, les règles fondamentales en matière de protection des données sont fixées dans les actes législatifs de l'UE suivants:

— Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO L 281, p. 31). Cette directive, ci-après dénommée «la directive 95/46/CE», fixe de manière détaillée les principes au regard desquels la proposition sera examinée, dans la mesure où elle doit s'appliquer aux États membres. Ce texte est d'autant plus pertinent que la proposition s'appliquera conjointement avec la législation nationale donnant effet à la directive. En conséquence, l'efficacité des dispositions et garanties proposées dépendra de l'efficacité de cette application conjointe dans chaque cas particulier.

— 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 (JO L 8, p. 1). Ce règlement, ci-après dénommé «le règlement 45/2001», fixe des principes similaires à ceux de la directive 95/46/CE et est pertinent pour notre examen dans la mesure où la proposition doit s'appliquer aux activités de la Commission en même temps que les dispositions du règlement. Cette application conjointe mérite également d'être prise en considération.

Il est nécessaire de lire la directive 95/46/CE et le règlement 45/2001 conjointement avec d'autres instruments. En d'autres termes, dans la mesure où ces actes portent sur un traitement de données à caractère personnel susceptible d'enfreindre les libertés fondamentales — en particulier le droit au respect de la vie privée —, ils doivent être interprétés en tenant compte des droits fondamentaux. C'est également ce qui ressort de la jurisprudence de la Cour de justice ([1]).

— Enfin, le CEPD prendra également en considération dans son analyse l'avis nº 7/2004 «sur l'insertion d'éléments biométriques dans les visas et titres de séjour en tenant compte de la création du système d'information visas (VIS)» adopté le 11 août 2004 par le Groupe «Article 29» de protection des personnes à l'égard du traitement des données à caractère personnel ([2]) ci-après dénommé «le Groupe Article 29». Dans cet avis, le groupe s'est déclaré préoccupé par plusieurs éléments de la proposition. Le CEPD entend vérifier si et de quelle manière la proposition a tenu compte de ces préoccupations.

3. **ANALYSE DE LA PROPOSITION**

3.1. **Généralités**

Le CEPD reconnaît que le développement d'une politique commune en matière de visas nécessite un échange efficace de données pertinentes. Le VIS constitue l'un des mécanismes susceptibles de garantir la fluidité des échanges d'informations. Néanmoins, ce nouvel instrument devrait se limiter à la collecte et à l'échange de données dans la mesure où ceux-ci sont nécessaires à la mise en place d'une politique commune en matière de visas et proportionnés à cet objectif.

Si la mise en place du VIS peut avoir des conséquences positives pour d'autres intérêts publics légitimes, elle ne modifie pas pour autant la finalité de ce système. La finalité limitée de ce système joue un rôle majeur dans la détermination du contenu et de l'utilisation légitimes du système et, dès lors, également dans l'octroi d'un droit d'accès au VIS (ou à certaines de ses données) aux autorités des États membres pour des intérêts publics légitimes.

En outre, la proposition introduit l'utilisation de données biométriques dans le VIS. Tout en reconnaissant les avantages que présente cette utilisation, le CEPD en souligne l'incidence majeure et suggère de l'assortir de garanties strictes.

Il importe de lire le présent avis à la lumière de ces considérations clés. Nous faisons observer que cet avis devrait être mentionné dans le préambule du règlement, avant les considérants («vu l'avis…»).

([1]) À cet égard, il est utile de citer l'arrêt de la Cour du 20 mai 2003 rendu en séance plénière dans les affaires jointes C-465/00, C-138/01 et C-139/01, Österreichischer Rundfunk et autres, Recueil 2003, p. I-4989. La Cour y examine une loi autrichienne prévoyant la transmission à la Cour des comptes autrichienne d'informations concernant les revenus des employés du secteur public ainsi que leur publication ultérieure. Elle fixe un certain nombre de critères, fondés sur l'article 8 de la Convention européenne des droits de l'homme, qu'il convient d'appliquer lors de la mise en œuvre de la directive 95/46/CE, dans la mesure où celle-ci autorise certaines limitations au droit à la vie privée.

([2]) Il s'agit d'un groupe consultatif indépendant, institué par la directive 95/46/CE et composé de représentants des autorités des États membres chargées de la protection des données, du CEPD et de la Commission.

3.2 **Finalité**

La finalité du VIS revêt une importance décisive, compte tenu à la fois de l'article 8 de la CEDH et du cadre général de la protection des données. Conformément à l'article 6 de la directive 95/46/CE, les données à caractère personnel doivent être «collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités». Seule une définition claire des finalités permettra d'évaluer correctement le caractère proportionné et adéquat du traitement des données à caractère personnel, ce qui est essentiel au vu de la nature des données (notamment biométriques) et de l'ampleur du traitement envisagé.

L'objet du VIS est clairement exposé à l'article 1er, paragraphe 2, de la proposition:

> «Le VIS améliore la mise en œuvre de la politique commune en matière de visas, la coopération consulaire et la consultation des autorités consulaires centrales en facilitant l'échange de données entre les États membres sur les demandes de visas et les décisions y relatives.»

En conséquence, tous les éléments du VIS doivent être des instruments nécessaires et proportionnés pour atteindre cet objectif dans l'intérêt de la politique commune en matière de visas.

L'article 1er, paragraphe 2, de la proposition énumère également d'autres effets bénéfiques de l'amélioration de la politique en matière de visas, en particulier:

a) prévenir les menaces pesant sur la sécurité intérieure,

b) faciliter la lutte contre la fraude,

c) faciliter les contrôles aux points de passage aux frontières extérieures.

Le CEPD estime que ces éléments sont des exemples des conséquences positives de la mise en place du VIS et de l'amélioration de la politique commune en matière de visas, mais ne constituent pas des finalités en soi.

Il en découle deux conséquences principales à ce stade:

— le CEPD est conscient que les services répressifs sont intéressés à se voir accorder l'accès au VIS; le Conseil a adopté des conclusions en ce sens le 7 mars 2005. Le VIS ayant pour objet d'améliorer la politique commune en matière de visas, il convient de noter qu'un accès systématique des services répressifs à ce système ne serait pas conforme à cette finalité. Certes, en application de l'article 13 de la directive 95/46/CE, cet accès pourrait être accordé sur une base ad hoc, dans certaines circonstances et sous réserve de garanties appropriées, mais un accès systématique ne peut être autorisé.

