CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

Avis du contrôleur européen de la protection des données sur la proposition de décision du Conseil concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités des États membres compétentes en matière de sécurité intérieure et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière (COM (2005) 600 final)

(2006/C 97/03)

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 29 novembre 2005,

A ADOPTÉ L'AVIS SUIVANT:

1. INTRODUCTION

1.1. Observation préliminaire

La Commission a transmis la proposition de décision du Conseil concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités des États membres compétentes en matière de sécurité intérieure et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière (dénommée ci-après «la proposition») au Contrôleur européen de la protection des données (CEPD) par lettre datée du 24 novembre 2005. Le CEPD interprète cette lettre comme une demande d'avis à formuler à l'intention des institutions et organes communautaires, comme cela est prévu à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001. Le CEPD est d'avis qu'il convient de mentionner le présent avis dans le préambule de la décision.

Le CEPD estime qu'il est important de rendre un avis sur ce sujet sensible, car la proposition découle directement de la création du VIS, qui sera soumis à son contrôle, et sur lequel il a rendu un avis le 23 mars 2005 [1]. Dans cet avis, l'hypothèse d'un accès des services répressifs était déjà examinée (cf. ci-dessous), la création de nouveaux droits d'accès au VIS ayant une incidence déterminante sur le système en ce qui concerne la protection des données. C'est pourquoi un avis sur cette proposition constitue une suite nécessaire au premier avis.

1.2. Importance de la proposition

a) *Contexte*

La proposition est importante non seulement en elle-même, mais aussi parce qu'elle s'inscrit dans la tendance générale qui est d'accorder aux services répressifs l'accès à plusieurs systèmes d'information et d'identification à grande échelle. Cette tendance se reflète entre autres dans la communication de la Commission au Conseil et au Parlement européen du 24 novembre 2005 sur le renforcement de l'efficacité et de l'interopérabilité des bases de données européennes dans le domaine de la justice et des affaires intérieures et sur la création de synergies entre ces bases de données [2], et notamment au point 4.6 qui indique que *«En ce qui concerne l'objectif de lutte contre le terrorisme et la criminalité, le Conseil considère maintenant comme une lacune l'absence d'accès des autorités chargées de la sécurité intérieure aux données du VIS. On pourrait formuler la même remarque au sujet des données d'immigration contenues dans le SIS II et à propos des données EURODAC.»*

On pourrait donc voir dans cette proposition le précurseur d'instruments juridiques similaires mis au point pour d'autres bases de données. Il est donc primordial de définir dès le départ les cas où cet accès serait admissible.

---

[1] 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).

[2] Doc. COM (2005) 597 final.

b) *Incidence d'un nouveau droit d'accès au VIS*

Le CEPD convient qu'il est nécessaire pour les services répressifs de bénéficier des meilleurs outils possible pour identifier les auteurs d'actes terroristes et autres formes graves de criminalité. Il est en outre conscient que les données du VIS peuvent constituer, dans certaines circonstances, une source d'informations essentielle pour ces autorités.

Toutefois, l'octroi aux services répressifs de l'accès à des bases de données relevant du premier pilier, même s'il peut être justifié par la lutte contre le terrorisme, est loin d'être anodin. Il convient de ne pas perdre de vue que le VIS est un système d'information mis au point aux fins de l'application de la politique européenne en matière de visas et non comme instrument de répression. Un accès systématique constituerait en effet une grave violation du principe de limitation de la finalité. Il entraînerait une ingérence disproportionnée dans la vie privée des voyageurs qui ont accepté que leurs données fassent l'objet d'un traitement en vue d'obtenir un visa, et s'attendent à ce que ces données soient collectées, consultées et communiquées uniquement à cette fin.

Étant donné que les systèmes d'information sont conçus dans un but spécifique, avec des garanties, des dispositifs de sécurité et des conditions d'accès définis en fonction de cet objectif, l'octroi de l'accès systématique à des fins autres que la finalité initiale non seulement serait contraire au principe de limitation de la finalité, mais risquerait de rendre ces protections inadéquates ou insuffisantes.

