CONSEIL DE L'UNION EUROPÉENNE

Bruxelles, le 28 avril 2004 (06.05)
(OR. en)

8958/04

CRIMORG 36
TELECOM 82

NOTE DE TRANSMISSION

de:	la République française, de l'Irlande, du Royaume de Suède et du Royaume-Uni
Date de réception:	le 28 avril 2004
Destinataire:	Monsieur Javier Solana, Secrétaire général/Haut représentant
Objet:	Projet de décision-cadre sur la rétention de données traitées et stockées en rapport avec la fourniture de services de communications électroniques accessibles au public ou de données transmises via des réseaux de communications publics, aux fins de la prévention, la recherche, la détection, la poursuite de délits et d'infractions pénales, y compris du terrorisme

Monsieur le Secrétaire général/Haut représentant,

En application de l'article 31, paragraphe 1, point c), et de l'article 34, paragraphe 2, point b), du traité sur l'Union européenne, veuillez trouver ci-joint une proposition de la République française, de l'Irlande, du Royaume de Suède et du Royaume-Uni en vue de l'adoption par le Conseil d'un projet de décision-cadre sur la rétention de données traitées et stockées en rapport avec la fourniture de services de communications électroniques accessibles au public ou de données transmises via des réseaux de communications publics, aux fins de la prévention, la recherche, la détection et la poursuite de délits et d'infractions pénales, y compris du terrorisme.

Nous vous saurions gré de bien vouloir prendre les mesures nécessaires, conformément à l'article 17 du règlement intérieur du Conseil, pour que le texte de la présente initiative soit publié au Journal officiel et transmis pour information au Parlement européen.

(Formule de politesse).

Signé:

Pierre SELLAL
Représentant permanent
de la France

Anne ANDERSON
Représentant permanent
de l'Irlande

Sven-Olof PETERSSON
Représentant permanent
de la Suède

John GRANT
Représentant permanent
du Royaume-Uni

Projet de décision-cadre

sur la rétention de données traitées et stockées en rapport avec la fourniture de services de communications électroniques accessibles au public ou de données transmises via des réseaux de communications publics, aux fins de la prévention, la recherche, la détection et la poursuite de délits et d'infractions pénales, y compris du terrorisme

LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur l'Union européenne, et notamment son article 31, paragraphe 1, point c), et son article 34, paragraphe 2, point b),

vu l'initiative de la République française, de l'Irlande, du Royaume de Suède et du Royaume-Uni,

vu l'avis du Parlement européen,

considérant ce qui suit:

1. Afin d'offrir un niveau élevé de protection dans un espace de liberté, de sécurité et de justice, il y a lieu de procéder de façon adéquate à la prévention, la recherche, la détection et la poursuite des délits et des infractions pénales.

2. Le Conseil et la Commission, dans leur plan d'action sur la meilleure façon de mettre en œuvre les dispositions du traité d'Amsterdam relatives à l'établissement d'un espace de liberté, de sécurité et de justice, le Conseil européen, réuni à Tampere les 15 et 16 octobre 1999, et le Conseil européen, réuni à Santa Maria da Feira les 19 et 20 juin 2000, dans leurs conclusions respectives, la Commission européenne, dans son tableau de bord, et le Parlement européen, dans sa résolution du 19 mai 2000, appellent à agir contre la criminalité utilisant les technologies avancées.

3. Dans les conclusions de sa session tenue le 20 septembre 2001, le Conseil demande que l'on veille à ce que les services répressifs soient en mesure d'enquêter sur des actes criminels comportant l'utilisation de systèmes de communications électroniques et de prendre des mesures contre les auteurs de ces délits, tout en assurant un équilibre entre la protection des données à caractère personnel et la nécessité, pour les autorités répressives, d'avoir accès à des données pour les besoins de l'enquête judiciaire. Dans ses conclusions de sa session tenue le 19 décembre 2002, le Conseil a noté que, du fait de l'accroissement important des possibilités qu'offrent les communications électroniques, les données relatives à l'utilisation de celles-ci constituent aujourd'hui un instrument particulièrement important et utile pour la prévention, la recherche, la détection et la poursuite de délits et d'infractions pénales, notamment de la criminalité organisée et du terrorisme.

4. Dans sa déclaration sur la lutte contre le terrorisme qu'il a adoptée le 25 mars 2004, le Conseil européen a chargé le Conseil d'envisager des mesures en vue de l'établissement de règles relatives à la conservation, par les fournisseurs de services, des données relatives au trafic des communications, en vue de leur adoption d'ici juin 2005.