  D'une manière plus générale, il sera essentiel d'évaluer la proportionnalité et la nécessité de l'accès au VIS si des décisions doivent être prises à l'avenir sur l'opportunité d'autoriser certaines autres autorités à accéder à ce système. Les missions au titre desquelles l'accès est octroyé doivent correspondre aux finalités du VIS.

— La mention explicite, au point a), de la «prévention des menaces pesant sur la sécurité intérieure des États membres» est regrettable. Le VIS aura pour principaux effets bénéfiques la prévention de la fraude et du «visa shopping» (la lutte contre la fraude étant également la principale raison de l'introduction de données biométriques dans le système) ([1]). Il convient donc de considérer la prévention des menaces pesant sur la sécurité comme un effet bénéfique «secondaire», même s'il est très positif.

  Le CEPD recommande de rendre plus explicite cette distinction entre «objet» et «effets bénéfiques» dans le libellé de l'article 1er, paragraphe 2, qui pourrait être formulé comme suit:

  «Le VIS a pour objet d'améliorer la mise en œuvre de la politique commune en matière de visas, la coopération consulaire et la consultation des autorités consulaires centrales en facilitant l'échange de données entre les États membres sur les demandes de visas et les décisions qui s'y rapportent. Ce faisant, il contribue également …»

([1]) L'AIA l'indique très clairement (point 1.6): *«un manque d'efficacité en matière de lutte contre le "visa shopping" et la fraude et en matière de contrôles entraîne également un manque d'efficacité dans le domaine de la sécurité intérieure des États membres»* (traduction du Conseil). Cela suppose que les menaces qui pèsent sur la sécurité s'expliquent en partie par un manque d'efficacité de la politique en matière de visas. À cet égard, il convient en premier lieu d'améliorer cette politique, principalement en luttant contre la fraude et en améliorant les contrôles. L'amélioration de la politique en matière de visas entraînera une amélioration de la sécurité.

Il convient également de noter à cet égard que les «lignes directrices concernant la mise en place d'un système commun d'échange de données relatives aux visas», adoptées par le Conseil «JAI» le 13 juin 2002 ([1]), mentionnaient la prévention des menaces pesant sur la sécurité intérieure à la fin de la liste des objectifs. La proposition pourrait adopter la même présentation, qui serait d'ailleurs beaucoup plus cohérente avec la finalité du VIS.

3.3. **Qualité des données**

Aux termes de l'article 6 de la directive 95/46/CE, les données à caractère personnel doivent être «adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement». Ce principe s'applique à la proportionnalité du VIS en tant que tel, mais également sur les données à collecter et à stocker dans le VIS et sur leur utilisation future, ainsi que sur les garanties complémentaires applicables à cet égard. Ces éléments sont tout aussi essentiels pour évaluer la proposition à la lumière de l'article 8 de la CEDH.

La mise en place du VIS constitue sans aucun doute une ingérence importante dans l'exercice du droit à la vie privée, ne serait-ce qu'en raison de l'ampleur du système et des catégories de données à caractère personnel traitées. C'est pourquoi, dans son avis n° 7/2004, le Groupe «Article 29» a souhaité «obtenir communication des études et estimations relatives à l'ampleur et à la gravité des phénomènes en cause, études pouvant justifier les exigences impérieuses en matière de sécurité ou d'ordre public qui imposeraient une telle approche».

Le CEPD a examiné attentivement les éléments d'information présentés dans l'AIA. Bien que ceux-ci ne soient pas totalement concluants, il apparaît qu'il existe des raisons suffisantes pour justifier la mise en place du VIS en vue d'améliorer la politique commune en matière de visas.

Dans ce contexte, il semble que le pouvoir législatif dispose d'une marge d'appréciation suffisante pour décider de la mise en place du VIS en tant qu'instrument visant à améliorer les conditions de délivrance de visas par les États membres. En soi, un tel système peut s'intégrer dans la mise en place progressive d'un espace de liberté, de sécurité et de justice prévue par le traité CE et venir appuyer ce processus.

Néanmoins, il serait inadmissible que la mise en place et l'utilisation du VIS se traduisent par l'impossibilité de continuer à assurer un niveau élevé de protection des données à caractère personnel dans ce domaine. Il appartient au CEPD, dans le cadre de sa mission consultative, d'examiner dans quelle mesure le VIS influera sur le niveau actuel de protection des données relatives aux personnes concernées.

Au vu de ce qui précède, le CEPD examinera plus particulièrement dans le présent avis les points suivants:

— le caractère proportionné et adéquat des données et de leur utilisation (par exemple, les catégories de données, l'accès des différentes autorités concernées aux données et la durée de conservation),

— le fonctionnement du système (par exemple, les responsabilités et la sécurité),

— les droits des personnes concernées (par exemple, leur information, la possibilité de corriger ou de supprimer des données inexactes ou non pertinentes),

— le suivi et le contrôle du système.

En dehors de ce qui suit, la proposition ne donne lieu à aucune observation majeure en ce qui concerne les catégories de données à inclure dans le VIS et leur utilisation. Les dispositions correspondantes ont été libellées avec le soin voulu et semblent cohérentes et appropriées dans leur ensemble.

([1]) Décision-cadre du Conseil du 13 juin 2002 relative à la lutte contre le terrorisme (2002/475/JAI), JO L 164 du 22.6.2002, p. 3.

3.4. **La biométrie**

3.4.1. *Impact du recours à la biométrie*

Le recours à la biométrie dans les systèmes d'information n'est jamais un choix anodin, surtout si le nombre d'individus concernés est très important. La biométrie n'est pas seulement une nouvelle technologie de l'information; en rendant possible la mesure des caractéristiques du corps humain par des machines et en permettant l'utilisation ultérieure de ces caractéristiques, la biométrie modifie définitivement la relation entre corps et identité. Même si les données biométriques ne sont pas accessibles à l'œil nu, des outils appropriés en permettent la lecture et l'utilisation, pour toujours et où que puisse se rendre la personne concernée.

Quel que soit l'intérêt de la biométrie à certains égards, son utilisation généralisée aura un impact majeur sur la société et devrait faire l'objet d'un débat large et ouvert. Le CEPD doit constater que ce débat n'a pas vraiment eu lieu avant l'élaboration de la proposition, ce qui souligne d'autant plus la nécessité de fixer des garanties très strictes en matière d'utilisation des données biométriques et de profiter du processus législatif pour mener une réflexion et un débat en profondeur.