Dans le même ordre d'idées, une modification aussi importante du système risquerait d'invalider les résultats de l'analyse d'impact (qui portait sur l'utilisation du système aux seules fins initialement prévues). Il en va de même pour les avis des autorités chargées de la protection des données. Celles-ci pourraient arguer que la nouvelle proposition modifie les fondements même de l'analyse qu'elles ont réalisée.

c) *Limitation stricte de cet accès*

À la lumière des observations qui précèdent, le CEPD souligne que l'accès des services de répression au VIS peut uniquement être accordé dans des circonstances précises, au cas par cas, et sous réserve de garanties strictes. En d'autres termes, il convient de limiter la consultation du VIS par les services de répression à des cas précis à l'aide de dispositifs techniques et juridiques appropriés.

Le CEPD avait déjà insisté sur ce point dans son avis sur le VIS en indiquant que: «Le CEPD est conscient que les services répressifs ont intérêt 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 cet objet. 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.»

En conclusion, les impératifs essentiels peuvent se résumer comme suit:

— L'accès systématique ne devrait pas être accordé: la décision doit garantir qu'il sera toujours examiné au cas par cas si l'accès d'autorités relevant du troisième pilier est nécessaire et proportionné. À cet égard, il est extrêmement important que le libellé de l'instrument juridique soit précis pour ne pas permettre une interprétation extensive qui aurait pour effet de rendre l'accès systématique.

— Dans les cas où l'accès est accordé, compte tenu de sa nature sensible, y a lieu de prévoir des garanties et des conditions appropriées, et notamment un régime global de protection des données applicable à l'utilisation des données au niveau national.

1.3. **Première observations**

Le CEPD reconnaît qu'une attention toute particulière a été portée dans l'instrument proposé à la protection des données, assurée principalement par la limitation de l'accès à des cas précis, uniquement dans le cadre de la lutte contre les formes graves de criminalité ([1]).

Le CEPD relève en outre les éléments positifs suivants:

— la limitation à certaines formes de criminalité visées dans la convention Europol;

— l'obligation pour les États membres d'établir une liste des autorités ayant accès au VIS et de rendre ces listes publiques;

— l'existence d'un point d'accès central par État membre (et d'une unité spécialisée au sein d'Europol) permettant de mieux filtrer les demandes d'accès et d'améliorer le contrôle;

— les règles strictes relatives à la transmission des données recueillies lors de l'accès au VIS prévues à l'article 8, paragraphe 5, de la proposition;

— l'obligation pour les États membres et Europol d'établir des relevés des personnes chargées de consulter les données.

2. **ANALYSE DE LA PROPOSITION**

2.1. **Observation préliminaire**

Pour pouvoir autoriser des autorités à consulter le VIS dans le cadre du troisième pilier, il faudrait que la proposition principale concernant le VIS, qui relève du premier pilier, contienne une clause passerelle définissant pour l'essentiel le contenu possible d'un instrument juridique relevant du troisième pilier tel que cette proposition. Lorsque le CEPD a rendu son avis sur le VIS, cette clause passerelle n'avait pas encore été introduite, et le CEPD n'était donc pas en mesure de la commenter. C'est pourquoi toutes les observations formulées ci-après s'entendent sous réserve du contenu de la clause passerelle.

([1]) Ce qui est conforme aux conclusions du Conseil de mars et juillet 2005, dans lesquelles il est demandé que l'accès au VIS soit accordé aux autorités des États membres compétentes en matière de sécurité intérieure *«dans le strict respect des règles relatives à la protection des données à caractère personnel»*.

2.2. **Objet de l'accès**

Pour assurer une limitation adéquate de l'accès au VIS, il importe de définir soigneusement les conditions d'accès au système. Le CEPD salue le fait qu'outre la décision proprement dite, l'exposé des motifs et les considérants (en particulier le considérant 7) de la proposition indiquent eux aussi très clairement que l'objectif est d'accorder l'accès au cas par cas uniquement.