5. Il est essentiel de pratiquer la rétention des données qui se trouvent sur des réseaux de communications publics et qui ont été générées par une communication, dénommées ci-après "données", aux fins de la prévention, la recherche, la détection et la poursuite de délits et d'infractions pénales commis au moyen de systèmes de communications électroniques. La présente proposition ne porte que sur les données générées par une communication et non sur le contenu proprement dit des informations communiquées. Plus particulièrement, il est nécessaire de procéder à la rétention des données en vue de remonter à la source de contenus illégaux, tels que des matériaux à caractère pédophile, raciste et xénophobe, ainsi qu'à l'origine des attaques informatiques, et d'identifier les individus utilisant des réseaux de communications électroniques pour mener des activités relevant de la criminalité organisée et du terrorisme.

6. Il ne suffit pas de stocker des données spécifiques concernant des personnes précises dans des cas déterminés. Au cours d'une enquête, il se peut que l'on ne puisse identifier les données voulues ou les personnes concernées que de nombreux mois ou de nombreuses années après la communication d'origine. Par conséquent, il y a lieu de retenir certains types de données, qui sont déjà traitées et stockées à des fins de facturation, des fins commerciales ou toute autre fin légitime, pendant un laps de temps supplémentaire en prévision du fait que ces données pourraient s'avérer nécessaires à l'avenir en cas d'enquête ou de poursuites judiciaires. La présente décision-cadre porte donc sur la rétention de données et non sur les conditions de stockage.

7. Eu égard à l'importance que revêt la rétention de données, l'article 15 de la directive 2002/58/CE permet l'adoption de mesures législatives autorisant, sous certaines conditions, la rétention de données pour assurer la prévention, la recherche, la détection ou la poursuite de délits et d'infractions pénales. La présente décision-cadre ne porte pas sur les autres objectifs visés à l'article 15 de ladite directive et ne prévoit donc pas de règles applicables à la rétention de données pour sauvegarder la sécurité nationale - c'est-à-dire la sûreté de l'État - la défense et la sécurité publique. Elle n'a pas non plus pour objet les utilisations non autorisées du système de communications électroniques lorsque ces utilisations ne constituent pas une infraction pénale.

8. De nombreux États membres ont voté des lois sur la rétention a priori de données pour permettre la prévention, la recherche, la détection ou la poursuite de délits et d'infractions pénales. Des travaux en la matière sont en cours dans d'autres États membres. La teneur de ces lois varie considérablement d'un État membre à l'autre.

9. Les différences existantes entre les législations des États membres nuisent à la coopération entre les autorités compétentes à des fins de prévention, de recherche, de détection et de poursuite des délits et des infractions pénales. Dans le but de garantir une coopération policière et judiciaire efficace en matière pénale, il y a donc lieu de veiller à ce que tous les États membres prennent les mesures nécessaires pour retenir certains types de données durant une période déterminée dans le cadre de paramètres définis, aux fins de la prévention, la recherche, la détection et la poursuite de délits et d'infractions pénales, y compris du terrorisme. Il conviendrait que ces données soient mises à la disposition des autres États membres conformément aux instruments de la coopération judiciaire en matière pénale adoptés en vertu du titre VI du traité sur l'Union européenne. Il importe également de se conformer aux instruments qui n'ont pas été adoptés en vertu dudit titre mais auxquels les États membres ont adhéré et auxquels il est fait référence dans les instruments précités.

10. La rétention a priori de données et l'accès à celles-ci pourraient constituer une ingérence dans la vie privée d'un individu. Toutefois, une telle ingérence n'enfreint pas les règles internationales applicables en matière de droit au respect de la vie privée et de traitement des données à caractère personnel, qui sont énoncées notamment dans la Convention européenne des droits de l'homme du 4 novembre 1950, dans la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, du 28 janvier 1981, et dans les directives 95/46/CE, 97/66/CE et 2002/58/CE, lorsqu'une telle ingérence est prévue par la loi et qu'elle est appropriée, rigoureusement proportionnée au but poursuivi, nécessaire dans une société démocratique et subordonnée à des garanties adéquates, afin de permettre la prévention, la recherche, la détection et la poursuite des délits et des infractions pénales, y compris du terrorisme.

11. Compte tenu de la nécessité, d'une part, de veiller à ce que les données soient retenues a priori de manière efficace et harmonisée et, d'autre part, de laisser aux États membres une grande latitude pour établir leurs propres évaluations, étant donné les différences qui existent entre leurs systèmes de justice pénale, il convient de fixer des paramètres en ce qui concerne la rétention a priori de données.

12. Des données peuvent être retenues a priori pendant des laps de temps différents en fonction des types de données. La durée de la période de rétention applicable à chaque type de données dépendra, d'une part, de l'utilité de ces données pour la prévention, la recherche, la détection et la poursuite de délits et d'infractions pénales et, d'autre part, du coût de leur rétention. La durée de la période de rétention devra être proportionnées, à l'utilité de ces données pour la prévention, la recherche, la détection et la poursuite des délits et des infractions pénales, en regard de l'intrusion dans la vie privée qu'occasionnera la rétention en cas de communication des données retenues.