3.4.2. *Spécificités de la biométrie*

Ainsi que cela a déjà été souligné dans plusieurs avis du Groupe de protection «Article 29» ([1]), la saisie et le traitement de données biométriques pour des documents d'identité doivent s'accompagner de garanties particulièrement cohérentes et sérieuses. Les données biométriques sont en effet rendues très sensibles du fait de certaines de leurs caractéristiques.

Il est effectivement pratiquement impossible de dissocier des données biométriques de la personne qu'elles concernent, ce qui n'est pas le cas pour un mot de passe ou une clé. Ces données se caractérisent par la possibilité d'une *identification quasi-certaine* (elles sont uniques pour chaque individu), par leur *permanence* (elles restent pratiquement inchangées au cours de la vie d'une personne) et par leur *universalité* (les mêmes «éléments» physiologiques se retrouvent chez tous les individus).

Cependant, la révocation de données biométriques est pratiquement impossible car il est difficile de changer un doigt ou de transformer un visage. Cet aspect, positif à bien des égards, présente un inconvénient majeur en cas d'*usurpation d'identité*: le stockage des empreintes digitales et de la photographie dans une base de données des identités usurpées pourrait causer des difficultés sérieuses et définitives à la victime de l'usurpation. De plus, de par leur nature, les données biométriques ne sont *nullement secrètes* et peuvent même *laisser des traces* (empreintes digitales, ADN) qui en permettent la collecte *sans que la personne concernée n'en soit consciente*.

Compte tenu de ces risques inhérents à la nature des données biométriques, il faudra mettre en œuvre de sérieuses garanties (notamment en termes de respect du principe de limitation de la finalité du traitement des données, de restriction de l'accès à celles-ci et de mesures de sécurité).

3.4.3. *Imperfections techniques du recours aux empreintes digitales*

Les principaux avantages des données biométriques décrits ci-dessus (universalité des données, pertinence, permanence, facilités d'utilisation, etc.) ne sont jamais absolus, ce qui a une incidence directe sur l'efficacité de la mesure de ces données et des procédures de vérification correspondantes prévues par le règlement.

La proportion de personnes dont les empreintes digitales ne sont pas exploitables ([2]) pourrait s'élever jusqu'à 5 % (en raison d'empreintes digitales illisibles ou faisant entièrement défaut). Il ressort de l'AIA annexée à la proposition qu'on peut estimer à quelque 20 millions le nombre de demandeurs de visas en 2007, ce qui signifie que près d'un million de personnes ne seront pas en mesure de suivre la procédure d'enregistrement «normale», ce qui aura des conséquences évidentes au niveau des demandes de visas et au niveau des contrôles aux frontières.

([1]) Avis n° 7/2004 sur l'insertion d'éléments biométriques dans les visas et titres de séjour en tenant compte de la création du système d'information Visas (VIS) (doc. MARKT/11487/04/FR — WP 96) et document de travail sur la biométrie (doc. MARKT/10595/03/FR — WP 80).

([2]) A. Sasse, *Cybertrust and Crime Prevention: Usability and Trust in Information Systems*, dans «Foresight cybertrust and crime prevention project». 04/1151, 10 juin 2004, p.7, et United States General Accounting Office, Technology Assessment, «Using Biometrics for Border Security», GAO-03-174, Novembre 2002.

L'identification biométrique est aussi, par définition, un processus statistique, affecté d'un taux d'erreur normal de 0,5 à 1 % ([1]); par conséquent, le pourcentage des rejets injustifiés (False Rejection Rate) du système de contrôle aux frontières extérieures oscillera entre 0,5 et 1 %. Ce pourcentage varie en fonction d'un seuil déterminé par la politique des autorités compétentes en matière de gestion des risques (qui correspond à l'établissement d'un équilibre entre le nombre de personnes rejetées par erreur et acceptées par erreur). C'est pourquoi, il est exagéré de considérer que ces technologies assurent une «identification exacte» des personnes, comme l'affirme le considérant 9 de la proposition de règlement.

Une étude prospective récente ([2]) demandée par la commission LIBE du Parlement européen indique qu'il faudrait assortir l'introduction des systèmes biométriques de *procédures de secours* visant à offrir les garanties fondamentales nécessaires, ces systèmes n'étant ni accessibles à tous, ni infaillibles. De telles procédures devraient être mises en œuvre et utilisées sans porter atteinte à la dignité des personnes dont les données biométriques sont inexploitables et en évitant de faire porter sur ces personnes le poids des imperfections du système ([3]).

Le CEPD recommande par conséquent d'élaborer des procédures de secours et de les inclure dans la proposition. Ces procédures ne devraient porter atteinte ni au niveau de sécurité souhaité en matière de politique des visas ni à la dignité des personnes dont les empreintes digitales sont illisibles.

3.5. **Catégories de données particulières**

Certaines catégories de données (outre les données biométriques) nécessitent une attention particulière: les motifs de refus d'un visa (point 3.5.1) et les données concernant d'autres membres du groupe (point 3.5.2).

3.5.1. *Motifs de refus d'un visa*

Lorsque la décision a été prise de refuser un visa, les motifs de ce refus sont prévus par l'article 10, paragraphe 2, de la proposition. Ces motifs sont tout à fait standardisés.

— Les deux premiers motifs, qui figurent aux points a) et b), sont de nature plutôt administrative: non-présentation d'un document de voyage valable ou de documents prouvant le but et les conditions du séjour prévu.

— Le point c) fait référence au «signalement du demandeur aux fins de l'interdiction d'entrée», ce qui suppose une consultation de la base de données du SIS.

— Enfin, le point d) mentionne comme motif de refus d'un visa le fait que «le demandeur représente une menace pour l'ordre public, la sécurité intérieure, la santé publique ou les relations internationales d'un des États membres».

([1])

Élément biométrique	Visage	Doigt	Iris
FTE (% d'enregistrements impossibles)	n/a	4	7
FNMR (% de rejets)	4	2,5	6
FMR1 (% d'erreurs en termes de contrôle)	10	< 0,01	< 0,001
FMR2 (% d'erreurs en termes d'identification pour des bases de données de plus d'un million d'entrées)	40	0,1	n/a
FMR3 (% d'erreurs en termes de contrôle pour des bases de données de 500 entrées)	12	< 1	n/a

A. K. Jain et al., *Biometrics: A grand Challenge*, Actes de la conférence internationale sur la reconnaissance de formes, Cambridge, Royaume-Uni, août 2004

([2]) *Biométrie aux frontières: évaluation des impacts sur la société*, février 2005, Institut de prospective technologique scientifique, Direction générale «Centre commun de recherche», Commission européenne.

