

PARLEMENT EUROPÉEN

2004



2009

Document de séance

FINAL
A6-0365/2005

28.11.2005

*****|**

RAPPORT

sur la proposition de directive du Parlement européen et du Conseil sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, et modifiant la directive 2002/58/CE
(COM(2005)0438 – C6-0293/2005 – 2005/0182(COD))

Commission des libertés civiles, de la justice et des affaires intérieures

Rapporteur: Alexander Nuno Alvaro

Légende des signes utilisés

- * Procédure de consultation
majorité des suffrages exprimés
- **I Procédure de coopération (première lecture)
majorité des suffrages exprimés
- **II Procédure de coopération (deuxième lecture)
majorité des suffrages exprimés pour approuver la position commune
majorité des membres qui composent le Parlement pour rejeter ou amender la position commune
- *** Avis conforme
majorité des membres qui composent le Parlement sauf dans les cas visés aux art. 105, 107, 161 et 300 du traité CE et à l'art. 7 du traité UE
- ***I Procédure de codécision (première lecture)
majorité des suffrages exprimés
- ***II Procédure de codécision (deuxième lecture)
majorité des suffrages exprimés pour approuver la position commune
majorité des membres qui composent le Parlement pour rejeter ou amender la position commune
- ***III Procédure de codécision (troisième lecture)
majorité des suffrages exprimés pour approuver le projet commun

(La procédure indiquée est fondée sur la base juridique proposée par la Commission.)

Amendements à un texte législatif

Dans les amendements du Parlement, le marquage est indiqué en ***gras et italique***. Le marquage en *italique maigre* est une indication à l'intention des services techniques qui concerne des éléments du texte législatif pour lesquels une correction est proposée en vue de l'élaboration du texte final (par exemple éléments manifestement erronés ou manquants dans une version linguistique). Ces suggestions de correction sont subordonnées à l'accord des services techniques concernés.

SOMMAIRE

| | Page |
|---|-------------|
| PROJET DE RÉSOLUTION LÉGISLATIVE DU PARLEMENT EUROPÉEN..... | 5 |
| EXPOSÉ DES MOTIFS..... | 30 |
| OPINION MINORITAIRE..... | 36 |
| AVIS DE LA COMMISSION DE L'INDUSTRIE, DE LA RECHERCHE ET DE L'ENERGIE..... | 37 |
| AVIS DE LA COMMISSION DU MARCHÉ INTERIEUR ET DE LA PROTECTION DES CONSOMMATEURS..... | 56 |
| PROCÉDURE | 67 |

PROJET DE RÉSOLUTION LÉGISLATIVE DU PARLEMENT EUROPÉEN

sur la proposition de directive du Parlement européen et du Conseil sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, et modifiant la directive 2002/58/CE (COM(2005)0438 – C6-0293/2005 – 2005/0182(COD))

(Procédure de codécision: première lecture)

Le Parlement européen,

- vu la proposition de la Commission au Parlement européen et au Conseil (COM(2005)0438)¹,
 - vu l'article 251, paragraphe 2, et l'article 95 du traité CE, conformément auxquels la proposition lui a été présentée par la Commission (C6-0293/2005),
 - vu l'article 51 de son règlement,
 - vu le rapport de la commission des libertés civiles, de la justice et des affaires intérieures, l'avis de la commission de l'industrie, de la recherche et de l'énergie et l'avis de la commission du marché intérieur et de la protection des consommateurs (A6-0365/2005),
1. approuve la proposition de la Commission telle qu'amendée;
 2. invite la Commission à commander, avant l'entrée en vigueur de la présente directive, une étude d'impact réalisée par un organisme indépendant représentant tous les acteurs concernés, couvrant toutes les questions relatives au marché intérieur et à la protection des consommateurs;
 3. demande à la Commission de le saisir à nouveau, si elle entend modifier de manière substantielle cette proposition ou la remplacer par un autre texte;
 4. charge son Président de transmettre la position du Parlement au Conseil et à la Commission.

Texte proposé par la Commission

Amendements du Parlement

Amendement 1 CONSIDÉRANT 3

(3) Les articles 5, 6 et 9 de la directive 2002/58/CE définissent les règles applicables au traitement, par les

(3) Les articles 6 et 9 de la directive 2002/58/CE définissent les règles applicables au traitement, par les

¹ JO C ... du ..., p.

fournisseurs de réseaux et de services, de données relatives au trafic et de données de localisation générées par l'utilisation de services de communications électroniques. **Ces données doivent** être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication, **sauf les données requises** pour établir les factures et les paiements pour interconnexion; **moyennant l'accord de l'intéressé, certaines données peuvent également être traitées afin de commercialiser des services de communications électroniques ou de fournir des services à valeur ajoutée.**

fournisseurs de réseaux et de services, de données relatives au trafic et de données de localisation générées par l'utilisation de services de communications électroniques. **En principe, ces données devraient** être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication: pour établir les factures **destinées aux abonnés et pour** les paiements pour interconnexion, **ces données peuvent être traitées mais uniquement jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou le paiement effectué.**

Amendement 2 CONSIDÉRANT 4

(4) L'article 15, paragraphe 1, de la directive 2002/58/CE énumère les conditions dans lesquelles les États membres peuvent limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3, et 4, et à l'article 9 de la directive; toute dérogation de ce type doit constituer une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour des raisons spécifiques d'ordre public, à savoir pour sauvegarder la sécurité nationale (c'est-à-dire la sûreté de l'État), la défense et la sécurité publique, ou assurer **la prévention**, la recherche, la détection et la poursuite d'infractions pénales **ou d'utilisations non autorisées de systèmes de communications électroniques.**

(4) L'article 15, paragraphe 1, de la directive 2002/58/CE énumère les conditions dans lesquelles les États membres peuvent limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3, et 4, et à l'article 9 de la directive; toute dérogation de ce type doit constituer une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour des raisons spécifiques d'ordre public, à savoir pour sauvegarder la sécurité nationale (c'est-à-dire la sûreté de l'État), la défense et la sécurité publique, ou assurer la recherche, la détection et la poursuite d'infractions pénales **graves.**

(Le présent amendement s'applique dans l'ensemble du texte. Son adoption nécessitera des changements correspondants du début à la fin du texte).

Amendement 3

CONSIDÉRANT 4 BIS (nouveau)

(4 bis) La Charte des droits fondamentaux reconnaît explicitement le droit au respect de la vie privée en son article 7 et le droit à la protection des données à caractère personnel en son article 8.

Amendement 4
CONSIDÉRANT 6

(6) Les disparités législatives et techniques *existant entre les dispositions nationales relatives à la conservation de données en vue de la prévention, de la recherche, de la détection et de la poursuite d'infractions pénales constituent des entraves au marché intérieur des communications électroniques; les fournisseurs de services doivent satisfaire à des exigences différentes* pour ce qui est des types de données relatives au trafic à conserver ainsi que des conditions et durées de conservation.

(6) Les *dispositions adoptées pour l'instant présentent* des disparités législatives et techniques *de même que* les exigences pour ce qui est des types de données relatives au trafic à conserver ainsi que des conditions et durées de conservation.

Amendement 5
CONSIDÉRANT 6 BIS (nouveau)

(6 bis) L'harmonisation du marché intérieur dans le domaine de la conservation des données montre combien il est nécessaire que les citoyens disposent d'un accès meilleur et plus équitable à la justice et aux procédures d'appel dans l'ensemble de l'Union européenne. Tous les citoyens devraient bénéficier d'un même droit à la protection juridique et à l'indemnisation contre une utilisation abusive des informations, qu'elle soit du fait d'une autorité ou d'un fournisseur.

Amendement 6
CONSIDÉRANT 7

(7) Dans ses conclusions, le Conseil «Justice et affaires intérieures» du 20 septembre 2001 appelle de ses vœux des propositions permettant de faire en sorte que les autorités répressives aient la possibilité d'enquêter sur des actes criminels comportant l'utilisation de systèmes de communications électroniques et de prendre des mesures contre leurs auteurs, tout en assurant un équilibre entre la protection des données à caractère personnel et les besoins des autorités répressives en matière d'accès à des données à des fins d'enquête criminelle.

supprimé

Amendement 7
CONSIDÉRANT 8

(8) Dans ses conclusions, le Conseil «Justice et affaires intérieures» du 19 décembre 2002 souligne qu'en raison de l'accroissement important des possibilités qu'offrent les communications électroniques, les données relatives à l'utilisation de celles-ci *sont particulièrement importantes et constituent donc* un instrument utile pour la prévention, la recherche, la détention et la poursuite de délits et d'infractions pénales, notamment de la criminalité organisée.

(8) Dans ses conclusions, le Conseil «Justice et affaires intérieures» du 19 décembre 2002 souligne qu'en raison de l'accroissement important des possibilités qu'offrent les communications électroniques, les données relatives à l'utilisation de celles-ci *peuvent constituer* un instrument utile pour la prévention, la recherche, la détention et la poursuite de délits et d'infractions pénales, notamment de la criminalité organisée.

Amendement 8
CONSIDÉRANT 10

(10) La déclaration adoptée par le Conseil spécial informel du 13 juillet 2005 réaffirme la nécessité d'adopter dans les meilleurs délais des mesures en matière de conservation de données relatives au trafic des communications électroniques.

(10) La déclaration adoptée par le Conseil spécial informel du 13 juillet 2005 réaffirme la nécessité d'adopter dans les meilleurs délais des mesures *communes* en matière de conservation de données relatives au trafic des communications électroniques.

Amendement 9
CONSIDÉRANT 10 BIS (nouveau)

(10 bis) Le groupe de protection des personnes à l'égard du traitement des données à caractère personnel, établi conformément à l'article 29 de la directive 95/46/CE, assume les tâches visées à l'article 30 de la directive susmentionnée en tenant compte également de la protection des droits et libertés fondamentaux et des intérêts légitimes dans le domaine relevant de la présente directive.

Amendement 10
CONSIDÉRANT 11

*(11) Eu égard à l'importance des données relatives au trafic pour la prévention, la recherche, la détection et la poursuite d'infractions graves, telles que les actes terroristes et la criminalité organisée, il est nécessaire, comme les travaux de recherche et l'expérience pratique de plusieurs États membres le démontrent, de garantir la conservation pendant un **certain** délai des données traitées par les fournisseurs de communications électroniques dans le cadre de la fourniture de services de communications électroniques accessibles au public ou d'un réseau public de communications.*

*(11) L'expérience pratique de certains États membres a démontré que des données relatives au trafic peuvent être **importantes pour** la recherche, la détection et la poursuite d'infractions graves, telles que les actes terroristes et la criminalité organisée. **Par conséquent**, il est nécessaire, comme les travaux de recherche et l'expérience pratique de plusieurs États membres le démontrent, de garantir la conservation pendant un délai **harmonisé** des données traitées par les fournisseurs **publics** de communications électroniques dans le cadre de la fourniture de services de communications électroniques accessibles au public ou d'un réseau public de communications.*

Amendement 11
CONSIDÉRANT 11 BIS (nouveau)

(11 bis) L'élaboration de toute liste des catégories d'information à conserver devrait refléter un équilibre entre, d'une part, les avantages pour la prévention, la recherche, la détection et la poursuite des infractions en cause et, d'autre part, le

niveau d'ingérence dans la vie privée qui en résultera.

Amendement 12
CONSIDÉRANT 14

(14) Les technologies liées aux communications électroniques progressent rapidement et les exigences légitimes des autorités compétentes peuvent évoluer; afin d'obtenir des avis à ce sujet, la Commission prévoit **de créer une** plateforme composée de représentants des services répressifs, des associations du secteur des communications électroniques et des autorités chargées de la protection des données.

(14) Les technologies liées aux communications électroniques progressent rapidement et les exigences légitimes des autorités compétentes peuvent évoluer; afin d'obtenir des avis à ce sujet, la Commission prévoit **une révision périodique de la stricte nécessité de ces dispositions et l'évaluation des types de données qui sont nécessaires. Une** plateforme composée de représentants **du Parlement européen**, des services répressifs, des associations du secteur des communications électroniques et des autorités **européennes et nationales** chargées de la protection des données **pourrait prêter assistance à la Commission.**

Amendement 13
CONSIDÉRANT 17

(17) Il y a lieu d'arrêter les mesures nécessaires pour la mise en œuvre de la présente directive en conformité avec la décision 1999/468/CE du Conseil du 28 juin 1999 fixant les modalités de l'exercice des compétences d'exécution conférées à la Commission.

supprimé

Amendement 14
CONSIDÉRANT 18

(18) Les objectifs de l'action envisagée, à savoir l'harmonisation des obligations incombant aux fournisseurs de conserver certaines données et de faire en sorte que ces données soient disponibles aux fins **de**

(18) Les objectifs de l'action envisagée, à savoir l'harmonisation des obligations incombant aux fournisseurs de conserver certaines données et de faire en sorte que ces données soient disponibles aux fins de

la prévention, de la recherche, de la détection et de la poursuite d'infractions graves, comme les actes terroristes et la criminalité organisée, ne peuvent pas être réalisés de manière suffisante par les États membres et peuvent donc, en raison des dimensions ou des effets de l'action envisagée, être mieux réalisés au niveau communautaire. Par conséquent, la Communauté peut adopter des mesures, en application du principe de subsidiarité énoncé à l'article 5 du traité. Conformément au principe de proportionnalité tel qu'énoncé audit article, la présente directive n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

la recherche, de la détection et de la poursuite d'infractions graves, comme les actes terroristes et la criminalité organisée, ne peuvent pas être réalisés de manière suffisante par les États membres et peuvent donc, en raison des dimensions ou des effets de l'action envisagée, être mieux réalisés au niveau communautaire. Par conséquent, la Communauté peut adopter des mesures, en application du principe de subsidiarité énoncé à l'article 5 du traité. Conformément au principe de proportionnalité tel qu'énoncé audit article, **il n'apparaît pas clairement que** la présente directive n'excède pas ce qui est nécessaire **et proportionné** pour atteindre ces objectifs, **comme l'a fait remarquer également le Contrôleur européen de la protection des données**.