13. L'établissement des listes énumérant les types de données à retenir doit assurer un équilibre entre, d'une part, les avantages que représente la rétention de chaque type de données pour la prévention, la recherche, la détection et la poursuite de délits et d'infractions pénales et, d'autre part, le niveau d'ingérence dans la vie privée qui en résultera.

14. La décision-cadre ne s'applique pas à l'accès aux données au moment de la transmission, par la surveillance, par l'interception ou par l'enregistrement de télécommunications.

15. Les États membres doivent veiller à ce que l'accès aux données retenues soit conforme aux règles de protection de la vie privée telles qu'elles sont définies dans le droit international applicable à la protection des données à caractère personnel.

16. Les États membres doivent veiller à ce que la mise en œuvre de la décision-cadre s'accompagne de consultations adéquates avec le secteur industriel,

A ARRÊTÉ LA PRÉSENTE DÉCISION-CADRE:

Article premier

Champ d'application et objectif

1. La présente décision-cadre vise à faciliter la coopération judiciaire dans le domaine pénal par le rapprochement des législations des États membres applicables à la rétention de données traitées et stockées par les fournisseurs d'un service de communications électroniques accessible au public ou d'un réseau de communications public, aux fins de la prévention, la recherche, la détection et la poursuite de délits ou d'infractions pénales, y compris du terrorisme.

2. La présente décision-cadre ne s'applique pas au contenu des communications échangées, en ce compris les informations consultées au moyen d'un réseau de communications électroniques dans les cas définis dans le droit national.

3. Un État membre peut décider de ne pas appliquer le paragraphe 1 du présent article, en ce qui concerne la prévention de délits ou d'infractions pénales comme une des finalités de la rétention de données qui sont traitées et stockées, si ledit État membre devrait rejeter cette finalité à l'issue d'une procédure ou d'un processus consultatif au niveau national. Les États membres qui décident à un moment donné de faire usage de cette dérogation doivent en avertir le Conseil et la Commission.

4. La présente décision-cadre ne préjuge pas:

   - les règles applicables à la coopération judiciaire en matière pénale en ce qui concerne l'interception et l'enregistrement de télécommunications;

   - les activités relatives à la sécurité publique, à la défense et à la sécurité nationale (c'est-à-dire la sûreté de l'État);

   - les règles nationales relatives à la rétention de types de données qui ne sont pas détenues par les fournisseurs d'un service de communications à des fins professionnelles.

Article 2

Définitions

1. Aux fins de la présente décision-cadre:

   a) la définition du terme "données" inclut les données relatives au trafic et les données de localisation telles qu'elles sont définies à l'article 2 de la directive 2002/58/CE et englobe les données relatives à l'abonné et celles relatives à l'utilisateur pour autant qu'elles soient liées aux données concernées;

   b) on entend par "données relatives à l'utilisateur" les données concernant toute personne physique utilisant un service de communications électroniques accessible au public à des fins privées ou professionnelles sans être nécessairement abonnée à ce service;

   c) on entend par "données relatives à l'abonné" les données concernant toute personne physique qui s'abonne à un service de communications électroniques accessible au public à des fins privées ou professionnelles sans nécessairement utiliser ce service.

2. Aux fins de la présente décision-cadre, les données incluent:

   a) les données nécessaires pour retrouver et identifier la source d'une communication, y compris des informations à caractère personnel, des informations sur les contacts et des informations permettant d'identifier les services pour lesquels un abonnement a été souscrit;

   b) les données nécessaires pour déterminer l'acheminement et la destination d'une communication;

   c) les données nécessaires pour déterminer l'heure, la date et la durée d'une communication;

   d) les données nécessaires pour identifier la télécommunication;

e) les données nécessaires pour identifier le dispositif de communication ou ce qui est censé être le dispositif;

f) les données nécessaires pour localiser la communication, au début de la communication et pendant toute la durée de celle-ci.

3. Les données précitées incluent les données générées par des services fournis dans le cadre des infrastructures, architectures et protocoles de communication suivants:

a) la téléphonie à l'exception des services de messages courts, des services de médias électroniques et des services de messagerie multimédias;

b) les services de messages courts, les services de médias électroniques et les services de messagerie multimédias fournis dans le cadre d'un service de téléphonie;

c) les protocoles Internet, y compris pour le courrier électronique, les protocoles de téléphonie vocale sur Internet, le web, les protocoles de transfert de fichiers, les protocoles de transfert réseau, les protocoles de transfert hypertexte, la téléphonie vocale à large bande et les sous-ensembles de numéros de protocoles Internet - données de traduction des adresses réseau.