L'article 5 de la proposition appelle une observation visant à en guider l'interprétation.

Cet article soumet les possibilités d'accès à des conditions de fond:

b) l'accès en consultation doit être nécessaire à la prévention ou à la détection d'infractions terroristes ou d'autres infractions pénales graves, ou aux enquêtes en la matière;

c) un cas spécifique doit rendre l'accès en consultation nécessaire (…) et

d) il doit exister, au vu d'éléments factuels, des motifs raisonnables de considérer que la consultation des données du VIS contribuera à la prévention ou à la détection des infractions en question, ou à l'enquête à leur sujet.

Ces conditions sont cumulatives, la condition b) relevant davantage d'une définition du champ d'application *ratione materiae*. En pratique, l'autorité qui sollicite l'accès doit se trouver face à une infraction pénale grave telle que visée au point b) de la proposition et d'un cas spécifique tel que visé au point c). Elle doit en outre être en mesure de démontrer que dans ce cas spécifique, la consultation du VIS contribuera à la prévention ou à la détection de l'infraction en question, ou à l'enquête à son sujet, comme le prévoit le point d).

Même si l'on interprète l'article 5 dans ce sens, le CEPD reste préoccupé par la formulation souple du point d), dont les termes «contribuera à» sont plutôt vagues. Il existe de nombreux cas dans lesquels les données du VIS pourraient «contribuer à» la prévention ou la détection d'une infraction grave. Afin de justifier un accès aux données du VIS en dérogation au principe de la limitation de la finalité, le CEPD estime que cette consultation devrait «contribuer substantiellement» à la prévention ou à la détection de l'infraction grave en question, ou à l'enquête à son sujet, et suggère de modifier l'article 5 en conséquence.

L'article 10 prévoit que les relevés doivent indiquer l'objet précis de l'accès. L' «objet précis» devrait inclure les éléments qui ont rendu la consultation du VIS nécessaire au sens de l'article 5, paragraphe 1, point d). Cela contribuerait à garantir que la nécessité de chaque consultation du VIS soit examinée et réduirait le risque que l'accès devienne systématique.

2.3. **Clés de recherche utilisées dans la base de données du VIS**

L'article 5, paragraphes 2 et 3, prévoit un accès aux données du VIS en deux étapes, aux termes duquel un ensemble de données n'est accessible que lorsqu'une réponse positive a été obtenue lors de la consultation du premier ensemble de données. Cette approche est en soi satisfaisante. Le premier ensemble de données semble toutefois très étendu. On peut notamment s'interroger de la pertinence de données telles que celles mentionnées à l'article 5, paragraphe 2, points e) et i) pour le premier ensemble de données:

— Le «but du voyage» est une clé qui paraît trop générale pour permettre une consultation efficace du système. Elle risque en outre d'entraîner le profilage de voyageurs sur la base de ce seul élément.

— En ce qui concerne les photographies, la possibilité d'interroger une base de données aussi vaste, sur la base de photos, est limitée; en l'état actuel de la technologie, les résultats de ces recherches comprennent un taux inacceptable de correspondances fausses. Les conséquences d'une identification incorrecte sont très graves pour la personne concernée.

Le CEPD demande donc que les données figurant à l'article 5, paragraphe 2, points e) et i) soient considérées comme des informations supplémentaires accessibles si la première consultation montre qu'il y a déjà des données dans le système et qu'elles soient déplacées à l'article 5, paragraphe 3.

Une alternative serait de conditionner la possibilité d'interroger la base de données à partir de photographies à une évaluation de cette technologie par le comité consultatif et de ne l'appliquer que lorsque cette technologie sera au point et considérée suffisamment fiable.

2.4. **Application aux États membres auxquels le règlement relatif au VIS n'est pas applicable**

L'accès au VIS en consultation peut être accordé aux autorités compétentes en matière de sécurité intérieure dans les États membres auxquels le règlement relatif au VIS n'est pas applicable. Ces services doivent effectuer la consultation par l'intermédiaire d'un État membre auquel le VIS est applicable, en respectant les conditions énoncées à l'article 5, paragraphe 1, points b) à d) (c'est-à-dire en s'appuyant sur le cas par cas), et soumettre une demande écrite dûment motivée.