([3]) *Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques*, Conseil de l'Europe, 2005, page 11.

Le recours à chacun de ces motifs de refus doit se faire avec une grande prudence étant donné les conséquences qui en découlent pour la personne. De plus, les motifs visés aux points c) et d) impliquent le traitement de «données sensibles» au sens de l'article 8 de la directive 95/46/CE.

En particulier, le CEPD aimerait attirer l'attention sur la condition relative à la santé publique, qui lui semble vague et suppose le traitement de données très sensibles. D'après le commentaire des articles joint à la proposition, la référence à la menace pour la santé publique se fonde sur la «proposition de règlement du Conseil établissant le code communautaire relatif au régime de franchissement des frontières par les personnes» (COM(2004)391 final).

Le CEPD est conscient du fait qu'un critère de «santé publique» est couramment utilisé dans le législation communautaire sur la libre circulation des personnes et qu'il fait l'objet d'une application très stricte, comme le montre la directive 2004/38/CE du Parlement européen et du Conseil du 29 avril 2004 relative au droit des citoyens de l'Union et des membres de leurs familles de circuler et de séjourner librement sur le territoire des États membres. L'article 29 de cette directive fixe les conditions de la prise en compte d'une menace pour la santé publique: «Les seules maladies justifiant des mesures restrictives de la libre circulation sont les maladies potentiellement épidémiques telles que définies dans les instruments pertinents de l'Organisation mondiale de la santé ainsi que d'autres maladies infectieuses ou parasitaires contagieuses pour autant qu'elles fassent, dans le pays d'accueil, l'objet de dispositions de protection à l'égard des ressortissants de l'État membre d'accueil.»

— Il convient néanmoins de noter que la proposition de règlement portant sur le code communautaire n'est encore, à ce jour, qu'une proposition et que l'introduction, au niveau du règlement concernant le VIS, de la condition portant sur l'absence de menace pour la santé publique dépend de l'adoption dudit code communautaire.

— De plus, s'il est adopté, un tel motif de refus d'entrée devrait être interprété de manière restrictive. En effet, la proposition de code communautaire repose elle-même sur la directive 2004/38/CE susmentionnée.

Le CEPD recommande par conséquent l'ajout d'une référence à l'article 29 de la directive 2004/38/CE dans le texte de la proposition afin de s'assurer que la «menace pour la santé publique» sera interprétée à la lumière de cette disposition. En tout état de cause, étant donné la nature sensible des données concernées, il convient de ne traiter celles-ci que si la menace pour la santé publique est avérée, effective et suffisamment sérieuse.

3.5.2. *Données concernant d'autres membres du groupe*

L'article 2, point 7, définit les «membres du groupe» comme étant «les autres demandeurs avec lesquels le demandeur voyage, y compris le conjoint et les enfants qui l'accompagnent». Le commentaire des articles précise que les définitions figurant à l'article 2 de la proposition renvoient au traité ou à l'acquis de Schengen en matière de politique des visas, sauf pour quelques expressions, comme «membres du groupe», qui ont été définies spécialement aux fins du règlement. On peut donc supposer que cette définition ne renvoie pas à celle du «visa collectif» qui figure au point 2.1.4 des Instructions consulaires communes. Le commentaire des articles mentionne des «demandeurs voyageant en groupe avec d'autres demandeurs, par exemple dans le cadre d'un accord portant sur le statut de destination approuvée, ou avec des membres de leur famille».

Le CEPD insiste sur le fait qu'une définition précise et complète des «membres du groupe» devrait figurer dans le règlement. Dans la proposition actuelle, en l'absence de référence précise au traité ou à l'acquis de Schengen, le CEPD doit constater que la définition donnée est trop vague. La formulation actuelle permettrait à la notion de «membres du groupe» de comprendre des collègues, d'autres clients d'une même agence de voyage participant à un voyage organisé, etc. Les conséquences en sont assurément très importantes:

selon l'article 5 du projet de règlement, le dossier de demande d'un demandeur sera lié aux dossiers des autres membres du groupe.

3.6. **Conservation des données**

L'article 20 du projet de règlement prévoit de conserver chaque dossier de demande pendant cinq ans. La fixation d'un délai raisonnable est un choix politique du législateur communautaire.

Rien n'indique que le choix politique ainsi retenu dans la proposition serait déraisonnable — particulièrement au vu des raisons avancées dans le commentaire des articles — ni que les conséquences en seraient inacceptables, à condition que tous les mécanismes de correction appropriés soient mis en place. Cela signifie qu'il faut veiller à corriger ou à effacer les données dès lors que celles-ci cessent d'être exactes et, en particulier, lorsqu'une personne a obtenu la nationalité d'un État membre ou un statut qui ne nécessite pas sa présence dans le système.

De plus, lorsque les données sont encore présentes dans le système, elles ne peuvent pas influencer une décision ultérieure. Certains motifs de refus (signalement du demandeur aux fins de refuser l'entrée et menace pour la santé publique, en particulier) ont une durée de validité limitée. Le fait qu'il ait été légitime de refuser l'entrée à un moment donné ne devrait pas influencer les décisions suivantes. Il faut entièrement réévaluer la situation à chaque nouvelle demande de visa — cette obligation doit figurer de manière explicite dans le règlement

3.7. **Accès et utilisation des données**

3.7.1. *Observations préliminaires*

Tout d'abord, le CEPD reconnaît l'attention qui a été manifestement accordée à la réglementation de l'accès et du recours aux données du VIS. L'accès de chaque autorité est limité à certaines données et à certaines finalités. Il s'agit là d'une approche que le CEPD ne peut qu'encourager et dont les observations qui suivent visent à favoriser l'application la plus complète.

3.7.2. *Contrôles des visas aux points de passage aux frontières extérieures et sur le territoire*

L'article 16 de la proposition de règlement indique clairement les deux objectifs précis des contrôles des visas aux frontières extérieures:

— «vérifier l'identité de la personne», ce qui selon la définition signifie un «contrôle par comparaison de deux échantillons»;

— «vérifier l'authenticité du visa». Il serait possible, comme le proposent les normes de l'OACI, que la puce du visa fasse appel à un système de clé publique/clé privée (Public Key Infrastructure) pour procéder à cette vérification.