4. Les développements technologiques futurs destinés à faciliter la transmission de communications relèvent du champ d'application de la présente décision-cadre.

Article 3

Rétention de données

Chaque État membre prend les mesures nécessaires pour veiller à ce que la rétention, aux fins de la coopération judiciaire en matière pénale, de données traitées et stockées par les fournisseurs d'un réseau de communications public ou de services de communications électroniques accessibles au public, y compris les données relatives à l'abonné et celles relatives à l'utilisateur pour autant qu'elles soient liées aux données concernées, respecte les dispositions de la présente décision-cadre.

Article 4

Durée de la période de rétention des données

1. Chaque État membre prend les mesures nécessaires afin de veiller à ce que les données soient retenues pendant une période d'au moins douze mois et de maximum 36 mois après leur création. Les États membres peuvent fixer des périodes de rétention plus longues en fonction de critères nationaux pour autant qu'une rétention plus longue constitue une mesure nécessaire, appropriée et proportionnée dans une société démocratique.

2. Un État membre peut décider de déroger au paragraphe 1 du présent article, pour ce qui concerne les types de données visées à l'article 2, paragraphe 2, et transmises au moyen des modes de communication énoncés à l'article 2, paragraphe 3, points b) et c), si ledit État membre considère ne pas pouvoir accepter, à l'issue d'une procédure ou d'un processus consultatif national, les périodes de rétention fixés au paragraphe 1 du présent article. L'État membre qui décide à un moment donné de faire usage de la présente dérogation doit en avertir le Conseil et la Commission en stipulant les nouveaux délais adoptés pour le type de données considéré. Les dérogations sont réexaminées chaque année.

Article 5

Accès aux données aux fins de la coopération judiciaire en matière pénale

Toute demande qu'un État membre adresse à un autre État membre afin d'avoir accès aux données visées à l'article 2 est conforme aux dispositions des instruments de la coopération judiciaire en matière pénale adoptés en vertu du titre VI du traité sur l'Union européenne et la réponse qui y est apportée respecte les mêmes formes. L'État membre auquel la demande a été adressée peut subordonner son consentement au respect des conditions qui seraient éventuellement imposées si un cas similaire se présentait au niveau national.

Article 6

Protection des données

Les États membres veillent à ce que la rétention de données effectuée en vertu de la présente décision-cadre respecte au minimum les principes de protection des données énoncés ci-après et ils établissent des voies de recours conformément aux dispositions du chapitre III de la directive 95/46/CE sur les recours juridictionnels, la responsabilité et les sanctions:

a) les autorités compétentes ont accès aux données pour des finalités déterminées, explicites et légitimes, au cas par cas et dans le respect du droit national; ces données ne seront pas traitées ultérieurement de manière incompatible avec ces finalités;

b) les données sont adéquates, pertinentes et non excessives au regard des finalités poursuivies. Elles sont traitées loyalement et licitement;

c) les données auxquelles les autorités compétentes ont accès sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement;

d) la confidentialité et l'intégrité des données sont garanties;

e) les données auxquelles l'accès est accordé sont exactes et toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées.

Article 7

Sécurité des données

Les États membres veillent à ce que la rétention de données effectuée en vertu de la présente décision-cadre respecte au minimum les principes de sécurité des données énoncés ci-après, tout en tenant compte des dispositions de l'article 4 de la directive:

a) les données retenues sont de la même qualité que les données sur le réseau;

b) les données font l'objet de mesures techniques et d'organisation appropriées pour les protéger contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, ainsi que contre toute autre forme de traitement illicite;

c) toutes les données sont détruites à la fin de la période de rétention, à l'exception des données ayant fait l'objet d'un accès et qui ont été conservées;

d) il appartient à chaque État membre de définir dans son droit national la procédure à suivre pour avoir accès aux données retenues et pour conserver les données ayant fait l'objet d'un accès.

Article 8

Mise en œuvre

Les États membres prennent les mesures nécessaires pour se conformer aux dispositions de la présente décision-cadre avant le [… juin 2007], dans un délai de deux ans à compter de la date de son adoption.

À la même date, les États membres communiquent au Secrétariat général du Conseil et à la Commission le texte des dispositions transposant dans leur droit national les obligations découlant de la présente décision-cadre. Le Secrétariat général du Conseil communique aux États membres les informations reçues en application du présent article.

La Commission présente au Conseil avant le [… 1er janvier 2008] un rapport évaluant dans quelle mesure les États membres se sont conformés aux dispositions de la présente décision-cadre.

Article 9

Entrée en vigueur

La présente décision-cadre entre en vigueur le vingtième jour suivant celui de sa publication au Journal officiel de l'Union européenne.

Fait à Bruxelles,

_____