Amendement 15

CONSIDÉRANT 18 BIS (nouveau)

(18 bis) Étant donné que la sécurité des données conservées en vertu de la présente directive présente une extrême importance pour la sauvegarde des droits des consommateurs, les États membres devraient veiller à ce que les normes les plus élevées de sécurité en matière de stockage des données soient appliquées, en particulier la protection des données contre toute altération et accès non autorisé ainsi que contre les menaces liées ou non à Internet.

Amendement 16

CONSIDÉRANT 18 TER (nouveau)

(18 ter) La protection des données dans le cadre de la présente directive est conforme aux dispositions relatives à la protection des données de la directive 2002/58/CE.

Amendement 17
CONSIDÉRANT 19

(19) La présente directive **respecte** les droits fondamentaux et **observe** les principes reconnus, notamment, par la Charte des droits fondamentaux de l'Union européenne; la présente directive ainsi que la directive 2002/58/CE visent notamment à veiller à ce que les droits fondamentaux liés au respect de la vie privée et des communications des citoyens et à la protection des données à caractère personnel (articles 7 et 8 de la Charte) soient pleinement respectés,

(19) La présente directive **pourrait davantage respecter** les droits fondamentaux et les principes reconnus, notamment, par la Charte des droits fondamentaux de l'Union européenne; la présente directive ainsi que la directive 2002/58/CE visent notamment à veiller à ce que les droits fondamentaux liés au respect de la vie privée et des communications des citoyens et à la protection des données à caractère personnel (articles 7 et 8 de la Charte) **ainsi que les arrêts de la Cour européenne des droits de l'homme¹** soient pleinement respectés.

¹ Voir en particulier les arrêts dans les affaires *Amann/Suisse* (n° 27798/95, CEDH 2000-II du 16 février 2000, dans laquelle la conservation d'informations sur une personne a été considérée comme une interférence avec sa vie privée bien que ces informations n'aient contenu aucune donnée sensible) et *Malone/Royaume-Uni* (n° 8691/79, du 2 août 1984, où les mêmes conclusions ont été appliquées à la pratique du "comptage" des communications téléphoniques, impliquant l'utilisation d'un appareil qui enregistre automatiquement les numéros formés sur un téléphone, ainsi que l'heure et la durée de chaque appel).

Amendement 18
CONSIDÉRANT 19 BIS (nouveau)

(19 bis) Les États membres veillent à ce que les opérateurs économiques soient dûment consultés avant la mise en application de la présente directive, en ce qui concerne en particulier la faisabilité et les coûts de la conservation des données. Étant donné que la conservation des données représente une charge matérielle et financière pour les opérateurs économiques, les États membres garantissent la compensation intégrale des

coûts supplémentaires à la charge des opérateurs économiques du fait d'obligations liées à la transposition de la présente directive ou d'obligations librement consenties.

Justification

La lutte contre la criminalité et la garantie de la sécurité publique sont des missions fondamentales de l'État moderne. Dès lors, les mesures adoptées en la matière doivent être financées intégralement par les pouvoirs publics et ne pas être à la charge des opérateurs économiques, faute de quoi l'Europe sera moins attrayante pour les entreprises. Il en résulte que l'intégralité des coûts (coûts d'investissement et d'exploitation) occasionnés par toutes les obligations découlant de la directive doit être supportée par les États membres. Cela vaut également pour l'élaboration de statistiques, qui doit incomber principalement aux États membres.

Amendement 19
ARTICLE 1, PARAGRAPHE 1

1. La présente directive a pour objectif d'harmoniser les dispositions des États membres relatives aux obligations des fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications en matière de traitement et de conservation de certaines données, en vue de garantir la disponibilité de ces données à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales graves, ***comme les actes terroristes et la criminalité organisée.***

1. La présente directive a pour objectif d'harmoniser les dispositions des États membres relatives aux obligations des fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications en matière de traitement et de conservation de certaines données ***et, à l'effet d'assurer que soient pleinement respectés les droits au respect de la vie privée et à la protection des données à caractère personnel dans le contexte de l'accès à ces données et de leur utilisation,*** en vue de garantir la disponibilité de ces données à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales graves ***au sens de l'article 2, paragraphe 2, de la décision-cadre du Conseil 2002/584/JHA.***

Amendement 20
ARTICLE 1, PARAGRAPHE 2

2. La présente directive s'applique aux données relatives au trafic et aux données

2. La présente directive s'applique aux données relatives au trafic et aux données

de localisation concernant les personnes tant physiques que morales, ainsi qu'aux données **connexes** nécessaires pour identifier l'abonné ou l'utilisateur enregistré. Elle ne s'applique pas au contenu des communications électroniques, notamment aux informations consultées en utilisant un réseau de communications électroniques.

de localisation concernant les personnes tant physiques que morales, ainsi qu'aux données nécessaires pour identifier l'abonné ou l'utilisateur enregistré. Elle ne s'applique pas au contenu des communications électroniques, notamment aux informations consultées en utilisant un réseau de communications électroniques.

(Le présent amendement s'applique dans l'ensemble du texte. Son adoption nécessitera des changements correspondants du début à la fin du texte).

Amendement 21

ARTICLE 2, PARAGRAPHE 2, POINT a) ET POINT a bis) (nouveau)

a) "données" les données relatives au trafic et les données de localisation, ainsi que les données **connexes** nécessaires pour identifier l'abonné ou l'utilisateur.

a) "données" les données relatives au trafic et les données de localisation, ainsi que les données nécessaires pour identifier l'abonné ou l'utilisateur.

a bis) "autorités nationales compétentes" les autorités judiciaires et les autorités nationales compétentes pour la recherche, la détection et la poursuite d'infractions pénales graves.

Amendement 22

ARTICLE 2, PARAGRAPHE 2, POINT b bis) (nouveau)

b bis) "infractions graves" infractions au sens de l'article 2, paragraphe 2, de la décision-cadre du Conseil 2002/584/JHA¹.

¹ *Décision-cadre du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres.*

Amendement 23

ARTICLE 2, PARAGRAPHE 2, POINT b ter) (nouveau)

b ter) "tentative de communication infructueuse" communication dans laquelle l'appel téléphonique a été établi mais n'a pas donné lieu à une réponse ou lorsqu'il y a eu intervention sur le réseau.

Amendement 24
ARTICLE 3, PARAGRAPHE 1

1. Par dérogation aux articles 5, 6 et 9 de la directive 2002/58/CE, les États membres prennent les mesures nécessaires pour **assurer la conservation**, conformément aux dispositions de la présente directive, de données générées **ou** traitées dans le cadre de la fourniture de services de communication **par des fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications, lorsque ces fournisseurs relèvent de leur juridiction.**

1. Par dérogation aux articles 5, 6 et 9 de la directive 2002/58/CE, les États membres prennent les mesures nécessaires pour **que les fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications qui offrent ce service, assurent la conservation et tiennent disponibles les données** générées **et** traitées dans le cadre de la fourniture de services de communication, **dans le cas d'une communication établie avec succès**, conformément aux dispositions de la présente directive, **par le fournisseur qui a offert le service de communication électronique utilisé.**

Amendement 25
ARTICLE 3, PARAGRAPHE 2

2. Les États membres prennent les mesures nécessaires pour veiller à ce que les données conservées conformément à la présente directive ne soient transmises qu'aux autorités nationales compétentes, dans des cas précis conformément **à la législation nationale**, et à des fins **de prévention**, de recherche, de détection et de poursuite des infractions pénales graves, **comme les actes terroristes et la criminalité organisée.**

2. Les États membres prennent les mesures nécessaires pour veiller à ce que les données conservées conformément à la présente directive ne soient transmises qu'aux autorités nationales compétentes, **après approbation des autorités judiciaires et des autres autorités compétentes conformément à la législation nationale**, dans des cas précis conformément **aux dispositions de la présente directive**, et à des fins de recherche, de détection et de poursuite des infractions pénales graves **au sens de l'article 2, paragraphe 2, de la décision-cadre du Conseil 2002/584/JHA.**

La présente directive est conforme aux principes établis dans la décision cadre du Conseil sur [la protection des données].

Amendement 26
ARTICLE 3, PARAGRAPHE 2 BIS (nouveau)

2 bis. À cette fin, il convient de rendre publique une liste mise à jour des autorités répressives compétentes désignées.

Amendement 27
ARTICLE 3 BIS (nouveau)

Article 3 bis

Accès aux données conservées

1. Chaque État membre veille à ce que l'accès aux données conservées en vertu de la présente directive soit réservé exclusivement aux fournisseurs de services de communications électroniques accessibles au public ou d'un réseau de communications et soumis aux conditions minimales suivantes, et établit des voies de recours conformément aux dispositions du chapitre III de la directive 95/46/CE:

a) les autorités nationales compétentes, dûment autorisées par une autorité judiciaire ou par une autre autorité nationale indépendante compétente, n'ont accès aux données que pour les finalités déterminées, explicites et légitimes définies par la présente directive, au cas par cas et dans le respect du secret professionnel, conformément au droit national;

b) les données ne font l'objet d'aucun traitement ultérieur qui soit incompatible avec ces finalités; tout traitement ultérieur de données par des services nationaux compétents aux fins d'autres procédures connexes doit être limité par le biais de

garanties rigoureuses;

c) tout accès aux données par d'autres entités publiques ou des organismes privés est interdit;

d) chaque État membre définit dans son droit national la procédure à suivre pour avoir accès aux données conservées et pour préserver les données ayant fait l'objet d'un accès; les fournisseurs ne sont pas autorisés à traiter des données conservées en vertu de la présente directive à leurs propres fins;

e) les données demandées sont nécessaires, pertinentes et non excessives au regard des finalités poursuivies; les données sont traitées loyalement et licitement: en tout état de cause, l'accès est limité aux données qui sont nécessaires dans le contexte d'une enquête spécifique et n'inclut pas l'extraction à grande échelle de données concernant les profils de déplacements et de communications de personnes non soupçonnées par les services nationaux compétents;

f) tout accès aux données conservées est enregistré dans un registre des traitements qui permet d'identifier le demandeur, les personnes chargées du contrôle des données, le personnel autorisé à l'accès et au traitement des données, l'autorisation judiciaire concernée, les données consultées et la finalité pour laquelle elles sont consultées;

g) les données sont conservées sous une forme permettant l'identification des matières concernées pendant une durée n'excédant pas celle nécessaire à la réalisation de la finalité pour laquelle les données ont été collectées ou traitées ultérieurement;

h) la confidentialité et l'intégrité des données sont garanties, en ce compris le respect du secret professionnel; toute consultation des données est enregistrée et

les enregistrements sont mis à la disposition des autorités nationales chargées de la protection des données;

i) les données auxquelles l'accès est accordé sont exactes et toute mesure nécessaire est prise 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;

j) les données sont effacées dès qu'elles ne sont plus nécessaires pour les finalités pour lesquelles elles ont été recueillies;

k) les autorités nationales ne peuvent transmettre ces données à des pays tiers que par le biais d'un accord international conclu sur la base de l'article 300 du traité et seulement si l'approbation de cet accord par le Parlement européen a été obtenue (article 300, paragraphe 3, alinéa 2, du traité).

Amendement 28
ARTICLE 3 TER (nouveau)

Article 3 ter

Protection des données et sécurité des données

Chaque État membre veille à ce que les données conservées conformément à la présente directive soient soumises au minimum aux dispositions d'exécution de l'article 17 de la directive 95/46/CE 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, aux dispositions des articles 4 et 5 de la directive 2002/58/CE et aux principes de sécurité des données suivants:

a) les données sont soumises à des mesures techniques et organisationnelles appropriées afin de protéger celles-ci

contre une destruction ou une perte accidentelle ou illégale, une altération, une divulgation ou un accès illicite ou illégal et contre tout autre forme illégale de traitement;

b) les données sont soumises à des mesures techniques et organisationnelles appropriées afin de garantir que la divulgation des données et l'accès aux données ne sont effectués que par des personnes autorisées dont le comportement fait l'objet d'un contrôle d'une autorité judiciaire ou administrative compétente;

c) les fournisseurs de services ou de réseaux de communications électroniques accessibles au public ainsi que les autorités des États membres ayant accès aux données enregistrent tous les accès et prennent les mesures de sécurité appropriées afin de prévenir la conservation, l'accès, le traitement, la divulgation ou l'utilisation non autorisés, inappropriés ou illégaux des données, y compris au moyen de systèmes techniques pleinement actualisés permettant de protéger l'intégrité des données et au travers de la désignation du personnel spécialement autorisé qui peut avoir accès exclusif aux données;

d) les fournisseurs de services ou de réseaux de communications électroniques accessibles au public créent un système séparé de conservation des données à des fins d'ordre public; les données de ce système distinct ne peuvent en aucune manière être utilisées à des fins commerciales ou à d'autres fins non explicitement autorisées conformément à la présente directive;

e) les autorités nationales ne peuvent transmettre ces données à des pays tiers que par le biais d'un accord international conclu sur la base de l'article 300 du traité et seulement si l'approbation de cet accord par le Parlement européen a été

obtenue (article 300, paragraphe 3, alinéa 2, du traité).

f) toutes les données sont détruites à la fin de la période de conservation, à l'exception des données qui ont été accessibles et préservées;

g) dans chaque État membre, l'autorité de protection des données ou une autorité indépendante compétente telle que prévue par le droit national est désignée pour surveiller l'application régulière de la présente directive.

