PARLEMENT EUROPÉEN

2004 *2009*

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

PROVISOIRE
2004/0813(CNS)

18.4.2005

*

PROJET DE RAPPORT

sur l'initiative de la République française, de l'Irlande, du Royaume de Suède et du Royaume-Uni en vue de l'adoption par le Conseil d'un projet de décision-cadre sur la rétention de données traitées et stockées en rapport avec la fourniture de services de communications électroniques accessibles au public ou de données transmises via des réseaux de communications publics, aux fins de la prévention, la recherche, la détection et la poursuite de délits et d'infractions pénales, y compris du terrorisme.
(8958/2004 – C6-0198/2004 – 2004/0813(CNS))

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

ESPOSÉ DES MOTIFS.....6

PROJET DE RÉSOLUTION LÉGISLATIVE DU PARLEMENT EUROPÉEN

sur l'initiative de la République française, de l'Irlande, du Royaume de Suède et du Royaume-Uni en vue de l'adoption par le Conseil d'un projet de décision-cadre sur la rétention de données traitées et stockées en rapport avec la fourniture de services de communications électroniques accessibles au public ou de données transmises via des réseaux de communications publics, aux fins de la prévention, la recherche, la détection et la poursuite de délits et d'infractions pénales, y compris du terrorisme.
(8958/2004 – C6-0198/2004 – 2004/0813(CNS))

(Procédure de consultation)

Le Parlement européen,

– vu l'initiative de la République française, de l'Irlande, du Royaume de Suède et du Royaume-Uni (8958/2004)[1],

– vu l'article 34, paragraphe 2, point b), du traité UE,

– vu l'article 39, paragraphe 1, du traité UE, conformément auquel il a été consulté par le Conseil (C6-0198/2004),

– vu l'avis de la commission des affaires juridiques sur la base juridique proposée,

– vu les articles 93, 51 et 35 de son règlement,

– vu le rapport de la commission des libertés civiles, de la justice et des affaires intérieures et l'avis de la commission de l'industrie, de la recherche et de l'énergie (A6-0000/2005),

1. rejette l'initiative de la République française, de l'Irlande, du Royaume de Suède et du Royaume-Uni;

2. invite la République française, l'Irlande, le Royaume de Suède et le Royaume-Uni à retirer leur initiative;

3. charge son Président de transmettre la position du Parlement au Conseil et à la Commission ainsi qu'aux gouvernements de la République française, de l'Irlande, du Royaume de Suède et du Royaume-Uni.

[1] Non encore publiée au JO.

ESPOSÉ DES MOTIFS

1. Objet de la proposition

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 commune[1] 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 terrorisme[2] 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.

Sont censées être enregistrées les données relatives au trafic et les données de localisation, y compris les données relatives à l'abonné et celles relatives à l'utilisateur, générées dans le cadre de la téléphonie, des services de messages courts et des protocoles Internet, y compris le courrier électronique. La teneur des communications n'est pas enregistrée. Il est normalement prévu, aux termes de la proposition, une durée de rétention d'au moins douze mois et de maximum trente-six mois. Pour les deuxième et troisième groupes, les États membres peuvent décider de déroger à la durée de rétention prévue. Les États membres doivent pouvoir, dans le cadre des commissions rogatoires, avoir accès aux données des autres États membres. La proposition ne comporte pas de règles d'indemnisation pour les frais occasionnés.

II. Évaluation de la proposition

Le rapporteur émet de grandes réserves quant à la base juridique choisie (1.) et la proportionnalité de la mesure (2.). En outre, il souligne la possibilité d'une violation de l'article 8 de la convention européenne des droits de l'homme (3.).

1. Base juridique

De l'avis du rapporteur, la base juridique choisie par le Conseil n'est pas conforme à la législation européenne. Il estime que la proposition s'articule plutôt autour de mesures qui relèvent du troisième et du premier piliers de l'Union.