Ces deux objectifs peuvent parfaitement être atteints si les autorités compétentes contrôlant les visas n'ont accès qu'à la micropuce sécurisée. Dans ce cas particulier, il serait donc excessif de consulter la base de données centrale du VIS, solution qui impliquerait la connexion au VIS d'un plus grand nombre d'autorités et pourrait donc augmenter le risque d'abus. Elle pourrait également se révéler être une solution plus coûteuse puisque le nombre d'accès sécurisés et contrôlés au VIS et les besoins en formations spécifiques qui y sont liés augmenteraient sensiblement.

De plus, le caractère adéquat de la consultation des données selon les modalités prévues à l'article 16, paragraphe 2 est contestable. Ce paragraphe 2 indique en effet que, s'il ressort d'une première recherche que le VIS contient des données sur le demandeur (ce qui devrait en principe être le cas), l'autorité compétente peut consulter d'autres données, toujours dans le seul but de vérifier l'identité de la personne. Ces données concernent l'ensemble des informations relatives à la demande, aux photographies, aux empreintes digitales, ainsi qu'à tout visa précédemment délivré, annulé, retiré ou prorogé.

Si la vérification d'identité a abouti, la consultation du reste de ces données s'avère difficilement justifiable. Elle ne devrait vraiment être autorisée, dans des conditions restrictives, qu'en cas d'échec des procédures de vérification. Dans ce cas, il pourrait être fait appel aux données visées à l'article 16, paragraphe 2, dans le cadre d'une procédure de secours visant à établir l'identité de la personne. La consultation de ces données devrait être autorisée non pas à tous les agents chargés du contrôle des points de passage aux frontières, mais uniquement aux fonctionnaires chargés des cas difficiles.

Enfin, la définition des autorités autorisées à consulter les données devrait être plus précise. En particulier, la nature des «autorités compétentes chargées des contrôles sur le territoire de l'État membre» n'est pas claire. Le CEPD suppose qu'il s'agit des autorités compétentes chargées des contrôles *des visas* et estime que l'article 16 devrait être modifié en ce sens.

3.7.3. *Utilisation des données aux fins de l'identification et du retour des personnes en situation irrégulière, ainsi que pour les procédures d'asile*

Dans les cas décrits aux articles 17, 18 et 19 (retour des personnes en situation irrégulière et procédures d'asile), le VIS est utilisé à des fins d'identification. Les photographies font partie des données qui pourraient être exploitées dans ce but. Cependant, en l'état actuel de la technologie en matière de reconnaissance faciale automatique s'appuyant sur d'aussi grandes bases de données, les photographies ne peuvent pas servir à l'identification (contrôle par comparaison de plusieurs échantillons) car elles ne permettent pas d'obtenir de résultats fiables. Il n'y a donc pas lieu de les considérer comme étant des données convenant à l'identification.

Par conséquent, le CEPD suggère avec force de supprimer les références aux «photographies» dans les paragraphes 1 de ces articles tout en les conservant dans les paragraphes 2 (les photographies peuvent servir à vérifier une identité, mais non à procéder à une identification à partir d'une très grande base de données).

Une autre possibilité serait de modifier l'article 36 en précisant que les fonctionnalités liées au traitement des photographies à des fins d'identification ne seront mises en œuvre que lorsque cette technologie sera considérée comme fiable (éventuellement après un avis du comité technique).

3.7.4. *Publication de la liste des autorités ayant accès au VIS*

L'article 4 du projet de règlement prévoit la publication au Journal officiel de l'Union européenne de la liste des autorités compétentes désignées pour avoir accès au VIS dans chaque État membre. Cette publication devrait se faire régulièrement (chaque année), de manière à avertir des changements intervenus dans chaque État membre. Le CEPD insiste sur l'importance que revêt cette publication, en tant qu'outil de contrôle indispensable, tant au niveau européen que national ou local.

3.8. **Responsabilités**

Il convient de rappeler que le VIS s'appuiera sur une architecture centralisée comportant une base de donnée centrale servant à stocker l'ensemble des données relatives aux visas, ainsi que des interfaces nationales situées dans les États membres et permettant aux autorités compétentes de ces derniers d'accéder au système central. D'après les considérants 14 et 15 du projet de règlement, la directive 95/46/CE s'appliquera au traitement des données à caractère personnel par les États membres en application du règlement proposé, et le règlement (CE) nº 45/2001 s'appliquera aux activités de la Commission liées à la protection des données à caractère personnel. Comme l'indiquent ces considérants dans ce contexte, la proposition vise à clarifier certains points, notamment en ce qui concerne la responsabilité en matière d'utilisation des données et la supervision de la protection des données.

En fait, ces points semblent se rapporter à certains éléments cruciaux sans lesquels les garanties prévues par la directive 95/46/CE et le règlement (CE) nº 45/2001 ne pourraient pas s'appliquer ou ne seraient pas pleinement cohérents avec la proposition. La mise en œuvre d'une législation nationale en application de la directive suppose en principe l'établissement d'un responsable du traitement dans l'État membre concerné (article 4), alors que le règlement s'applique au traitement de données à caractère personnel par une institution ou un organisme communautaire dans l'exercice d'activités qui relèvent, en tout ou en partie, du droit communautaire (article 3).

Selon l'article 23, paragraphe 2, du projet de règlement, «les données sont traitées par le VIS pour le compte des États membres». Le paragraphe 3 précise que «chaque État membre désigne l'autorité qui sera considérée comme responsable du traitement, conformément à l'article 2, point d), de la directive 95/46/CE». Cela semble indiquer que, dans la logique de la directive, la Commission devrait être considérée comme un «sous-traitant», ce que confirme l'explication des articles ([1]).

Cette formulation tend à minimiser le rôle très important et en fait crucial qui échoit à la Commission pendant la phase de développement du système et dans le cadre de son fonctionnement opérationnel normal. Il est malaisé de faire coïncider exactement le rôle de la Commission avec le concept de responsable du traitement ou de sous-traitant: elle est soit un sous-traitant doté de pouvoirs inhabituels (notamment pour concevoir le système), soit un responsable du traitement aux attributions limitées (puisque les données sont saisies et utilisées par les États membres). Il faut reconnaître que la Commission joue vraiment un rôle *sui generis* ([2]) à l'égard du VIS.