Amendement 29

ARTICLE 4

Catégories de données à conserver

Les États membres veillent à ce que soient conservées en application de la présente directive les catégories de données suivantes:

- (a) les données nécessaires pour retrouver et identifier la source d'une communication;
- (b) les données nécessaires pour retrouver et identifier la destination d'une communication;
- (c) les données nécessaires pour déterminer la date, l'heure et la durée d'une communication;
- (d) les données nécessaires pour déterminer le type de communication;
- (e) les données nécessaires pour déterminer le dispositif de communication utilisé ou ce qui est censé avoir été utilisé comme dispositif de communication;
- (f) les données nécessaires pour localiser le matériel de communication mobile.

Les types de données à conserver pour chacune des catégories de données susmentionnées sont précisés en annexe.

Catégories *et types* de données à conserver

I. Les États membres veillent à ce que soient conservées en application de la présente directive les catégories de données suivantes:

- (a) les données nécessaires pour retrouver et identifier la source d'une communication;
- (b) les données nécessaires pour retrouver et identifier la destination d'une communication;
- (c) les données nécessaires pour déterminer la date, l'heure et la durée d'une communication;
- (d) les données nécessaires pour déterminer le type de communication;
- (e) les données nécessaires pour déterminer le dispositif de communication utilisé ou ce qui est censé avoir été utilisé comme dispositif de communication;
- (f) les données nécessaires pour localiser le matériel de communication mobile.

Aucune donnée révélant le contenu de la communication ne peut être conservée.

Amendement 30
ARTICLE 4, ALINÉA 1 BIS (nouveau)

1 bis. Types de données à conserver:

1) En ce qui concerne la téléphonie fixe en réseau:

a) Données nécessaires pour retrouver et identifier la source d'une communication:

(i) le numéro de téléphone de l'appelant,

(ii) les nom et adresse de l'abonné ou de l'utilisateur enregistré.

b) Données nécessaires pour retrouver et identifier la destination d'une communication:

(i) le ou les numéros de téléphone appelés,

(ii) les nom et adresse de l'abonné ou de l'utilisateur enregistré.

c) Données nécessaires pour déterminer la date, l'heure et la durée d'une communication:

(i) la date et l'heure de début et de fin de la communication.

d) Données nécessaires pour déterminer le type de communication:

(i) le service téléphonique utilisé, par exemple, voix, conférence téléphonique, télécopie et services de messagerie.

2) En ce qui concerne la téléphonie mobile:

a) Données nécessaires pour retrouver et identifier la source d'une communication:

(i) le numéro de téléphone de l'appelant,

(ii) les nom et adresse de l'abonné ou de l'utilisateur enregistré.

b) Données nécessaires pour retrouver et identifier la destination d'une communication:

(i) le ou les numéros de téléphone appelés,

(ii) les nom et adresse de l'abonné ou de l'utilisateur enregistré.

c) Données nécessaires pour déterminer la date, l'heure et la durée d'une communication:

(i) la date et l'heure de début et de fin de la communication.

d) Données nécessaires pour déterminer le type de communication:

(i) le service téléphonique utilisé, par exemple, voix, conférence téléphonique, service de mini messages (SMS), service de messagerie amélioré (EMS) ou service de messagerie multimédia (MMS).

e) Données nécessaires pour déterminer le dispositif de communication utilisé ou ce qui est censé avoir été utilisé comme dispositif de communication:

(i) l'identité internationale d'abonné mobile (IMSI) de l'appelant et de l'appelé,

(ii) en cas de cartes/services anonymes prépayés, la date et le moment de l'activation initiale de la carte et du label (Cell ID) à partir duquel l'activation a été faite.

f) Données nécessaires pour localiser le matériel de communication mobile:

(i) l'identité de localisation (identifiant cellulaire) au début de la communication.

3) En ce qui concerne Internet et ses services:

a) Données nécessaires pour retrouver et identifier la source d'une communication:

(i) l'adresse du protocole Internet (adresse IP), qu'elle soit dynamique ou statique, attribuée à une communication par le fournisseur d'accès internet,

(ii) l'identité de connexion ou numéro de téléphone attribué à toute communication entrant dans le réseau téléphonique public,

(iii) les nom et adresse de l'abonné ou de l'utilisateur enregistré à qui l'adresse IP,

l'identité de connexion ou le code d'identification personnel ont été attribués au moment de la communication.

b) Données nécessaires pour déterminer la date, l'heure et la durée d'une communication:

(i) la date et l'heure d'ouverture et de fermeture des sessions Internet dans un fuseau horaire déterminé.

c) Données nécessaires pour déterminer le dispositif de communication utilisé ou ce qui est censé avoir été utilisé comme dispositif de communication:

(i) le numéro de téléphone de l'appelant pour l'accès commuté,

(ii) la ligne d'abonné numérique (DSL) ou tout autre identifiant terminal de l'auteur de la communication.

Amendement 31
ARTICLE 4, ALINÉA 2

Les types de données à conserver pour chacune des catégories de données susmentionnées sont précisés en annexe.

Il est loisible aux États membres de demander aux fournisseurs de services de communications accessibles au public ou d'un réseau de communications de conserver les données relatives aux tentatives d'appel infructueuses effectuées pour obtenir une communication relevant de ces catégories de données, en vertu de la législation nationale.

Sont exclues les données révélant le contenu d'une communication.

Amendement 32
ARTICLE 5

Révision de l'annexe

supprimé

L'annexe fait l'objet d'une révision régulière s'il y a lieu, selon la procédure prévue à l'article 6, paragraphe 2.

Amendement 33
ARTICLE 6

Comité

supprimé

1. La Commission est assistée par un comité composé de représentants des États membres et présidé par le représentant de la Commission.

2. Dans le cas où il est fait référence au présent paragraphe, les articles 5 et 7 de la décision 199/468/CE s'appliquent, dans le respect des dispositions de l'article 8 de celle-ci.

3. Le délai prévu à l'article 5, paragraphe 6, de la décision 1999/468/CE est fixé à trois mois.

Amendement 34
ARTICLE 7

*Les États membres veillent à ce que les catégories de données visées à l'article 4 soient conservées pour une durée **d'un an** à compter de la date de la communication, à l'exception des données relatives à des communications électroniques utilisant uniquement ou principalement le protocole Internet. Ces dernières données sont conservées pour une durée de six mois.*

*Les États membres veillent à ce que les catégories de données visées à l'article 4 soient conservées pour une durée **de 6 à 12 mois** à compter de la date de la communication; **ensuite, les données doivent être effacées.***

Les services répressifs compétents veillent à ce que les données transférées soient effacées par des moyens automatiques une fois achevée la recherche pour laquelle l'accès aux données a été octroyé.

Amendement 35
ARTICLE 7, ALINÉA 1 BIS (nouveau)

La Commission maintient le Parlement européen dûment informé des

notifications apportées par les États membres conformément à l'article 95, paragraphe 4, du traité.

Amendement 36
ARTICLE 8

Les États membres veillent à ce que les données soient conservées conformément à la présente directive de manière à ce que **les données conservées et toute autre information nécessaire concernant** ces données puissent, à leur demande, être transmises sans délai aux autorités compétentes.

Les États membres veillent à ce que les données **visées à l'article 4** soient conservées **par les fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications** conformément à la présente directive de manière à ce que ces données puissent, à leur demande, être transmises sans délai aux autorités **nationales** compétentes **de l'État membre concerné**.

Les données sont traitées conformément aux dispositions de l'article 17 de la directive 95/46/CE et de l'article 4 de la directive 2002/58/CE.

Amendement 37
ARTICLE 8, ALINÉA 1 BIS (nouveau)

Les États membres veillent à ce que les fournisseurs de services de communications électroniques accessibles au public ou de réseaux de communication publics concernés implantés sur leur territoire mettent en place un point de contact chargé de traiter les demandes d'accès aux données.

Amendement 38
ARTICLE 8 BIS (nouveau)

Article 8 bis

Sanctions

1. Les États membres imposent des sanctions pour infractions aux

dispositions nationales adoptées en vue de la mise en œuvre de la présente directive. Les sanctions sont effectives, proportionnées et dissuasives (elles comprennent des sanctions pénales et administratives).

2. Les États membres veillent à ce que les personnes visées par une procédure ayant pour objet l'imposition de sanctions bénéficient effectivement du droit à la défense et du droit de recours.

Amendement 39
ARTICLE 9

Les États membres font en sorte que des statistiques sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques **accessibles au public** soient transmises annuellement à la Commission européenne. Ces statistiques concernent notamment:

- les cas dans lesquels des informations ont été transmises aux autorités compétentes conformément à la législation nationale applicable,
- le laps de temps écoulé entre la date à partir de laquelle les données ont été conservées et la date à laquelle les autorités compétentes ont demandé leur transmission,
- *les cas dans lesquels des demandes de données n'ont pu être satisfaites.*

Les États membres font en sorte que des statistiques sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques soient transmises annuellement à la Commission européenne. **L'ENISA (Agence européenne chargée de la sécurité des réseaux et de l'information) peut aider les États membres à réunir ces statistiques.** Ces statistiques, **établies par les autorités nationales compétentes**, concernent notamment:

- les cas dans lesquels des informations ont été transmises aux autorités compétentes conformément à la législation nationale applicable,
- le laps de temps écoulé entre la date à partir de laquelle les données ont été conservées et la date à laquelle les autorités compétentes ont demandé leur transmission,
- **le nombre de cas dans lesquels les données demandées n'ont pas abouti directement au succès de l'enquête;**
- **le nombre de cas dans lesquels des données ont été demandées, qui n'étaient pas à la disposition des organismes concernés;**
- **les cas dans lesquels des infractions aux règles de sécurité ont été soupçonnées ou se**

sont effectivement produites;

La Commission porte ces statistiques à la connaissance du Parlement européen chaque année et, par la suite, tous les trois ans.

Ces statistiques ne contiennent pas de données à caractère personnel.

Ces statistiques ne contiennent pas de données à caractère personnel.

Amendement 40
ARTICLE 9 BIS (nouveau)

Article 9 bis

1. Chaque État membre veille à ce que le contrôle de l'application sur son territoire des dispositions adoptées au titre de la présente directive en ce qui concerne la sécurité des données conservées soit confié à une ou plusieurs autorité(s) publique(s).

2. Ces autorités exercent en toute indépendance les fonctions visées au paragraphe 1.

Amendement 41
ARTICLE 10

Les États membres veillent à ce que les fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications obtiennent le remboursement des surcoûts qu'ils justifient avoir supportés pour s'acquitter des obligations leur incombant en vertu de la présente directive.

Les États membres veillent à ce que les fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications obtiennent le remboursement des surcoûts *en investissement et en frais de fonctionnement* qu'ils justifient avoir supportés pour s'acquitter des obligations leur incombant en vertu de la présente directive *et de toute future modification de celle-ci, y compris les surcoûts prouvés afférents à la protection des données. Le remboursement inclut les coûts prouvés liés à la transmission des données conservées mises à la disposition des*

autorités nationales compétentes.

Amendement 42

ARTICLE 11

Article 15, paragraphe 1 bis (directive 2002/58/CE)

«1 bis. Le paragraphe 1 n'est pas applicable aux obligations en matière de conservation de données pour la **prévention**, la recherche, la détection et la poursuite d'infractions pénales graves, comme les actes terroristes et la criminalité organisée, résultant de la directive 2005/./CE*. * JO L n° du »

«1 bis. Le paragraphe 1 n'est pas applicable aux obligations en matière de conservation de données pour la recherche, la détection et la poursuite d'infractions pénales graves, comme les actes terroristes et la criminalité organisée, résultant de la **transposition** de la directive 2005/./CE*. * JO L n° du »

Les États membres s'abstiennent d'adopter des mesures législatives dans les secteurs couverts par la présente directive.

Amendement 43

ARTICLE 12, PARAGRAPHE 1

1. Au plus tard **trois ans** après la date visée à l'article 13, paragraphe 1, la Commission présente au Parlement européen et au Conseil une évaluation de **l'application** de la présente directive et de **ses** effets sur les opérateurs économiques et les consommateurs, compte tenu des statistiques transmises à la Commission en vertu de l'article 9 **afin de déterminer s'il y a lieu de modifier les dispositions de la présente directive, notamment la durée de conservation prévue à l'article 7.**

1. Au plus tard **deux ans** après la date visée à l'article 13, paragraphe 1, la Commission présente au Parlement européen et au Conseil une évaluation de **la nécessité et de l'efficacité des dispositions** de la présente directive et de **leurs effets sur les droits fondamentaux des personnes concernées. L'évaluation porte également sur l'impact des mesures** sur les opérateurs économiques et les consommateurs, compte tenu des statistiques transmises à la Commission en vertu de l'article 9. **Les résultats des évaluations sont accessibles au public.**

Les résultats des évaluations sont accessibles au public.

Amendement 44

ARTICLE 12, PARAGRAPHE 2

2. À cette fin, la Commission examine toute observation qui pourrait lui être transmise par les États membres ou le groupe de protection des personnes à l'égard du traitement des données à caractère personnel institué par l'article 29 de la directive 95/46/CE.

2. À cette fin, la Commission examine toute observation qui pourrait lui être transmise par les États membres ou le groupe de protection des personnes ***ou par l'autorité européenne chargée de la protection des données*** à l'égard du traitement des données à caractère personnel institué par l'article 29 de la directive 95/46/CE.

Amendement 45
ARTICLE 14 BIS (nouveau)

Article 14 bis

Révision

Au plus tard deux ans après la date visée à l'article 13, paragraphe 1, la présente directive est révisée conformément à la procédure prévue à l'article 251 du traité CE. En particulier, les types de données conservés et les délais de conservation sont examinés du point de vue de leur intérêt pour la lutte contre le terrorisme et la criminalité organisée, sur la base des statistiques prévues à l'article 9. La révision a lieu tous les trois ans.

Amendement 46
ANNEXE

L'annexe est supprimée.