Le CEPD souhaite attirer l'attention sur la nécessité d'imposer certaines conditions au traitement allant au-delà de la consultation. Aux termes de la règle s'appliquant aux États membres auxquels le VIS est applicable, une fois extraites du VIS, les données doivent être traitées conformément à la décision-cadre relative à la protection des données dans le troisième pilier (voir ci-dessous). La même condition devrait s'appliquer aux États membres auxquels le règlement relatif au VIS n'est pas applicable, mais qui consultent les données du VIS. Ce même raisonnement devrait s'appliquer à l'établissement des relevés en vue de futurs contrôles. Par conséquent, le CEPD recommande d'ajouter à l'article 6 de la proposition un paragraphe aux termes duquel les articles 8 et 10 de la décision s'appliquent également à tous les États membres auxquels le règlement relatif au VIS n'est pas applicable.

2.5. **Régime de protection des données**

a) *Application de la décision-cadre relative à la protection des données dans le troisième pilier*

Étant donné que l'accès par les autorités compétentes en matière de sécurité intérieure constitue une exception aux objectifs du VIS, il devrait faire l'objet d'un régime de protection des données cohérent qui permette d'assurer un niveau élevé dans la protection des données extraites du VIS et traitées par les autorités nationales ou par Europol.

Conformément à l'article 8 de la proposition, la décision-cadre relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (ci-après la décision-cadre) est applicable aux traitements de données à caractère personnel réalisés en vertu de la décision proposée. En ce qui concerne la protection des données, la présente proposition devrait donc être considérée comme une *lex specialis* qui s'ajoute ou précise une *lex generalis* (par exemple, la décision-cadre). Par exemple, les règles relatives au transfert ultérieur de données sont plus strictes dans cette proposition et devraient être suivies. Il en va de même des motifs de l'accès aux données.

b) *Portée*

Le CEPD salue le fait que le régime de protection des données de la décision-cadre soit applicable à tout traitement de données à caractère personnel réalisé en vertu de la décision proposée. Cela signifie que le niveau de protection des données doit être équivalent, quelle que soit l'autorité qui consulte les données du VIS.

Étant donné que l'article 2 utilise un critère fonctionnel pour définir ces autorités («les autorités des États membres qui sont chargées de la prévention et de la détection des infractions terroristes et autres infractions pénales graves, ainsi que des enquêtes en la matière»), cette définition pourrait s'appliquer aux services de renseignement de même qu'aux services répressifs. Par conséquent, les services de renseignement qui consultent le VIS sont en principe soumis aux mêmes obligations en matière de protection des données, ce qui est évidemment un signe positif.

Toutefois, en raison des doutes que pourrait susciter l'interprétation relative à l'applicabilité de la décision-cadre aux services de renseignement, lorsque ceux-ci accèdent aux données du VIS, le CEPD propose de libeller l'article comme suit:

«Dans les cas où la décision-cadre (...) n'est pas applicable, les États membres doivent assurer un niveau de protection des données au moins équivalent à celui de la décision-cadre.»

c) *Contrôle*

En ce qui concerne le libellé de l'article 8, il faudrait préciser que le paragraphe 1 concerne le traitement des données à l'intérieur du territoire des États membres. Les paragraphes 2 et 3 précisent leur champ d'application (traitement des données par Europol et par la Commission). Il faudrait donc préciser que le paragraphe 1 concerne un autre cas de figure.

L'attribution des compétences de contrôle en fonction des activités respectives des différents acteurs est une bonne approche. Il manque toutefois un élément: la nécessité d'une approche coordonnée dans l'exercice du contrôle. Comme déjà indiqué dans l'avis du CEPD sur le VIS: «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. En fait, il est nécessaire d'harmoniser la mise en œuvre du règlement et de rechercher des solutions communes aux problèmes communs.