Ce rôle significatif devrait être reconnu par le biais d'un description exhaustive des tâches de la Commission, plutôt que par une formulation qui ne correspond pas tout à fait à la réalité parce qu'elle est trop restrictive, qui ne change rien au fonctionnement du VIS et ne fait que créer de la confusion. Ce point est également important dans la perspective d'un contrôle cohérent et efficace du VIS (voir aussi le point 3.11). C'est pourquoi, le CEPD recommande la suppression de l'article 23, paragraphe 2.

Le CEPD aimerait souligner qu'une description complète des tâches de la Commission à l'égard du VIS est encore plus importante que la Commission pourrait confier ses tâches de gestion à un autre organisme. La «Fiche financière» annexée à la proposition évoque la possibilité d'un transfert de ces tâches à l'Agence pour la gestion des frontières extérieures. Dans un tel contexte, il est crucial que la Commission lève toutes les incertitudes concernant l'étendue de ses compétences, de manière à permettre à l'organisme qui lui succéderait de connaître les limites de l'action qu'il pourra mener.

3.9. **Sécurité**

Afin que les données à caractère personnel que contient sa banque de données bénéficient du niveau de protection requis, le VIS lui-même doit présenter un niveau de sécurité optimal; à cette fin, il faut instaurer des garanties adéquates contre les risques potentiels auxquels sont exposées tant l'infrastructure du système que les personnes concernées. Cette question est abordée dans plusieurs parties de la proposition, et certaines améliorations méritent d'être apportées dans ce domaine.

Les articles 25 et 26 de la proposition prévoient un certain nombre de mesures destinées à assurer la sécurité des données et précisent le type d'utilisations abusives qu'il y a lieu d'empêcher. Toutefois, il serait utile de compléter ces mesures par un dispositif permettant d'en surveiller l'efficacité et d'en rendre compte systématiquement. Le CEPD recommande en particulier d'ajouter à ces articles des dispositions instaurant un mécanisme d'audit (interne) systématique des mesures de sécurité.

Cette question doit être abordée en liaison avec l'article 40 de la proposition, qui traite du suivi et de l'évaluation. Le suivi et l'évaluation doivent porter non seulement sur les objectifs fixés en termes de résultats, de coût-efficacité et de qualité du service, mais aussi sur le respect des exigences légales, notamment dans le domaine de la protection des données. C'est pourquoi le CEPD recommande d'étendre le champ d'application de l'article 40 à la licéité du traitement des données.

En outre, en complément des dispositions de l'article 24, paragraphe 4, point c), et de l'article 26, paragraphe 2, point e), concernant l'accès des personnes dûment autorisées aux données, les États membres devraient aussi veiller à ce que des profils d'utilisateurs précis soient accessibles (tenus à la disposition des autorités de contrôle nationales pour effectuer des vérifications). Outre ces profils d'utilisateurs, les États membres doivent établir et tenir à jour en permanence la liste complète des identités des utilisateurs. La même obligation doit être faite à la Commission: il y a donc lieu de compléter dans cette optique l'article 25, paragraphe 2, point b).

([1]) Voir page 37 de la proposition.

([2]) Mais la définition du responsable du traitement qui figure dans la directive 95/46/CE et le règlement (CE) n° 45/2001 permet aussi d'établir plusieurs responsables du traitement, chargés de tâches différentes.

Les mesures de sécurité susmentionnées sont complétées par des garanties en matière de suivi et d'organisation. L'article 28 de la proposition définit les conditions et la finalité de l'établissement de relevés de toutes les opérations de traitement des données effectuées. Ces relevés doivent être conservés aux fins non seulement du suivi en matière de protection des données, mais aussi des vérifications internes régulières du VIS. Les rapports de vérification interne aideront les autorités de contrôle à s'acquitter efficacement de leur mission et à recenser les points faibles qu'elles examineront en détail dans le cadre de leur propre procédure de vérification.

3.10. **Droits de la personne concernée**

3.10.1. *Information de la personne concernée*

Il est de la plus haute importance, pour garantir un traitement loyal des données, d'informer la personne concernée. Il s'agit même d'une mesure indispensable pour protéger ses droits. Dans cette optique, l'article 30 de la proposition suit pour l'essentiel, l'article 10 de la directive 95/46/CE.

Toutefois, il serait utile d'apporter à cette disposition certaines modifications lui permettant de mieux répondre aux besoins du VIS. Si la directive prévoit la communication obligatoire de certaines informations, elle permet aussi d'en communiquer davantage si nécessaire ([1]). Par conséquent, il conviendrait de modifier l'article 30 afin de tenir compte des aspects suivants:

— les personnes concernées devraient aussi être informées de la durée de conservation des données;

— l'article 30, paragraphe 1, point e), porte sur «l'existence du droit d'accès aux données concernant la personne en question et du droit de rectification de ces données». Il serait plus adéquat de faire état de «l'existence du droit d'accès aux données concernant la personne en question et du droit *d'en demander la rectification ou l'effacement*». À cet égard, les personnes concernées devraient être informées de la possibilité de solliciter des conseils ou une assistance de la part des autorités de contrôle compétentes;

— enfin, l'article 30, paragraphe 1, point a), mentionne l'identité du responsable du traitement et de son représentant, le cas échéant. Le responsable du traitement étant toujours établi sur le territoire de l'Union européenne, cette dernière possibilité est sans objet.

3.10.2. *Droits d'accès, de rectification et d'effacement*

L'article 31, paragraphe 1, dernière phrase, dispose que «cet accès aux données ne peut être accordé que par un État membre». On peut supposer que cela signifie que l'accès aux données (ou leur transmission) peut être autorisé non par l'unité centrale, mais par tout État membre. Le CEPD recommande qu'il soit précisé expressément que la communication des données peut être demandée dans tout État membre.

En outre, le libellé de cette disposition laisse supposer que cet accès ne peut pas être refusé et qu'il sera accordé sans l'autorisation de l'État membre responsable. Cela expliquerait pourquoi les autorités nationales sont tenues de coopérer aux fins de l'application des droits prévus à l'article 31, paragraphes 2, 3 et 4, mais non de ceux prévus à l'article 31, paragraphe 1 ([2]).