EXPOSÉ DES MOTIFS

1. Rappel

Lors de la réunion du Conseil "Justice et affaires intérieures" des 29 et 30 avril 2004, la France, le Royaume-Uni, l'Irlande et la Suède ont déposé une proposition commune¹ en vue de l'adoption d'une décision-cadre sur la rétention de données de communication. Cette initiative fait suite à la déclaration sur la lutte contre le terrorisme² que le Conseil européen a adoptée le 25 mars 2004 et dans laquelle le Conseil avait été chargé d'envisager des mesures visant à établir des règles relatives à la conservation, par les fournisseurs de services, des données relatives au trafic des communications.

La proposition a pour objet de faciliter la coopération judiciaire en matière pénale en harmonisant les législations des États membres réglementant la rétention de données traitées et stockées par les fournisseurs de services de communications électroniques accessibles au public aux fins de la prévention, la recherche, la détection, la poursuite de délits et d'infractions pénales, y compris du terrorisme.

Au cours de ses séances plénières de juin et septembre 2005, le Parlement européen a rejeté à l'unanimité la proposition du Conseil concernant l'adoption d'une décision-cadre sur la rétention de données. Pour le Parlement européen, le Conseil avait choisi la mauvaise base juridique. Le Conseil posait en principe sa seule compétence législative conférée par le titre VI du traité sur l'Union européenne et se référerait à l'article 31, paragraphe 1 c), en liaison avec l'article 34, paragraphe 2 b), du traité.

Comme les services juridiques du Conseil et de la Commission, le Parlement estime que l'article 95 CEE est la base juridique appropriée. Conformément à celle-ci, le Parlement est pleinement impliqué dans le processus législatif et de codécision.

Le 21 septembre 2005, la Commission a présenté une proposition de directive concernant la conservation des données en vertu de l'article 95 du traité et ainsi posé les jalons des négociations avec le Conseil. Par la suite, les discussions entre le Conseil et le Parlement se sont intensifiées, bien que le Conseil se réserve la liberté d'imposer sa décision-cadre.

Outre la question formelle des compétences, le Parlement européen avait exprimé de sensibles réserves quant au contenu de la décision-cadre sur la rétention de données. Il a été tenu compte partiellement de ses préoccupations dans la proposition de directive de la Commission.

Le 24 novembre, la commission des libertés civiles, de la justice et des affaires intérieures a défini sa position sur la présente proposition de directive.

¹ Document du Conseil 8958/04 du 28 avril 2004.

² Document du Conseil 7764/04 du 28 mars 2004.

2. Situation de départ selon la proposition de la Commission

a) Sur le fond

La proposition de directive de la Commission sur la rétention de données prévoit la réglementation suivante:

| | |
|---|--|
| <i>Champ d'application</i> | Données relatives au trafic pour la téléphonie fixe et mobile, internet, le courrier électronique et la téléphonie IP – données de localisation et appels infructueux inclus |
| <i>Objectif de la rétention</i> | Prévention, détection, recherche et poursuite d'infractions graves telles que les actes terroristes et la criminalité organisée |
| <i>Autorités pouvant accéder aux données</i> | Autorités compétentes déterminées par les États membres |
| <i>Accès aux données</i> | Non inclus |
| <i>Périodes de rétention</i> | 12 mois pour la téléphonie, 6 mois pour internet |
| <i>Coûts</i> | Remboursement des coûts supplémentaires pouvant être établis comme une conséquence de la directive |
| <i>Flexibilité en vertu de l'article 15, paragraphe 1, de la directive 2002/58/CE</i> | Flexibilité: elle permet l'utilisation de la rétention de données à d'autres fins – mais fixation de données harmonisées pour la lutte contre les infractions graves |
| <i>Dispositions en matière de protection des données</i> | Non nécessaires – la protection des données est couverte par les directives existantes 95/46/CE et 2002/58/CE |
| <i>Sanctions pénales</i> | Non incluses – couvertes par la directive-cadre sur les atteintes aux systèmes d'information et les directives sur la protection des données |
| <i>Procédure de comitologie (mise à jour de la liste de données)</i> | Incluse |
| <i>Clause de révision</i> | Trois ans |
| <i>Données devant être conservées (annexe)</i> | |

b) Sur le plan formel

La proposition de la Commission sur la réglementation de la rétention de données a été communiquée au Parlement le 21 septembre. La directive était sur le point d'être adoptée en commission deux mois auparavant.

La présidence britannique a fait part de son intérêt à voir adopter une réglementation avant la fin de l'année 2005 en tant que compromis de première lecture. La Conférence des présidents a confirmé l'intérêt du Parlement pour l'adoption d'un compromis avant la fin de l'année.

Le Parlement a repris avec zèle ses travaux en vue de définir une position commune et de contribuer ainsi à l'avènement d'un compromis. La dernière occasion de parvenir à un compromis en première lecture est la semaine de session du 12 au 15 décembre. Cette procédure législative extrêmement accélérée a entraîné notamment, compte tenu des délais de traduction, un manque de temps pour délibérer ou des lacunes concernant la traduction. Manque également une évaluation des conséquences techniques ou une étude sur les répercussions sur le marché intérieur.

Dans la perspective des mesures et des projets vers une meilleure réglementation au niveau européen, il faut espérer que la procédure suivie pour les délibérations sur la rétention de données ne deviendra pas la règle.

Afin de permettre l'adoption le 24 novembre d'une proposition au sein de la commission des libertés civiles, de la justice et des affaires intérieures ainsi le règlement des nombreuses questions de fond litigieuses, un groupe de travail "Rétention de données" s'est réuni régulièrement. Au sein de ce groupe de travail, le rapporteur, les rapporteurs fictifs, les rapporteurs des commissions IMCO et ITRE, la présidence et le secrétariat des commissions, les coordinateurs ainsi que les collaborateurs ont élaboré, dans un délai de sept semaines, des amendements de compromis. Parallèlement, se sont déroulées des rencontres régulières avec le Conseil et la Commission afin de discuter de l'avancement du dossier au sein de ces institutions.

3. Votes de la commission des libertés civiles, de la justice et des affaires intérieures

Le 24 novembre 2005, la commission des libertés civiles, de la justice et des affaires intérieures a défini sa position sur la proposition de directive de la Commission à une nette majorité des trois quarts. Avant le vote, les députés du PPE-DE, du PSE et du groupe ALDE ont pu s'entendre sur 21 amendements de compromis, qui doivent remplacer une grande partie des 250 amendements déposés.

| <i>Position de la commission LIBE s'appuyant sur les amendements de compromis (vote en commission, 1^{ère} lecture)</i> | |
|---|--|
| <i>Champ d'application</i> | Données relatives au trafic pour la téléphonie fixe et mobile – données de localisation (au début d'un appel) (amendement de compromis 9): système d'option pour les appels infructueux Respect de la vie privée/protection des données |

| | |
|--|--|
| | personnelles concernant l'accès/utilisation des données (amendement de compromis 1) |
| <i>Objectif de la rétention</i> | Recherche, détection et poursuite de formes spécifiées d'infractions graves (pour définir la liste des infractions, reprendre celle utilisée pour le mandat d'arrêt européen) La " prévention " est exclue étant donné qu'il s'agit d'un concept vague rendant les données conservées plus vulnérables aux abus (amendement de compromis 1) |
| <i>Autorités pouvant avoir accès aux données</i> | Accès des autorités judiciaires et des autres autorités chargées de la recherche, de la détection et de la poursuite d' infractions pénales graves (suivant la liste du mandat d'arrêt européen) Dans tous les cas, les autorités nationales sont soumises à une autorisation judiciaire . (amendements de compromis 2, 4) |
| <i>Accès aux données</i> | Une disposition concernant les conditions d'accès aux données a été introduite par la commission: – uniquement à des fins spécifiques, définies par la directive et au cas par cas; – les raisons doivent être nécessaires/proportionnées; – effacement des données lorsqu'elles ne sont plus nécessaires/lorsqu'elles sont inexactes; – il est interdit aux fournisseurs d'utiliser les données; – tout accès aux données conservées est enregistré; – la confidentialité/l'intégrité des données est garantie; – les données ne peuvent être transmises qu'à des pays tiers par le biais d'un accord international sur la base de l'article 300, paragraphe 3, alinéa 2, du traité; (amendement de compromis 5) |
| <i>Périodes de rétention</i> | 6-12 mois pour tout. Après cette période, toutes les données doivent être effacées (amendement de compromis 12) |
| <i>Coûts</i> | Les États membres garantissent la compensation des coûts supplémentaires à la charge de l'industrie des télécommunications (y compris les coûts d'investissement et d'exploitation, ainsi que les coûts résultant de modifications ultérieures de la directive). * au Conseil, la tendance est d'exclure la compensation des coûts liés à la directive (amendement de compromis 18) |

| | |
|---|--|
| <i>Flexibilité en vertu de l'article 15, paragraphe 1, de la directive 2002/58/CE</i> | Les États membres s'abstiennent d'adopter des mesures législatives dans les secteurs couverts par la directive (amendement 224) |
| <i>Dispositions en matière de protection des données</i> | Données complémentaires en matière de sécurité des données, proposées conformément aux directives existantes (voir une liste détaillée dans l'amendement de compromis) (amendement de compromis 6) |
| <i>Sanctions pénales</i> | Des sanctions effectives, proportionnées et dissuasives pour les infractions aux dispositions nationales adoptées en vue de la mise en œuvre de la directive (amendement de compromis 15) |
| <i>Procédure de comitologie (mise à jour de la liste de données)</i> | Non incluse |
| <i>Clause de révision</i> | Révision 2 ans après l'entrée en vigueur et révision périodique tous les 3 ans (amendement de compromis 21) |
| <i>Données à conserver</i> | La commission préconise par son vote l'insertion de l'annexe dans le corps du texte Inclut les cartes/services anonymes prépayés, la date et le moment de l'activation initiale de la carte et le label (Cell ID) à partir duquel l'activation a été faite – "types" de données à conserver: TÉLÉPHONE FIXE – nom/adresse de l'appelant + numéro de téléphone – nom/adresse de l'abonné + numéro de téléphone – date et moment du début et de la fin de la conversation TÉLÉPHONE MOBILE – nom/adresse de l'appelant + numéro de téléphone – nom/adresse de l'abonné + numéro de téléphone – date et moment du début et de la fin de la conversation – numéro IMSI (international mobile subscriber identity) ou carte d'identité de la SIME – label de localisation au début de la communication INTERNET – adresse IP de l'ordinateur – numéro de téléphone reliant à internet – nom/adresse de l'abonné – date/moment du log-in et du log-off – numéro de téléphone d'appel ADSL en entrée et abonné numérique ADSL (amendement de compromis 8) |

Ces amendements adoptés à la majorité montrent que le Parlement était parfaitement en mesure de parvenir à un accord transcendant les groupes sur des points essentiels concernant la rétention de données. Le Conseil n'a pas encore obtenu un résultat comparable, du moins au moment de la rédaction du présent rapport. Il reste à voir quelle sera l'évolution au sein du Conseil. Le rapporteur estime toutefois qu'il n'y a pas de marge de manœuvre pour des modifications substantielles aux amendements de compromis obtenus.

4. Tendance de l'opinion au sein du Conseil

Le vote de la commission des libertés civiles, de la justice et des affaires intérieures du 24 novembre fait apparaître les divergences suivantes par rapport à l'opinion majoritaire au sein du Conseil.

| | Parlement européen | Tendance des négociations au sein du Conseil |
|----------------------------------|---|---|
| Durée de la période de rétention | 6–12 mois pour tout (téléphonie et internet) | 6 mois pour internet, de 6 à 24 mois pour la téléphonie |
| Champ d'application | Utilise la définition de l'"infraction grave" du mandat d'arrêt européen (catalogue + 3 ans d'emprisonnement) | Toutes les infractions sont incluses |
| Remboursement des coûts | Obligatoire pour tous les coûts supplémentaires que pose la directive + les coûts liés aux exigences de la protection des données | Un régime national à option |
| Appels infructueux | Une option laissant aux États membres la possibilité d'imposer une obligation aux Télécom | Rétention obligatoire des appels infructueux |
| Sanctions pénales | Sanctions pénales pour utilisation abusive des données | Contre |

OPINION MINORITAIRE

**exprimée, conformément à l'article 48, paragraphe 3, du règlement,
par Giusto Catania, Ole Krarup, Sylvia-Yvonne Kaufmann
et Kathalijne Maria Buitenweg**

Nous rejetons ce rapport étant donné qu'il ne corrige suffisamment ni politiquement ni juridiquement la proposition de directive sur la rétention de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public.

L'acte juridique proposé par la Commission, avec les propositions de modification du présent rapport, va à l'encontre du principe de proportionnalité. Il n'est en outre ni nécessaire ni efficace. La durée de conservation des données proposée est beaucoup trop longue et l'éventail des types de données à conserver beaucoup trop large. Quant à la définition des autorités compétentes qui ont accès aux données, elle manque de précision et l'accès des services secrets n'est pas exclu. Les mécanismes de contrôle concernant la sécurité des données sont insuffisamment réglementés.

La proposition de directive porte gravement atteinte aux droits fondamentaux des citoyens, ce que nous ne pouvons approuver. Les citoyens de l'Union ne doivent pas être suspectés. Il reste au Conseil et à la Commission à prouver que les délits graves peuvent être effectivement détectés plus efficacement grâce à la rétention de toute une série de données très diverses en matière de communication.

Si l'on tient compte du fait que l'introduction de cette mesure serait très coûteuse, il est souhaitable d'en affecter le montant à des mesures plus efficaces de lutte contre des infractions graves, comme par exemple des enquêtes ciblées et une meilleure coopération entre les autorités chargées de la répression.