L'article 35 (de la proposition relative au VIS) devrait dès lors contenir une disposition dans ce sens, prévoyant que, une fois par an au moins, le CEPD invite toutes les autorités de contrôle nationales à une réunion.»

Il en va de même pour cet usage spécifique du système VIS (avec, dans ce cas, la participation également de l'autorité de contrôle commune d'Europol). Le contrôle devrait être pleinement compatible avec le contrôle du «VIS dans le premier pilier», étant donné qu'il s'agit du même système. Par ailleurs, les réunions de coordination convoquées par le CEPD s'adressant à toutes les parties concernées par le contrôle est également le modèle choisi dans le cadre du contrôle d'autre systèmes d'information à grande échelle, tels qu'Eurodac.

Le CEPD est conscient du fait que la coordination est dans une certaine mesure prévue dans la proposition, puisque cette dernière mentionne le futur rôle du groupe de protection des personnes à l'égard du traitement des données à caractère personnel institué par l'article 31 de la proposition de décision-cadre. Toutefois, il conviendrait de préciser une nouvelle fois que le contrôle proprement dit ne relève pas de la mission de l'instance consultative.

Le CEPD propose d'ajouter une disposition aux termes de laquelle la réunion de coordination convoquée par CEPD dans le cadre du contrôle du «VIS du premier pilier» est également compétente pour les données traitées en vertu de cette proposition et, à cet effet, l'autorité de contrôle commune d'Europol devrait être représentée.

2.6. **Audit interne**

L'article 12 de la proposition prévoit des systèmes de suivi du VIS. Le CEPD estime que ce suivi ne doit pas uniquement porter sur les résultats, le rapport coût-efficacité et la qualité du service, mais également sur la conformité aux exigences prévues par la législation, notamment dans le domaine de la protection des données. L'article 12 devrait par conséquent être modifié en conséquence.

Afin de procéder à cette vérification interne de la légalité du traitement, la Commission devrait être autorisée à utiliser les relevés conservés conformément à l'article 10 de la proposition. En conséquence, l'article 10 devrait stipuler que les relevés établis ne doivent pas seulement être stockés pour assurer le suivi de la protection des données et garantir leur sécurité, mais également pour procéder à des vérifications internes régulières du VIS. Les rapports de vérification interne contribueront à la tâche de contrôle du CEPD et des autres contrôleurs qui seront plus à même de sélectionner leurs domaines prioritaires de contrôle.

3. **CONCLUSION**

À la lumière de ce qui précède, le CEPD souligne l'importance cruciale de ne permettre l'accès aux autorités compétentes chargées de la sécurité intérieure et à Europol, qu'au cas par cas et selon des mesures de précaution très strictes. La proposition atteint ce but d'une manière globalement satisfaisante, en dépit des quelques améliorations dont elle pourrait faire l'objet et qui sont suggérées dans l'avis ci-après.

— L'une des conditions d'accès au VIS conformément à l'article 5 devrait être que la consultation contribuera de «manière substantielle» à la prévention et à la détection d'une infraction grave; les relevés exigés par l'article 10 devraient permettre une évaluation de cette condition dans chaque cas individuel.

— Les deux clés de recherche pour l'accès au VIS, mentionnées à l'article 5, paragraphe 2, a savoir «le but du voyage» et les «photographies» devraient être réexaminées et devraient être mises à disposition, en tant qu'information supplémentaire en cas de réponse positive.

— Le niveau de protection des données appliqué à la consultation devrait être équivalent, quelle que soit l'autorité consultant les données VIS. L'article 8 et l'article 10 devraient également s'appliquer aux États membres auxquels le Règlement VIS n'est pas applicable.

— Une approche coordonnée en matière de contrôle devrait être assurée, également en ce qui concerne l'accès au VIS tel qu'il est prévu dans la présente proposition.

— Les dispositions relatives aux systèmes de suivi devraient également permettre des vérifications internes de conformité avec les exigences de protection des données.

Fait à Bruxelles, le 20 janvier 2006.

Peter HUSTINX

Contrôleur européen de la protection des données