3.10.3. *Assistance fournie par les autorités de contrôle*

L'article 33, paragraphe 2, prévoit que l'obligation, pour les autorités de contrôle nationales, d'assister la personne concernée et, si elle le demande, de la conseiller subsiste pendant toute la durée de la procédure judiciaire. La signification de ce paragraphe n'est pas claire. Les autorités de contrôle nationales n'ont pas toutes la même attitude quant à leur rôle dans le cadre d'une procédure judiciaire. En l'occurrence, il semble qu'elles doivent jouer le rôle de conseil du plaignant, ce qui est impossible dans nombre de pays.

([1]) La directive mentionne «toute information supplémentaire (…) dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données».

([2]) Par conséquent, l'article 31, paragraphe 3, concernant la coopération entre les autorités nationales aux fins de l'exercice des droits de rectification ou d'effacement pourrait être modifié, pour plus de clarté, comme suit: «si la demande *visée au paragraphe 2*…». Les demandes visées à l'article 31, paragraphe 1, (accès) ne supposent pas une coopération entre les autorités.

3.11. **Contrôle**

La proposition répartit les missions de contrôle entre les autorités de contrôle nationales et le CEPD. Cette solution est compatible avec l'approche adoptée dans la proposition quant au droit applicable et aux responsabilités en ce qui concerne le fonctionnement et l'exploitation du VIS, et répond à la nécessité d'instaurer un contrôle efficace. Le CEPD approuve par conséquent l'approche prévue aux articles 34 et 35.

Les autorités de contrôle nationales contrôlent la légalité du traitement des données à caractère personnel par les États membres, *y compris leur transmission du VIS et vers celui-ci*. Le CEPD supervise les activités de la Commission et *(…) contrôle en outre la licéité de la transmission des données à caractère personnel entre les interfaces nationales et le système central d'information sur les visas*. Il pourrait résulter des chevauchements, dès lors que l'autorité de contrôle nationale et le CEPD sont tous deux chargés de contrôler la légalité de la transmission des données entre les interfaces nationales et le système central d'information sur les visas.

Par conséquent, le CEPD propose de modifier l'article 34 de manière à préciser que les autorités de contrôle nationales contrôlent la légalité du traitement des données à caractère personnel par l'État membre, y compris pour ce qui concerne la transmission de ces données à partir de l'interface nationale du VIS et vers celle-ci.

Pour ce qui concerne le contrôle du VIS, il importe aussi de souligner qu'il faut veiller, dans une certaine mesure, à coordonner les activités des autorités de contrôle nationales et celles du CEPD, afin de garantir un niveau suffisant de cohérence et d'efficacité globale. En fait, il est nécessaire d'harmoniser la mise en œuvre du règlement et de rechercher des solutions communes aux problèmes communs. En outre, pour ce qui est de la sécurité, on ajoutera que le niveau de sécurité du VIS sera en dernière analyse déterminé par le niveau de sécurité de son maillon le plus faible. À cet égard également, la coopération entre le CEPD et les autorités de contrôle nationales doit être structurée et renforcée. L'article 35 devrait dès lors contenir une disposition dans ce sens, prévoyant que, une fois par an au moins, le CEPD sollicite la participation de toutes les autorités de contrôle nationales à une réunion.

3.12. **Mise en œuvre**

L'article 36, paragraphe 2, de la proposition dispose que «*les mesures nécessaires à la mise en œuvre technique des fonctionnalités visées au paragraphe 1 sont adoptées conformément à la procédure prévue par l'article 39, paragraphe 2*». L'article 39 prévoit que la Commission est assistée du comité institué en décembre 2001 ([1]), auquel plusieurs autres instruments font appel.

La mise en œuvre technique des fonctionnalités du VIS (interaction avec les autorités compétentes et modèle type de visa) pourrait à certains égards avoir un impact sur la protection des données. Par exemple, la décision d'insérer ou non une puce dans le visa aura une incidence sur la manière dont la base de données centrale sera utilisée, de même que les caractéristiques du modèle utilisé pour échanger les données biométriques contribueront à orienter la politique de protection des données ([2]) correspondante.

Le choix des technologies aura une incidence déterminante sur la mise en œuvre adéquate des principes de finalité et de proportionnalité et devrait dès lors faire l'objet d'un contrôle. Par conséquent, il serait préférable que les choix technologiques ayant une incidence significative sur la protection des données soient opérés par voie de règlement, selon la procédure de codécision. Ce n'est qu'à cette condition que le contrôle politique nécessaire pourra être exercé. Dans tous les autres cas ayant une incidence sur la protection des données, le CEPD devrait avoir la possibilité d'émettre un avis quant aux choix faits par ce comité.

3.13. **Interopérabilité**

Une condition préalable essentielle et déterminante pour garantir l'efficacité de l'exploitation de systèmes informatiques à grande échelle tels que le VIS consiste à en assurer l'interopérabilité. Celle-ci permet d'en réduire substantiellement le coût global et d'éviter les doubles emplois que ne manquent pas de provoquer des éléments disparates. L'interopérabilité peut aussi contribuer à atteindre l'objectif d'une politique commune en matière de visas par l'application de normes de procédure identiques à tous les éléments constitutifs de cette politique. Toutefois, il est capital de distinguer deux niveaux d'interopérabilité:

— il est hautement souhaitable d'assurer l'interopérabilité des systèmes des États membres de l'UE; en effet, les demandes de visa transmises par les autorités d'un État membre doivent être compatibles avec celles qui sont transmises par les autorités de tout autre État membre;

([1]) Règlement nº 2424/2001 du Conseil du 6 décembre 2001 relatif au développement du système d'information de Schengen de deuxième génération (SIS II).

([2]) La proposition de règlement du Conseil modifiant le règlement (CE) nº 1683/95 établissant un modèle type de visa, de septembre 2003, prévoyait une disposition analogue.

— par contre, on peut s'interroger sur l'opportunité d'assurer l'interopérabilité entre des systèmes servant à des finalités différentes ou avec les systèmes de pays tiers.

Une des précautions pouvant être prises pour limiter l'objet du système et éviter les utilisations détournées («function creep») consiste à utiliser des normes technologiques différentes. En outre, toute forme d'interaction entre deux systèmes distincts devrait faire l'objet d'une documentation complète. L'interopérabilité ne devrait jamais permettre qu'une autorité qui n'est pas habilitée à consulter ou à exploiter certaines données puisse y accéder par l'intermédiaire d'un autre système informatique.