23.11.2005

AVIS DE LA COMMISSION DE L'INDUSTRIE, DE LA RECHERCHE ET DE L'ENERGIE

à l'intention de la commission des libertés civiles, de la justice et des affaires intérieures

sur la proposition de directive du Parlement européen et du Conseil sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, et modifiant la directive 2002/58/CE (COM(2005)0438 – C6-0293/2005 – 2005/0182(COD))

Rapporteuse pour avis: Angelika Niebler

JUSTIFICATION SUCCINCTE

Contexte

Le 21 septembre 2005, la Commission a présenté une proposition de directive sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, et modifiant la directive 2002/58/CE. Ce faisant, la Commission présente sciemment une contreproposition, sur la base de l'article 95 du traité CE, à la décision-cadre du Conseil proposée par la République française, l'Irlande, le Royaume-Uni et la Suède concernant la conservation de données.¹

Il convient de se féliciter de cette évolution, notamment du point de vue du Parlement: la Commission opte pour une base juridique ouvrant le droit à la codécision pour le Parlement dans ce domaine si important pour les citoyens et les entreprises. La décision-cadre, qui repose sur l'article 31, paragraphe 1, c) et l'article 34, paragraphe 2, b) du traité sur l'Union européenne, ne prévoit en revanche qu'un droit d'audition du Parlement.

Du point de vue de leur contenu, la proposition de directive de la Commission et la proposition de décision-cadre ont des objectifs semblables. Les deux actes juridiques doivent permettre d'améliorer la lutte contre le terrorisme et les infractions pénales graves, en obligeant les fournisseurs de réseaux publics de communications à conserver certaines données selon des dispositions harmonisées.

¹ Doc. 8958/04 du 28.4.2004.

Le texte concerne les données relatives au trafic et à la localisation, au sens de l'article 2 de la directive 2002/58/CE, y compris les données relatives aux utilisateurs et aux abonnés. De la sorte, toutes les informations concernant le lieu, l'heure, la durée et les interlocuteurs de conversations téléphoniques, de fax, de courrier électronique, de sms et de protocoles Internet pourront être conservées. Le contenu des conversations en est expressément exclu.

Évaluation

À l'heure actuelle, les États membres de l'Union européenne règlent de manière diverse les délais de conservation des données concernant les communications individuelles. Dans l'optique d'une lutte efficace et transnationale du terrorisme et de la criminalité, cela constitue indubitablement un désavantage, les délinquants opérant de plus en plus souvent au-delà des frontières en utilisant les moyens de communication modernes. C'est pourquoi la directive proposée peut devenir un instrument important de la lutte contre la criminalité.

Cependant, la rapporteure estime qu'il existe plusieurs points importants soulevant la critique, qui devraient être abordés notamment par la commission de l'industrie, de la recherche et de l'énergie afin de tenir dûment compte des aspects particuliers de la société de la communication et de l'information sur lesquels la directive porte.

Comme le Conseil dans la décision-cadre susmentionnée, la Commission ne parvient à prouver que de manière très globale que les mesures proposées permettront d'améliorer réellement la lutte contre la criminalité et le terrorisme. Or, cette preuve est la condition fondamentale permettant de justifier les répercussions et contraintes considérables qui pèseront sur les citoyens et les entreprises. Dans la pratique des poursuites pénales, il s'avère au contraire que les données requises par les autorités ne remontent en règle générale pas à plus de trois mois. C'est pourquoi les délais légaux de conservation doivent être adaptés aux besoins réels.

Pour les entreprises de télécommunications, la proposition signifie qu'elles sont tenues de conserver un volume inimaginable de données. Afin de conserver, d'archiver et de rendre utilisable ce volume, des adaptations coûteuses des systèmes en place sont nécessaires. Des calculs internes menés au niveau des branches escomptent que ces adaptations, selon l'entreprise, s'accompagneront de coûts s'élevant à plusieurs centaines de millions d'euros, sans parler des coûts de suivi pour l'entretien et la réparation des systèmes.

Dans ce contexte, il convient de réduire non seulement la durée de conservation, mais également le nombre des types de données à conserver, tels que figurant en annexe de la proposition. Il s'agit avant tout des tentatives infructueuses de communication, sur lesquelles porte la proposition de la Commission et qui signifiaient des coûts supplémentaires considérables, précisément dans le domaine des réseaux fixes, sans pour autant améliorer la lutte contre la criminalité. Il en va de même pour les données concernant la caractérisation des appareils, l'adresse MAC ou la localisation pendant et à la fin d'une conversation téléphonique par téléphone portable.

La rapporteure s'inquiète en particulier de ce qu'en vertu des articles 5 et 6 de la proposition, l'annexe et, partant, les principales dispositions régissant les types de données à conserver puissent être modifiées par le biais de la procédure de comitologie. Dès lors, le Parlement

serait totalement exclu des décisions à prendre dans ce domaine sensible. Les dispositions portant sur ce point doivent par conséquent être supprimées.

L'obligation pour les États membres, à l'article 9 de la proposition, de présenter des statistiques concernant la conservation de données ne doit pas se solder par un effort bureaucratique supplémentaire pour les entreprises. Néanmoins, ces statistiques pourraient également être utilisées pour établir le nombre de cas dans lesquels les demandes ont effectivement permis de mener à bien une enquête.

En conclusion, il convient d'observer que le Parlement ne doit pas se laisser mettre sous pression dans cette question si sensible pour le citoyen. Même s'il est compréhensible de vouloir achever dans les meilleurs délais la procédure législative, il est capital que la réflexion soit menée avec soin. Il convient par ailleurs, dans l'intérêt de la crédibilité de l'Union européenne, d'éviter une situation dans laquelle deux actes juridiques au contenu similaire sont traités simultanément dans le même but. De l'avis de la rapporteure, le Conseil devrait par conséquent à l'avenir examiner uniquement la directive proposée par la Commission.

AMENDEMENTS

La commission de l'industrie, de la recherche et de l'énergie invite la commission des libertés civiles, de la justice et des affaires intérieures, compétente au fond, à incorporer dans son rapport les amendements suivants:

Texte proposé par la Commission¹

Amendements du Parlement

Amendement 1 CONSIDÉRANT 12

(12) Les catégories d'informations à conserver reflètent un juste équilibre entre, d'une part, les avantages pour la prévention, la recherche, la détection et la poursuite des infractions en cause et, d'autre part, le niveau d'ingérence dans la vie privée qui en résultera; les durées de conservation applicables, à savoir **un an**, ou **six mois** lorsque les données concernent des communications électroniques ayant lieu uniquement grâce au protocole Internet, établissent aussi un équilibre approprié entre tous les intérêts en jeu.

(12) Les catégories d'informations à conserver reflètent un juste équilibre entre, d'une part, les avantages pour la prévention, la recherche, la détection et la poursuite des infractions en cause et, d'autre part, le niveau d'ingérence dans la vie privée qui en résultera; les durées de conservation applicables, à savoir **six mois**, ou **trois mois** lorsque les données concernent des communications électroniques ayant lieu uniquement grâce au protocole Internet, établissent aussi un équilibre approprié entre tous les intérêts en jeu.

Justification

Une durée de six mois maximum respecte le principe de proportionnalité, la quasi-totalité des enquêtes étant résolue par une exploitation de données ayant moins de six mois d'ancienneté.

Amendement 2 CONSIDÉRANT 13

(13) Considérant que la conservation de données **crée** des coûts significatifs supplémentaires pour les fournisseurs de services de communications électroniques, alors que les bénéfices en *terme* de sécurité publique visent la société dans son ensemble, il est nécessaire de prévoir que les

(13) Considérant que la conservation **et la mise à disposition** de données **créent** des coûts significatifs supplémentaires pour les fournisseurs de services de communications électroniques, alors que les bénéfices en *termes* de sécurité publique visent la société dans son ensemble, il est nécessaire de

¹ JO C ... / Non encore publié au JO.

États membres *veillent à ce que* les fournisseurs de services de communications électroniques *obtiennent* le remboursement des surcoûts qu'ils justifient avoir supportés pour s'acquitter des obligations leur incombant en vertu de la présente directive.

prévoir que les États membres *assurent à tous* les fournisseurs de services de communications électroniques le remboursement *intégral* des surcoûts qu'ils justifient avoir supportés pour s'acquitter des obligations leur incombant en vertu de la présente directive.

Justification

Le surcoût occasionné par cette procédure utile à la sécurité des États européens ne doit pas être à la charge des opérateurs.

Amendement 3 CONSIDÉRANT 14

(14) Les technologies liées aux communications électroniques progressent rapidement et les exigences légitimes des autorités compétentes peuvent évoluer; afin d'obtenir des avis à ce sujet, la Commission prévoit de créer une plate-forme composée de représentants des services répressifs, des associations du secteur des communications électroniques et des autorités chargées de la protection des données.

(14) Les technologies liées aux communications électroniques progressent rapidement et les exigences légitimes des autorités compétentes peuvent évoluer; afin d'obtenir des avis à ce sujet, la Commission prévoit de créer une plate-forme composée de représentants des services répressifs, des associations du secteur des communications électroniques et des autorités chargées de la protection des données. ***La Commission s'engage à consulter le Parlement européen sur toute perspective d'adaptation des dispositions de la présente directive.***

Justification

L'implication du Parlement européen dans toute révision de la présente directive s'impose, au regard des éventuelles atteintes aux libertés et droits fondamentaux.

Amendement 4 CONSIDÉRANT 16

(16) Il est fondamental que les États membres prennent des mesures législatives pour faire en sorte que les données conservées en vertu de la présente directive ne soient transmises qu'aux autorités nationales compétentes conformément à la législation nationale, les droits

(16) Il est fondamental que les États membres prennent des mesures législatives pour faire en sorte que les données conservées en vertu de la présente directive ne soient transmises qu'aux autorités nationales compétentes conformément à la législation nationale ***et exploitées par elles,***

fondamentaux des personnes concernées étant pleinement respectés; de telles mesures portent notamment sur les conditions, limites et garanties requises pour assurer la conformité de cette transmission avec les droits fondamentaux tels qu'ils sont consacrés en particulier dans la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

les droits fondamentaux des personnes concernées étant pleinement respectés; de telles mesures portent notamment sur les conditions, limites et garanties requises pour assurer la conformité de cette transmission avec les droits fondamentaux tels qu'ils sont consacrés en particulier dans la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

Justification

Le respect des libertés et droits fondamentaux impose que seules les autorités nationales puissent exploiter ces données.

Amendement 5
CONSIDÉRANT 17

(17) Il y a lieu d'arrêter les mesures nécessaires pour la mise en œuvre de la présente directive en conformité avec la décision 1999/468/CE du Conseil du 28 juin 1999 fixant les modalités de l'exercice des compétences d'exécution conférées à la Commission. ***supprimé***

Justification

L'on ne peut accepter la procédure de comitologie prévue par la Commission, qui permet aux représentants de la Commission et des États membres de continuer à compléter les données à conserver en dehors de la participation du Parlement et des entreprises concernées. Tout ajout à la liste des types de données à conserver constitue une mesure touchant aux droits fondamentaux, à propos de laquelle le Parlement doit pouvoir émettre une réserve. C'est pourquoi ce considérant doit être supprimé.

Amendement 6
CONSIDÉRANT 19 BIS (nouveau)

(19 bis) Les États membres veillent à ce que les opérateurs économiques soient dûment consultés avant la mise en application de la présente directive, en ce qui concerne en particulier la faisabilité et les coûts de la conservation des données. Étant donné que la conservation des données représente une

charge matérielle et financière pour les opérateurs économiques, les États membres garantissent la compensation intégrale des coûts supplémentaires à la charge des opérateurs économiques du fait d'obligations liées à l'application de la présente directive ou d'obligations librement consenties.

Justification

La lutte contre la criminalité et la garantie de la sécurité publique sont des missions fondamentales de l'État moderne. Dès lors, les mesures adoptées en la matière doivent être financées intégralement par les pouvoirs publics et ne pas être à la charge des opérateurs économiques, faute de quoi l'Europe sera moins attrayante pour les entreprises. Il en résulte que l'intégralité des coûts (coûts d'investissement et d'exploitation) occasionnés par toutes les obligations découlant de la directive doit être supportée par les États membres. Cela vaut également pour l'élaboration de statistiques, qui doit incomber principalement aux États membres.

Amendement 7

ARTICLE 1, PARAGRAPHE 2

2. La présente directive s'applique aux données relatives au trafic et aux données de localisation concernant les personnes tant physiques que morales, ainsi qu'aux données connexes nécessaires pour identifier l'abonné ou l'utilisateur enregistré. Elle ne s'applique pas au contenu des communications électroniques, notamment aux informations consultées en utilisant un réseau de communications électroniques.

2. La présente directive comportant des dispositions dérogatoires, son application sera soumise à évaluation régulière sous le contrôle du Parlement européen. Celui-ci doit disposer des informations lui permettant de constater que l'application de la présente directive ne contrevient pas au respect de la Charte des droits fondamentaux de l'Union européenne, notamment concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

La présente directive s'applique aux données relatives au trafic et aux données de localisation concernant les personnes tant physiques que morales, ainsi qu'aux données connexes nécessaires pour identifier l'abonné ou l'utilisateur enregistré. Elle ne s'applique pas au contenu des communications électroniques, notamment aux informations consultées en utilisant un réseau de communications électroniques.

Justification

L'implication du Parlement européen dans toute révision de la présente directive s'impose, au regard des éventuelles atteintes aux libertés et droits fondamentaux.

Amendement 8 ARTICLE 3, PARAGRAPHE 1

1. Par dérogation aux articles 5, 6 et 9 de la directive 2002/58/CE, les États membres prennent les mesures nécessaires pour **assurer la conservation**, conformément aux dispositions de la présente directive, **de** données générées ou traitées dans le cadre de la fourniture de services de communication par des fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications, lorsque ces fournisseurs relèvent de leur juridiction.

1. Par dérogation aux articles 5, 6 et 9 de la directive 2002/58/CE, les États membres prennent les mesures nécessaires pour **que, lorsque la connexion a été établie avec succès, les données répondant à l'objectif visé à l'article 1, paragraphe 1, soient conservées** conformément aux dispositions de la présente directive **si ces données sont** générées ou traitées dans le cadre de la fourniture de services de communication par des fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications, lorsque ces fournisseurs relèvent de leur juridiction.

Justification

L'amendement au paragraphe 1 vise à préciser que la conservation des données ne peut être exigée que dans le cas où celles-ci sont générées ou traitées dans le cadre de la fourniture de services de communication. Sinon, des services qui ne génèrent pas certains types de données ne pourraient plus être offerts du fait de l'obligation de conservation (par exemple, les services téléphoniques prépayés). Il serait préjudiciable à l'ensemble de l'économie européenne et contraire aux objectifs de Lisbonne d'empêcher la fourniture de ces services ou de la soumettre à des contraintes excessives.

Amendement 9 ARTICLE 3, PARAGRAPHE 1 BIS (nouveau)

1 bis. Les États membres peuvent prévoir, eu égard aux critères de nécessité et de proportionnalité, que le paragraphe 1 ne s'applique pas aux fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communication, compte tenu des parts de marché, du nombre d'abonnés ainsi que

de la dimension du réseau géré par rapport à celle du marché.

Justification

Les petits fournisseurs de services ne sont pas à même de respecter les nombreuses obligations prévues en matière de conservation des données, même s'ils sont entièrement indemnisés de leurs frais, étant donné qu'ils seraient contraints non seulement de modifier leurs systèmes, mais aussi de revoir leurs méthodes commerciales et de répondre en permanence à des demandes émanant des autorités. Cela ne serait pas viable financièrement et entraînerait la disparition des petits et moyens prestataires de services. Cela aurait aussi de graves répercussions sur l'économie européenne, où les PME sont la principale force d'innovation.

Amendement 10
ARTICLE 3, PARAGRAPHE 2

2. Les États membres prennent les mesures nécessaires pour veiller à ce que les données conservées conformément à la présente directive ne soient transmises qu'aux autorités nationales compétentes, dans des cas précis conformément à la législation nationale, et à des fins de prévention, de recherche, de détection et de poursuite des infractions pénales graves, comme les actes terroristes et la criminalité organisée.

2. Les États membres prennent les mesures nécessaires pour veiller à ce que les données conservées conformément à la présente directive ne soient transmises qu'aux autorités nationales compétentes, ***et ne soient exploitées que par elles***, dans des cas précis conformément à la législation nationale, et à des fins de prévention, de recherche, de détection et de poursuite des infractions pénales graves, comme les actes terroristes et la criminalité organisée. ***Les autorités nationales compétentes doivent pouvoir justifier de leur demande de transmission sans qu'il soit porté atteinte à la relation contractuelle liant le fournisseur à son client et sans contrevenir au respect de la Charte des droits fondamentaux de l'Union européenne, notamment concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.***

Justification

La relation contractuelle existant entre l'opérateur et son client ne doit pas être modifiée par ces mesures de conservation des données. Les autorités compétentes doivent être en mesure de prouver que leur demande est utile au regard de la prévention, de la recherche, de la

détection ou de la poursuite d'infractions pénales graves, comme les actes terroristes et la criminalité organisée.

Amendement 11
ARTICLE 4, PARTIE INTRODUCTIVE

Les États membres veillent à ce que soient conservées en application de la présente directive **les catégories de données suivantes**:

Les États membres veillent à ce que, ***dans le cas de communications établies avec succès, les catégories de données suivantes*** soient conservées en application de la présente directive ***et aux fins visées à l'article 1, paragraphe 1, à la condition qu'elles soient générées ou traitées dans le cadre de la fourniture de services de communications par des fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communication***:

Justification

D'ores et déjà, les entreprises de télécommunications conservent un grand nombre des données requises par la proposition de directive. L'obligation renforcée de conserver des données n'entraînerait qu'une charge financière supplémentaire considérable, les bases de données existantes devant être élargies et adaptées. L'obligation de conserver des données ne doit par conséquent se concentrer que sur les communications établies avec succès.

Amendement 12
ARTICLE 4, POINT A)

a) les données nécessaires pour retrouver et identifier la source d'une communication;

a) les données nécessaires pour retrouver et identifier la source d'une communication:

(1) en ce qui concerne la téléphonie fixe en réseau:

a) le numéro de téléphone de l'appelant,

b) les nom et adresse de l'abonné ou de l'utilisateur enregistré;

(2) en ce qui concerne la téléphonie mobile:

a) le numéro de téléphone de l'appelant,

b) les nom et adresse de l'abonné ou de l'utilisateur enregistré;

(3) en ce qui concerne les services d'accès à Internet:

a) l'adresse du protocole Internet (adresse IP), qu'elle soit dynamique ou statique, attribuée à une communication par le fournisseur d'accès Internet,

b) le code d'identification personnel de la source d'une communication,

c) les nom et adresse de l'abonné ou de l'utilisateur enregistré à qui l'adresse IP, l'identité de connexion ou le code d'identification personnel ont été attribués au moment de la communication;

Amendement 13
ARTICLE 4, POINT B)

b) les données nécessaires pour *retrouver et* identifier la destination d'une communication;

b) les données nécessaires pour identifier la destination d'une communication:

(1) en ce qui concerne la téléphonie fixe en réseau:

a) le ou les numéros de téléphone appelés;

(2) en ce qui concerne la téléphonie mobile:

a) le ou les numéros de téléphone appelés;

(3) en ce qui concerne les services d'accès à Internet:

a) l'identité de connexion ou le code d'identification personnel du ou des destinataires visés d'une communication;

Amendement 14
ARTICLE 4, POINT C)

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

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

(1) en ce qui concerne la téléphonie fixe en réseau et la téléphonie mobile:

a) la date et l'heure de début et de fin de la communication;

(2) en ce qui concerne les services d'accès à Internet:

a) la date et l'heure d'ouverture et de fermeture des sessions Internet dans un fuseau horaire déterminé;

Amendement 15
ARTICLE 4, POINT D)

d) les données nécessaires pour déterminer le type de communication;

d) les données nécessaires pour déterminer le type de communication:

(1) en ce qui concerne la téléphonie fixe en réseau:

a) le service téléphonique utilisé, par exemple voix, télécopie et services de messagerie;

(2) en ce qui concerne la téléphonie mobile:

a) le service téléphonique utilisé, par exemple voix, service de minimessages (SMS);

Amendement 16
ARTICLE 4, POINT E)

e) les données nécessaires pour déterminer le dispositif de communication utilisé ou ce qui est censé avoir été utilisé comme dispositif de communication;

e) les données nécessaires pour déterminer le dispositif de communication utilisé ou ce qui est censé avoir été utilisé comme dispositif de communication:

(1) en ce qui concerne la téléphonie mobile:

a) l'identité internationale d'abonné mobile (IMSI) de l'appelant;

(2) en ce qui concerne les services d'accès à Internet:

a) le numéro de téléphone de l'appelant pour l'accès commuté,

b) la ligne d'abonné numérique (DSL) ou tout autre identifiant terminal de l'auteur de la communication;

Justification

Le numéro de série du téléphone mobile est attribué plusieurs fois par le fabricant et peut être manipulé par l'utilisateur.

Le numéro d'identification de la carte réseau d'un ordinateur ne peut être rattaché clairement à l'appelant étant donné qu'il peut également être attribué plusieurs fois par le fabricant et être facilement manipulé ultérieurement par l'utilisateur. La conservation de ces deux types de données n'est guère de nature à améliorer sensiblement la lutte contre la criminalité.

Amendement 17
ARTICLE 4, POINT F)

f) les données nécessaires pour localiser le matériel de communication mobile.

f) les données nécessaires pour localiser le matériel de communication mobile:

(1) l'identité de localisation (identifiant cellulaire) au début de la communication.

Justification

La proposition visant à conserver les identités de localisation, y compris à la fin d'une communication, signifie un surcoût considérable. Jusqu'à présent, certains États membres ne conservent que la localisation au début d'une communication. En outre, l'identité de localisation conservée au début de chaque nouvelle communication suffit pour établir rétrospectivement un profil de déplacement relativement précis.

Amendement 18
ARTICLE 4, ALINÉA 2

Les types de données à conserver pour chacune des catégories de données susmentionnées sont précisés en annexe.

supprimé

Amendement 19
ARTICLE 5

Article 5
Révision de l'annexe

supprimé

L'annexe fait l'objet d'une révision régulière s'il y a lieu, selon la procédure prévue à l'article 6, paragraphe 2.

Justification

L'on ne peut accepter la procédure de comitologie prévue par la Commission, qui permet aux représentants de la Commission et des États membres de continuer à compléter les données à conserver en dehors de la participation du Parlement et des entreprises concernées. Tout ajout à la liste des types de données à conserver constitue une mesure touchant aux droits fondamentaux, à propos de laquelle le Parlement doit pouvoir émettre une réserve. C'est pourquoi ces dispositions doivent être supprimées.

Amendement 20
ARTICLE 6

Article 6

supprimé

Comité

1. La Commission est assistée par un comité composé de représentants des États membres et présidé par le représentant de la Commission.

2. Dans le cas où il est fait référence au présent paragraphe, les articles 5 et 7 de la décision 199/468/CE s'appliquent, dans le respect des dispositions de l'article 8 de celle-ci.

3. Le délai prévu à l'article 5, paragraphe 6, de la décision 1999/468/CE est fixé à trois mois.

Justification

L'on ne peut accepter la procédure de comitologie prévue par la Commission, qui permet aux représentants de la Commission et des États membres de continuer à compléter les données à conserver en dehors de la participation du Parlement et des entreprises concernées. Tout ajout à la liste des types de données à conserver constitue une mesure touchant aux droits fondamentaux, à propos de laquelle le Parlement doit pouvoir émettre une réserve. C'est pourquoi cet article doit être supprimé.

Amendement 21
ARTICLE 7

Les États membres veillent à ce que les catégories de données visées à l'article 4 soient conservées pour une durée **d'un an** à compter de la date de la communication, à l'exception des données relatives à des communications électroniques utilisant uniquement ou principalement le protocole Internet. Ces dernières données sont conservées pour une durée de **six mois**.

Les États membres veillent à ce que les catégories de données visées à l'article 4 soient conservées pour une durée **de six mois** à compter de la date de la communication, à l'exception des données relatives à des communications électroniques utilisant uniquement ou principalement le protocole Internet. Ces dernières données sont conservées pour une durée de **trois mois**. **À la fin de cette période, les données doivent être effacées ou rendues anonymes, conformément à la directive 2002/58/CE.**

Justification

Une durée de six mois maximum respecte le principe de proportionnalité, la quasi-totalité des enquêtes étant résolues grâce à des données d'une ancienneté maximale de six mois.

Amendement 22 ARTICLE 8

Les États membres veillent à ce que les données soient conservées conformément à la présente directive de manière ce **que les données conservées et toute autre information nécessaire concernant ces données** puissent, **à leur demande**, être transmises **sans** délai aux autorités compétentes.

Les États membres veillent à ce que les données soient conservées conformément à la présente directive de manière à ce **qu'elles** puissent être transmises **dans un** délai **raisonnable** aux autorités compétentes, **sur instruction écrite et motivée de leur part**.

Justification

Les dispositions de la directive à l'examen font exception aux dispositions des articles 5, 6 et 9 de la directive 2002/58/CE. Il y a lieu par conséquent de trancher la question des données à transmettre. Il faut prévoir également une procédure pour la transmission afin de garantir la sécurité juridique et la protection des données. L'expérience montre que la transmission peut prendre du temps pour des raisons techniques, aussi ne peut-elle pas toujours être effectuée sans délai.

Amendement 23 ARTICLE 9, ALINÉA 1

Les États membres font en sorte que des statistiques sur la conservation de données

Les États membres font en sorte que des statistiques sur la conservation de données

traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public soient transmises annuellement à la Commission *européenne*. Ces statistiques concernent notamment:

- les cas dans lesquels des informations ont été transmises aux autorités compétentes conformément à la législation nationale applicable,
- le laps de temps écoulé entre la date à partir de laquelle les données ont été conservées et la date à laquelle les autorités compétentes ont demandé leur transmission,
- les cas dans lesquels des demandes de données n’ont pu être satisfaites.

traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public soient transmises annuellement *par les autorités compétentes* à la Commission *et au Parlement européen*. Ces statistiques concernent notamment:

- les cas dans lesquels des informations ont été transmises aux autorités compétentes conformément à la législation nationale applicable,
- le laps de temps écoulé entre la date à partir de laquelle les données ont été conservées et la date à laquelle les autorités compétentes ont demandé leur transmission,
- les cas dans lesquels des demandes de données n’ont pu être satisfaites, *et*
– les cas dans lesquels des demandes de certains types de données ont abouti à un résultat positif en matière de poursuites.

Justification

L'obligation pour les États membres, à l'article 9 de la proposition, de présenter des statistiques concernant la conservation ne doit pas se solder par un effort bureaucratique supplémentaire pour les entreprises. Néanmoins, ces statistiques pourraient également être utilisées pour établir le nombre de cas dans lesquels les demandes ont effectivement permis de mener à bien une enquête.

Amendement 24 ARTICLE 10

Les États membres veillent à ce que les fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications obtiennent le remboursement des surcoûts qu'ils justifient avoir supportés pour s'acquitter des obligations leur incombant en vertu de la présente directive.

Les États membres veillent à ce que *tous* les fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications obtiennent le remboursement *intégral de l'ensemble* des surcoûts qu'ils justifient avoir supportés pour s'acquitter des obligations leur incombant en vertu de la présente directive.

Justification

Il est positif que la proposition de la Commission prévoit le remboursement des coûts d'investissement et de fonctionnement pour les entreprises. L'ajout ne sert qu'à clarifier le texte. Parallèlement, le remboursement des coûts est également une mesure régulatoire

importante permettant de limiter au minimum les demandes formulées par les autorités chargées des poursuites pénales et d'éviter les distorsions de la concurrence entre États membres dues à la diversité des modes de remboursement.