À cet égard, le CEPD renvoie à la déclaration du Conseil du 25 mars 2004 sur la lutte contre le terrorisme, dans laquelle le Conseil demande à la Commission de présenter des propositions visant à accroître l'interopérabilité des bases de données européennes et d'envisager la création de synergies entre les systèmes d'information actuels et futurs (SIS II, VIS et EURODAC).

Il renvoie aussi à la discussion en cours concernant l'organisme auquel pourrait être confiée à l'avenir la gestion des différents grands systèmes (voir également à cet égard le point 3.8. du présent avis).

Le CEPD tient à souligner une fois encore que l'interopérabilité des systèmes ne peut être instaurée en violation du principe de limitation des finalités du traitement des données, et que toute proposition dans ce domaine devrait lui être soumise.

4. **CONCLUSIONS**

4.1. **Observations d'ordre général**

1. Le CEPD reconnaît que le développement d'une politique commune en matière de visas nécessite un échange efficace de données pertinentes. Le VIS constitue l'un des mécanismes susceptibles de garantir la fluidité des échanges d'informations. Le CEPD a examiné attentivement les éléments d'information présentés dans l'AIA. Bien que ceux-ci ne soient pas totalement concluants, il apparaît qu'il existe des raisons suffisantes pour justifier la mise en place du VIS en vue d'améliorer la politique commune en matière de visas.

   Néanmoins, ce nouvel instrument devrait se limiter à la collecte et à l'échange de données dans la mesure où ceux-ci sont nécessaires à la mise en place d'une politique commune en matière de visas et proportionnés à cet objectif.

2. Si la mise en place du VIS peut avoir des conséquences positives pour d'autres intérêts publics légitimes, elle ne modifie pas pour autant la finalité de ce système. Par conséquent, tous les éléments du VIS doivent être des instrumens nécessaires et proportionnés pour atteindre l'objectif politique susmentionné. En outre:

   — un accès systématique des services répressifs au système ne serait pas conforme à la finalité de ce dernier;

   — le CEPD recommande de rendre plus explicite la distinction entre «objet» et «effets bénéfiques» dans le libellé de l'article 1er, paragraphe 2;

   — l'interopérabilité avec d'autres systèmes ne peut être instaurée en violation du principe de limitation de l'objet du traitement des données.

3. Tout en reconnaissant les avantages que présente l'utilisation de données biométriques, le CEPD en souligne l'incidence majeure et suggère de l'assortir de garanties strictes. En outre, en raison des imperfections techniques du recours aux empreintes digitales, il y a lieu d'élaborer des procédures de secours et de les inclure dans la proposition.

4. Le présent avis devrait être mentionné dans le préambule du règlement, avant les considérants («vu l'avis …»).

4.2. **Autres observations**

5. Pour ce qui concerne les motifs de refus d'un visa, il conviendrait d'ajouter une référence à l'article 29 de la directive 2004/38/CE dans le texte de la proposition afin de s'assurer que la notion de «menace pour la santé publique» sera interprétée à la lumière de cette disposition.

6. Les données relatives aux «membres du groupe» ayant une signification particulière aux fins de la proposition, il conviendrait d'en donner une définition précise et complète.

7. Rien ne prouve que le choix politique qui a été fait dans la proposition s'agissant de la période de conservation des données soit déraisonnable ou qu'il aurait des conséquences inacceptables, à condition que tous les mécanismes de correction appropriés soient mis en place.

   Il convient également que la proposition indique explicitement que les données à caractère personnel doivent être entièrement réexaminées à chaque nouvelle demande de visa.

8. Pour ce qui concerne le contrôle des visas aux frontières extérieures, il conviendrait de modifier l'article 16 de la proposition, car un accès à la base de données centrale du VIS serait en l'occurrence disproportionné. Il suffirait que les autorités compétentes contrôlant les visas n'aient accès qu'à la puce sécurisée.

   En outre, si la vérification d'identité a abouti, la consultation du reste des données s'avère difficilement justifiable.

9. Pour ce qui concerne l'utilisation des données aux fins de l'identification et du retour des personnes en situation irrégulière ainsi que pour les procédures d'asile, il conviendrait de supprimer les références aux «photographies» dans les paragraphes 1 des articles 17, 18 et 19, tout en les conservant dans les paragraphes 2.

10. Pour ce qui concerne les responsabilités de la Commission et des États membres, il faudrait supprimer l'article 23, paragraphe 2.

11. Il conviendrait d'ajouter à la proposition des dispositions instaurant un mécanisme d'audit (interne) systématique des mesures de sécurité. Le champ d'application de l'article 40 devrait être étendu à la légalité du traitement des données. En outre,

   — les États membres doivent établir et tenir à jour en permanence la liste complète des identités des utilisateurs. La même obligation doit être faite à la Commission; il y a donc lieu de compléter dans cette optique l'article 25, paragraphe 2, point b);

   — l'article 28 de la proposition définit les conditions et la finalité de l'établissement de relevés de toutes les opérations de traitement. Ces relevés doivent être conservés aux fins non seulement du suivi en matière de protection des données mais aussi des vérifications internes régulières du VIS.

12. Pour ce qui concerne les droits de la personne concernée:

   — il conviendrait de modifier l'article 30 afin de veiller à ce que les personnes concernées soient aussi informées de la durée de conservation des données;

   — l'article 30, paragraphe 1, point e), devrait mentionner «l'existence du droit d'accès aux données concernant la personne en question et du droit d'en demander la rectification ou l'effacement»;

   — l'article 31, paragraphe 1, devrait indiquer de manière explicite que la communication de certaines données peut être demandée dans tout État membre.

13. En ce qui concerne le contrôle:

— il conviendrait de modifier l'article 34 de manière à préciser que les autorités de contrôle nationales contrôlent la légalité du traitement des données à caractère personnel par l'État membre, y compris pour ce qui concerne la transmission de ces données à partir de l'interface nationale du VIS et vers celle-ci;

— l'article 35 devrait dès lors contenir une disposition prévoyant que, uns fois par an au moins, le CEDP sollicite la participation de toutes les autorités de contrôle nationales à une réunion.

14. En ce qui concerne la mise en œuvre:

— il serait préférable que les choix technologiques ayant une incidence significative sur la protection des données soient opérés par voie de règlement, selon la procédure de codécision;

— dans les autres cas, le CEPD devrait avoir la possibilité de formuler des conseils quant aux choix faits par le comité prévu par la proposition.

Fait à Bruxelles, le 23 mars 2005.

Peter HUSTINX

Contrôleur européen de la protection des données