Amendement 25
ARTICLE 12, PARAGRAPHE 1

1. Au plus tard trois ans après la date visée à l'article 13, paragraphe 1, la Commission présente au Parlement européen et au Conseil une évaluation de l'application de la présente directive et de ses effets sur les opérateurs économiques et les consommateurs, compte tenu des statistiques transmises à la Commission en vertu de l'article 9 afin de déterminer s'il y a lieu de modifier les dispositions de la présente directive, notamment **la durée de conservation prévue à l'article 7.**

1. Au plus tard trois ans après la date visée à l'article 13, paragraphe 1, la Commission présente au Parlement européen et au Conseil une évaluation de l'application de la présente directive et de ses effets sur les opérateurs économiques et les consommateurs, compte tenu des statistiques transmises à la Commission en vertu de l'article 9, afin de déterminer s'il y a lieu de modifier les dispositions de la présente directive, notamment **les types de données visés à l'article 4.**

Justification

Eu égard à la proposition de suppression de la procédure de comitologie prévue à l'article 5, il y a lieu de prévoir une évaluation de toutes les dispositions de la directive, sans distinction. Étant donné que les entreprises sont soumises à l'obligation de conservation des données, laquelle implique des coûts considérables pour l'économie, cet aspect doit être pris en considération dans le cadre d'une évaluation de la directive.

Amendement 26
ARTICLE 12, PARAGRAPHE 2

2. À cette fin, la Commission examine toute observation qui pourrait lui être transmise par les États membres ou le groupe de protection des personnes à l'égard du traitement des données à caractère personnel institué par l'article 29 de la directive 95/46/CE.

2. À cette fin, la Commission examine toute observation qui pourrait lui être transmise par les États membres, **par les opérateurs économiques** ou le groupe de protection des personnes à l'égard du traitement des données à caractère personnel institué par l'article 29 de la directive 95/46/CE **ainsi que tout rapport établi par le Parlement européen au titre de l'article premier de la présente directive.**

Justification

L'implication du Parlement européen dans toute révision de la présente directive s'impose, au regard des éventuelles atteintes aux libertés et droits fondamentaux.

Amendement 27
ANNEXE

Cette annexe est supprimée.

Justification

Il y a lieu de supprimer intégralement l'annexe et de l'intégrer à l'article 4. La liste des données constitue la disposition fondamentale de la directive à l'examen et n'est pas seulement une disposition à caractère technique concernant des points de détail. L'utilité, la faisabilité, les coûts et le caractère proportionné de la conservation des données dépendent du type de données à conserver. Par conséquent, la liste des données devrait figurer, non pas dans une annexe, séparée du dispositif de la directive, mais directement à l'article 4.

PROCÉDURE

| | |
|---|--|
| Titre | Proposition de directive du Parlement européen et du Conseil sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, et modifiant la directive 2002/58/CE |
| Références | COM(2005)0438 – C6-0293/2005 – 2005/0182(COD) |
| Commission compétente au fond | LIBE |
| Avis émis par Date de l'annonce en séance | ITRE 15.11.2005 |
| Coopération renforcée – date de l'annonce en séance | Non |
| Rapporteure pour avis Date de la nomination | Angelika Niebler 5.10.2005 |
| Rapporteur pour avis remplacé | |
| Examen en commission | 22.11.2005 23.11.2005 |
| Date de l'adoption | 23.11.2005 |
| Résultat du vote final | +: 37 –: 4 0: 1 |
| Membres présents au moment du vote final | Ivo Belet, Jan Březina, Philippe Busquin, Jerzy Buzek, Joan Calabuig Rull, Pilar del Castillo Vera, Jorgo Chatzimarkakis, Giles Chichester, Den Dover, Lena Ek, Nicole Fontaine, Adam Gierek, Norbert Glante, Umberto Guidoni, András Gyürk, Fiona Hall, David Hammerstein Mintz, Ján Hudacký, Romana Jordan Cizelj, Werner Langen, Anne Laperrouze, Nils Lundgren, Eluned Morgan, Angelika Niebler, Reino Paasilinna, Umberto Pirilli, Miloslav Ransdorf, Vladimír Remek, Herbert Reul, Mechtild Rothe, Paul Rübig, Britta Thomsen, Patrizia Toia, Catherine Trautmann, Claude Turmes, Nikolaos Vakalis, Alejo Vidal-Quadras Roca, Dominique Vlasto |
| Suppléant(s) présent(s) au moment du vote final | Avril Doyle, Erna Hennicot-Schoepges, Vittorio Prodi, Hannes Swoboda |
| Suppléant(s) (art. 178, par. 2) présent(s) au moment du vote final | |
| Observations (données disponibles dans une seule langue) | ... |

22.11.2005

AVIS DE LA COMMISSION DU MARCHÉ INTERIEUR ET DE LA PROTECTION DES CONSOMMATEURS

à l'intention de la commission des libertés civiles, de la justice et des affaires intérieures

sur la proposition de directive du Parlement européen et du Conseil sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public et modifiant la directive 2005/58/CE (COM(2005)0438 – C6-0293/2005 – 2002/0182(COD))

Rapporteur pour avis: Charlotte Cederschiöld

JUSTIFICATION SUCCINCTE

Étant donné que la proposition de la Commission repose sur l'article 95 du traité – l'article concernant le marché intérieur –, il est indispensable que la commission du marché intérieur et de la protection des consommateurs puisse émettre un avis.

Les mesures relatives à la conservation de données affectent toutes les catégories sociales avec de larges implications économiques, sociales et industrielles. Les dispositions concernant l'harmonisation de la conservation de données dans l'UE ont des répercussions importantes non seulement pour les consommateurs européens mais également pour l'industrie européenne et finalement pour le marché intérieur. Si l'harmonisation n'est pas mise en place avec l'attention nécessaire, les droits fondamentaux des citoyens et la compétitivité européenne seront menacés.

Situation actuelle

Tous les États membres ont mis en place des régimes différents en ce qui concerne les périodes de conservation de données, les types de données à conserver et le remboursement des frais supportés par les industriels. Une approche européenne harmonisée pourrait améliorer la situation si elle était soigneusement conçue tout en respectant l'équilibre entre tous les intérêts en présence et les parties concernées.

La conservation de données représente une évolution dans la façon dont la société considère les données relatives au trafic. Selon la législation actuelle, les fournisseurs de services de communications électroniques sont seuls autorisés à conserver des données relatives au trafic à des fins commerciales légitimes et spécifiques et ont l'obligation d'effacer ces données une fois l'objectif atteint. La nouvelle proposition prévoit que les opérateurs seront tenus de

stocker de grandes quantités de données nouvelles pour des raisons spécifiques d'ordre public, ce qui place l'Union européenne dans une position unique, aucun autre pays démocratique dans le monde n'ayant instauré jusqu'à présent de telles obligations. Ce fait mérite d'être examiné avec attention, en termes de confidentialité, de compétitivité et de sécurité.

Dans l'intérêt d'une meilleure réglementation, il est permis de se demander si l'UE devrait introduire de telles obligations à ce stade sans examiner avec soin les conséquences à long terme par le biais d'une étude d'impact approfondie. Le système de préservation et de "gel" de données pourrait être un meilleur moyen de renforcer la coopération entre les industriels et les administrations répressives et devrait être analysé du point de vue du consommateur et du point de vue du marché intérieur.

Les procédures de comitologie proposées ne sont pas acceptables – une solution doit être trouvée à un niveau plus large qui inclut tous les acteurs intéressés qui n'ont pas été suffisamment consultés avant la présentation de la proposition.

Impact sur le marché intérieur et la compétitivité européenne

Les chefs d'État et de gouvernement ont à plusieurs reprises défini les communications électroniques comme un pilier de l'économie européenne: indispensables à une croissance durable et optimisant l'emploi. Toute réglementation, y compris en matière de conservation de données doit être examinée avec attention avant d'être mise en place afin de ne pas entraver la compétitivité et le développement des entreprises européennes.

Coûts

Réussir à collecter de grandes quantités de données comme prévu dans la proposition de directive est difficile et coûteux. S'efforcer de rendre cohérents les différents formats de données et les interpréter en éléments utiles pour les administrations répressives est encore plus difficile.

Les coûts, proportionnels au volume de données conservées, augmenteront considérablement en raison des changements apportés à la conception des systèmes de gestion, de plates-formes plus puissantes et plus sophistiquées, de mesures de sécurité renforcées, d'infrastructures de stockage et de soutien ainsi qu'en raison des ressources humaines nécessaires pour gérer ce type de système.

Il est évident que la conservation de données entraînera pour l'industrie européenne des communications des coûts très importants. Le risque d'une approche fragmentée à l'égard de la question des coûts est évident: si certains États membres remboursent les fournisseurs de services de communications électroniques pour la conservation de données alors que d'autres ne le font pas, le marché intérieur des services de communications souffrira de graves distorsions de concurrence.

Investissements

Les fournisseurs de services de communications européens rodent actuellement les réseaux de la prochaine génération afin de répondre à la nécessité de nouveaux services informatiques dans le domaine privé et public. Instaurer la conservation de données sans une pleine

compensation des coûts contraindrait les opérateurs à consacrer des ressources à l'adaptation au nouveau système, alors que ces ressources pourraient être affectées à la constitution des réseaux de demain.

Concurrence

Indépendamment de la question de savoir si l'harmonisation est pleinement achevée dans l'UE, il reste que les fournisseurs de services de pays tiers ne seront pas soumis aux mêmes obligations et aux mêmes contraintes. Ceci affectera la compétitivité et l'équilibre entre l'UE et les économies rivales. De nombreux prestataires de services de communications électroniques, en particulier les fournisseurs de services Internet sont basés dans un pays tiers tout en exerçant une concurrence dans le marché intérieur. Des plates-formes de services peuvent être créées n'importe où dans le monde: ainsi, les fournisseurs de pays tiers se trouveront même en position d'offrir des "*services de non-conservation*" et pourront justifier leur attitude par le souci d'intégrité et de confidentialité des usagers. Des obligations contraignantes en matière de conservation de données pourraient dissuader les consommateurs européens de recourir à des services européens.

Lorsqu'un opérateur européen fournit l'accès à Internet alors que l'utilisateur a recours à un fournisseur de courrier électronique américain (par exemple Hotmail, Gmail, Yahoo), le fournisseur d'accès européen n'a pas accès aux données de localisation comme l'exige la proposition de la Commission. En outre, un grand nombre des principaux fournisseurs de courrier électronique sont basés dans un pays tiers et ne seront donc en aucun cas soumis aux exigences prévues.

Sécurité

S'il est possible d'atteindre des niveaux élevés de sécurité de l'information, une garantie de sécurité totale est virtuellement impossible à obtenir. Il sera essentiel de veiller à ce que les données stockées soient authentiques et protégées contre toute altération, que les contrôles d'accès soient vigilants et que la traçabilité et les étapes de la conservation puissent être clairement contrôlées. La conservation et le stockage de grandes quantités de données sensibles seront également confrontés à des défis au niveau du logiciel et du réseau (codes nocifs, logiciels espions, spam, phishing) ainsi qu'à des menaces non liées à Internet (par exemple le vol physique de cassettes de données conservées).

En outre, la proposition ne contient pas de dispositions de sécurité concernant la procédure à suivre une fois les informations collectées dans l'État membre, elle n'indique pas si et comment elles peuvent être transférées à d'autres États membres et ne contient pas non plus de dispositions interdisant le transfert de données conservées vers des pays tiers. Tous ces aspects de sécurité sont une menace potentielle pour le consommateur européen.

AMENDEMENTS

La commission du marché intérieur et de la protection des consommateurs invite la commission des libertés civiles, de la justice et des affaires intérieures, compétente au fond, à

incorporer dans son rapport les amendements suivants:

Projet de résolution législative

Amendement 1 Paragraphe 1 bis (nouveau)

1 bis. *invite la Commission à commander, avant l'entrée en vigueur de la présente directive, une étude d'impact réalisée par un organisme indépendant représentant tous les acteurs concernés, couvrant toutes les questions relatives au marché intérieur et à la protection des consommateurs;*

Proposition pour une directive

Texte proposé par la Commission¹

Amendements du Parlement

Amendement 2 CONSIDÉRANT 13

(13) Considérant que la conservation de données crée des coûts significatifs supplémentaires pour les fournisseurs de services de communications électroniques, alors que les bénéfices en terme de sécurité publique visent la société dans son ensemble, il est nécessaire de prévoir que les États membres veillent à ce que les fournisseurs de services de communications électroniques **obtiennent le** remboursement des surcoûts qu'ils justifient avoir supportés pour s'acquitter des obligations leur incombant en vertu de la présente directive.

(13) Considérant que la conservation de données crée des coûts significatifs supplémentaires pour les fournisseurs de services de communications électroniques, alors que les bénéfices en terme de sécurité publique visent la société dans son ensemble, **et afin d'éviter des distorsions dans le marché intérieur**, il est nécessaire de prévoir que les **tous** États membres veillent à ce que les fournisseurs de services de communications électroniques **accessibles au public ou d'un réseau public de communications bénéficient du plein** remboursement **harmonisé** des surcoûts qu'ils justifient avoir supportés pour s'acquitter des obligations leur incombant en vertu de la présente directive.

Amendement 3 CONSIDÉRANT 13 BIS (nouveau)

(13 bis) Les coûts doivent être maintenus

¹ JO C ... / Non encore publié au JO.

aussi bas que possible afin d'éviter de placer les sociétés européennes dans une situation de concurrence défavorable par rapport aux sociétés de pays tiers.

Amendement 4
Considérant 14

(14) Les technologies liées aux communications électroniques progressent rapidement et les exigences légitimes des autorités compétentes peuvent évoluer; afin d'obtenir des avis à ce sujet, **la Commission prévoit** de créer **une plate-forme composée** de représentants des services répressifs, **des associations** du secteur des communications électroniques et des autorités chargées de la protection des données.

(14) Les technologies liées aux communications électroniques progressent rapidement et les exigences légitimes des autorités compétentes peuvent évoluer; afin d'obtenir des avis à ce sujet, **il est nécessaire** de créer **un comité permanent composé** de représentants **du Parlement européen**, des services répressifs, du secteur des communications électroniques, **des associations de protection des consommateurs** et des autorités chargées de la protection des données.

Amendement 5
Considérant 18 bis (nouveau)

(18 bis) Étant donné que la sécurité des données conservées en vertu de la présente directive présente une extrême importance pour la sauvegarde des droits des consommateurs, les États membres devraient veiller à ce que les normes les plus élevées de sécurité en matière de stockage des données soient appliquées, en particulier en ce qui concerne la protection des données contre toute altération et accès non autorisé ainsi que contre les menaces liées ou non à Internet.

Amendement 6
CONSIDERANT 18 BIS (nouveau)

(18 bis) La protection des données conservées en vertu de la présente directive est conforme aux dispositions relatives à la protection des données de la

directive 2002/58/CE.

Amendement 7
ARTICLE 1, PARAGRAPHE 1

1. La présente directive a pour objectif d'harmoniser les dispositions des États membres relatives aux obligations des fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications en matière de traitement et de conservation de certaines données, en vue de garantir la disponibilité de ces données à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales ***graves, comme les actes terroristes et la criminalité organisée.***

1. La présente directive a pour objectif d'harmoniser les dispositions des États membres relatives aux obligations des fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications en matière de traitement et de conservation de certaines données, en vue de garantir la disponibilité de ces données à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales.

Justification

Cette proposition a trait à l'article 15 de la directive sur la protection des données dans le secteur des communications électroniques (2002/58) laquelle établit que les États membres peuvent adopter des dispositions relatives à la conservation des données "pour sauvegarder la sécurité nationale..., la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques". Le champ d'application de la proposition de la Commission est cependant beaucoup plus limité que le "mandat" donné par l'article 15 et devrait être étendu. Les exigences en matière de conservation des données sont de première importance pour permettre que soient prises des mesures en vue d'appliquer la loi et que des procédures judiciaires puissent être engagées contre toutes les formes de crimes commis par le biais du système de communications électroniques. Sans l'obligation de conserver les données, les autorités sont confrontées à des obstacles importants pour poursuivre les activités illégales et identifier les suspects d'infractions ainsi que pour prendre des mesures d'application des peines et des droits légaux. En outre, la définition de "graves" prête à interprétation, ce qui pourrait créer une forte incertitude juridique.

Amendement 8
Article 3, paragraphe 1

1. Par dérogation aux articles 5, 6 et 9 de la directive 2002/58/CE, les États membres prennent les mesures nécessaires pour assurer la conservation, conformément aux dispositions de la présente directive, de données ***générées ou*** traitées dans le cadre

1. Par dérogation aux articles 5, 6 et 9 de la directive 2002/58/CE, les États membres prennent les mesures nécessaires pour assurer la conservation, conformément aux dispositions de la présente directive, de données traitées ***et stockées*** dans le cadre de

de la fourniture de services de communication par des fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications, lorsque ces fournisseurs relèvent de leur juridiction.

la fourniture de services de communication par des fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications, lorsque ces fournisseurs relèvent de leur juridiction.

Justification

Il est indispensable que le champ d'application de la directive soit clairement défini: le terme "général" étant très large et peu explicite devrait être remplacé par un terme d'ores et déjà en usage dans la législation européenne. Le traitement est défini dans la directive générale concernant la protection des données (article 2 bis) alors que la directive sur la conservation de données dans le domaine des communications électroniques se réfère au traitement et au stockage dans son article 6.

Amendement 9 ARTICLE 3, PARAGRAPHE 2

2. Les États membres prennent les mesures nécessaires pour veiller à ce que les données conservées conformément à la présente directive **ne** soient transmises **qu'**aux autorités nationales compétentes, dans des cas précis conformément à la législation nationale, et à des fins de prévention, de recherche, de détection et de poursuite des infractions pénales **graves, comme les actes terroristes et la criminalité organisée.**

2. Les États membres prennent les mesures nécessaires pour veiller à ce que les données conservées conformément à la présente directive soient transmises aux autorités nationales compétentes, dans des cas précis conformément à la législation nationale, et à des fins de prévention, de recherche, de détection et de poursuite des infractions pénales.

Justification

La proposition de la Commission est trop restrictive comparée au "mandat" donné par l'article 15 de la directive sur la protection des données dans le secteur des communications électroniques (2002/58) et devrait par conséquent être élargie. Les exigences en matière de conservation des données sont de première importance pour permettre que soient prises des mesures en vue d'appliquer la loi et que des procédures judiciaires puissent être engagées contre toutes les formes de crimes commis par le biais du système de communications électroniques. Sans l'obligation de conserver les données, les autorités sont confrontées à des obstacles importants pour poursuivre les activités illégales et identifier les suspects d'infractions ainsi que pour prendre des mesures d'application des peines et des droits légaux. En outre, la définition de "graves" prête à interprétation, ce qui pourrait créer une forte incertitude juridique. Enfin, cet instrument ne peut préjuger d'autres mesures communautaires ou nationales en vue de l'application des droits.

Amendement 10
Article 5

Article 5
Révision de l'annexe

supprimé

L'annexe fait l'objet d'une révision régulière s'il y a lieu, selon la procédure prévue à l'article 6, paragraphe 2.

Amendement 11
Article 6

Article 6
Comité

supprimé

- 1. La Commission est assistée par un comité composé de représentants des États membres et présidé par le représentant de la Commission.*
- 2. Dans le cas où il est fait référence au présent paragraphe, les articles 5 et 7 de la décision 199/468/CE s'appliquent, dans le respect des dispositions de l'article 8 de celle-ci.*
- 3. Le délai prévu à l'article 5, paragraphe 6, de la décision 1999/468/CE est fixé à trois mois.*

Amendement 12
ARTICLE 7

Les États membres veillent à ce que les catégories de données visées à l'article 4 soient conservées pour une durée d'un an à compter de la date de la communication, **à l'exception des données relatives à des communications électroniques utilisant uniquement ou principalement le protocole Internet. Ces dernières données sont conservées pour une durée de six mois.**

Les États membres veillent à ce que les catégories de données visées à l'article 4 soient conservées pour une durée d'un an à compter de la date de la communication. **Les États membres veillent à ce que toutes les données soient effacées à la fin de cette période de conservation.**

Justification

La période de conservation doit être suffisamment longue pour permettre aux autorités nationales de trouver des preuves et de poursuivre les infractions à la loi. La conduite

d'enquêtes sur d'éventuelles infractions liées à l'utilisation des communications électroniques peut prendre beaucoup de temps et certains cas peuvent intéresser des structures on line complexes. Il est par conséquent important que la proposition de la Commission donne aux États membres des procédures de mise en œuvre qui permettent aux instances chargées de veiller à l'application de la loi, des moyens souples et fiables d'assurer que les preuves critiques sont conservées le plus longtemps possible afin de préparer un dossier solide.

Amendement 13

Article 8

Les États membres veillent à ce que les données soient conservées conformément à la présente directive de manière ce que les données conservées et toute autre information nécessaire concernant ces données puissent, à leur demande, être transmises sans délai aux autorités compétentes.

Les États membres veillent à ce que les données soient conservées conformément à la présente directive de manière ce que les données conservées et toute autre information nécessaire concernant ces données puissent, à leur demande, être transmises sans délai aux autorités compétentes. ***Toute demande d'accès à des données entre États membres doit s'accompagner de la garantie que les données conservées en vertu de la présente directive ne seront transmises qu'à des services répressifs dûment autorisés et qu'elles ne seront pas transmises à des pays tiers.***

Amendement 14

Article 10

Les États membres ***veillent*** à ce que les fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications obtiennent le remboursement des surcoûts qu'ils justifient avoir supportés pour s'acquitter des obligations leur incombant en vertu de la présente directive.

Les États membres ***veillent*** à ce que les fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications obtiennent le ***plein*** remboursement des surcoûts ***d'investissement et de fonctionnement*** qu'ils justifient avoir supportés pour s'acquitter des obligations leur incombant en vertu de la présente directive, ***y compris les surcoûts générés par la protection des données et tout amendement futur à celle-ci. Le remboursement devrait comprendre les coûts justifiés générés par la mise à disposition des autorités nationales compétentes des données conservées.***

Justification

Amendement de compromis tel que proposé par LIBE. (??)

PROCÉDURE

| | |
|---|---|
| Titre | Proposition de directive du Parlement européen et du Conseil sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public et modifiant la directive 2005/58/CE |
| Références | (COM(2005)0438 – C6-0293/2005 – 2005/0182(COD)) |
| Commission compétente au fond | LIBE |
| Avis émis par Date de l'annonce en séance | IMCO 15.11.2005 |
| Coopération renforcée – date de l'annonce en séance | |
| Rapporteur pour avis Date de la nomination | Charlotte Cederschiöld 24.10.2005 |
| Rapporteur pour avis remplacé | |
| Examen en commission | 21.11.2005 |
| Date de l'adoption | 22.11.2005 |
| Résultat du vote final | +: 27 –: 5 0: 2 |
| Membres présents au moment du vote final | Mia De Vits, Janelly Fourtou, Evelyne Gebhardt, Malcolm Harbour, Christopher Heaton-Harris, Anna Hedh, Edit Herczog, Anneli Jäätteenmäki, Pierre Jonckheer, Henrik Dam Kristensen, Alexander Lambsdorff, Kurt Lechner, Lasse Lehtinen, Toine Manders, Arlene McCarthy, Manuel Medina Ortega, Bill Newton Dunn, Zita Pleštinská, Zuzana Roithová, Luisa Fernanda Rudi Ubeda, Heide Rühle, Leopold Józef Rutowicz, Andreas Schwab, Eva-Britt Svensson, József Szájer, Marianne Thyssen, Jacques Toubon, Bernadette Vergnaud, Phillip Whitehead, Joachim Wuermeling, |
| Suppléant(s) présent(s) au moment du vote final | Charlotte Cederschiöld, Joel Hasse Ferreira, Othmar Karas, Joseph Muscat, Alexander Stubb |
| Suppléant(s) (art. 178, par. 2) présent(s) au moment du vote final | |
| Observations (données disponibles dans une seule langue) | ... |

PROCÉDURE

| | | | | | |
|---|--|-----------|-----------------------|------------|------------|
| Titre | Proposition de directive du Parlement européen et du Conseil sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, et modifiant la directive 2002/58/CE | | | | |
| Références | COM(2005)0438 – C6-0293/2005 – 2005/0182(COD) | | | | |
| Base juridique | Articles 251, paragraphe 2, et 95 du traité CE | | | | |
| Base réglementaire | Article 51 | | | | |
| Date de la présentation au PE | 21.9.2005 | | | | |
| Commission compétente au fond Date de l'annonce en séance | LIBE 15.11.2005 | | | | |
| Commission(s) saisie(s) pour avis Date de l'annonce en séance | ITRE | IMCO | 15.11.2005 15.11.2005 | | |
| Avis non émis Date de la décision | | | | | |
| Coopération renforcée Date de l'annonce en séance | | | | | |
| Rapporteur(s) Date de la nomination | Alexander Nuno Alvaro 26.09.2005 | | | | |
| Rapporteur(s) remplacé(s) | | | | | |
| Procédure simplifiée – date de la décision | | | | | |
| Contestation de la base juridique Date de l'avis JURI | | | | | |
| Modification de la dotation financière Date de l'avis BUDG | | | | | |
| Consultation du Comité économique et social européen par le PE – date de la décision en séance | | | | | |
| Consultation du Comité des régions par le PE – date de la décision en séance | | | | | |
| Examen en commission | 5.9.2005 | 26.9.2005 | 5.10.2005 | 13.10.2005 | 24.10.2005 |
| Date de l'adoption | 14.11.2005 24.11.2005 | | | | |
| | 24.11.2005 | | | | |
| Résultat du vote final | + | 33 | | | |
| | - | 8 | | | |
| | 0 | 5 | | | |
| Membres présents au moment du vote final | Alexander Nuno Alvaro, Edit Bauer, Johannes Blokland, Mario Borghezio, Mihael Brejc, Kathalijne Maria Buitenweg, Maria Carlshamre, Michael Cashman, Giusto Catania, Charlotte Cederschiöld, Carlos Coelho, Agustín Díaz de Mera García Consuegra, Rosa Díez González, Patrick Gaubert, Elly de Groen-Kouwenhoven, Adeline Hazan, Timothy Kirkhope, Ewa Klamt, Magda Kósáné Kovács, Wolfgang Kreissl-Dörfler, Barbara Kudrycka, Stavros Lambrinidis, Sarah Ludford, Edith Mastenbroek, Martine Roure, Inger Segelström, Antonio Tajani, Ioannis Varvitsiotis, Manfred Weber, Stefano Zappalà, Tatjana Ždanoka | | | | |

| | |
|---|--|
| Suppléant(s) présent(s) au moment du vote final | Richard Corbett, Panayiotis Demetriou, Gérard Deprez, Lutz Goepel, Genowefa Grabowska, Jeanine Hennis-Plasschaert, Luis Herrero-Tejedor, Sylvia-Yvonne Kaufmann, Katalin Lévai, Bill Newton Dunn, Herbert Reul, Marie-Line Reynaud |
| Suppléant(s) (art. 178, par. 2) présent(s) au moment du vote final | Sharon Margaret Bowles, Daniel Caspary, Othmar Karas, Gabriele Zimmer |
| Date du dépôt | 28.11.2005 A6-0365/2005 |
| Observations (données disponibles dans une seule langue) | ... |