Le Conseil se prévaut du pouvoir législatif exclusif que lui confère le titre VI du traité sur l'Union européenne (TUE) et invoque l'article 31, paragraphe 1, point c), et l'article 34, paragraphe 2, point b), du TUE.

Toutefois, le rapporteur estime que les mesures proposées concernent deux domaines distincts. D'une part, la proposition du Conseil vise à établir notamment l'obligation de conservation des données par les fournisseurs de services, la définition des données et leur durée de conservation, ce qui relève du droit communautaire. D'autre part, la proposition porte

[1] Document du Conseil 8958/04 du 28 avril 2004.
[2] Document du Conseil 7764/04 du 28 mars 2004.

notamment sur l'accès et l'échange des données stockées dans les États membres, ce qui constitue une action commune dans le domaine de la coopération judiciaire en matière pénale et relève donc du troisième pilier.

Les obligations des fournisseurs de services sont déjà régies par des dispositions communautaires. Les données visées par la proposition à l'examen sont couvertes par l'article 1 et l'article 2, point a), de la directive 95/46/CE du 24 octobre 1995. La directive porte sur les obligations générales des États membres en ce qui concerne la protection de la vie privée des personnes physiques à l'égard du traitement des données à caractère personnel. De plus, la directive 2002/58/CE du 12 juillet 2002 contient des dispositions spécifiques concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques. Le principe qui sous-tend ces deux directives est que les données stockées doivent être supprimées lorsque leur conservation n'est plus justifiée. L'article 15 de la directive 2002/58/CE permet aux États membres de conserver des données à titre exceptionnel, lorsqu'il s'agit d'une mesure nécessaire, appropriée et proportionnée pour lutter contre la criminalité. Les États membres n'étant pas parvenus à un accord sur un délai de conservation lors des négociations sur la directive relative à la protection des données dans le secteur des communications, aucune disposition n'a été prise en la matière.

Par conséquent, la base juridique choisie par le Conseil est contraire à l'article 47 du TUE qui dispose que le TUE ne doit pas affecter le traité instituant la Communauté européenne (traité CE). En vertu de cet article, aucune disposition du TUE ne peut affecter les dispositions du traité CE. En l'espèce, le non-respect du cadre juridique existant affecte le droit communautaire. Par conséquent, l'obligation faite aux fournisseurs de services de conserver les données, la définition des données ainsi que la durée de conservation relèvent du traité CE.

Les mesures proposées doivent logiquement reposer sur la même base juridique que le cadre juridique existant. L'article 95 du traité CE, qui prévoit la procédure de codécision, devrait donc également servir de base en l'espèce.

La commission des affaires juridiques du Parlement européen partage également cet avis. Le rapporteur a été informé que les services juridiques de la Commission européenne et du Conseil se ralliaient à cette interprétation juridique.

2. Proportionnalité de la mesure

De surcroît, le rapporteur doute de la proportionnalité des mesures individuelles. Les moyens mis en œuvre ne sont pas en rapport avec la finalité prévue, car les mesures ne sont ni appropriées ni nécessaires et frappent de manière excessive les intéressés.

Au regard du volume de données à retenir, notamment dans le domaine de l'Internet, on peut se demander si en définitive, une analyse ciblée des données est possible.

Il ne sera pas difficile pour les abonnés issus de la criminalité organisée et du terrorisme d'empêcher la traçabilité de leurs données. Pour ce faire, ils pourraient confier à des hommes de paille le soin d'acquérir des cartes de téléphone, utiliser à tour de rôle des téléphones portables de fournisseurs étrangers, passer leurs appels depuis des cabines publiques, changer l'adresse IP ou l'adresse du courrier électronique dont ils se servent quand ils ont recours à un

service dédié, voire utiliser directement les services de fournisseurs d'accès à Internet domiciliés hors d'Europe et qui ne sont donc pas concernés par une obligation de rétention des données.

Dans l'hypothèse où la totalité des données relatives au trafic, visées par la décision, doit vraiment faire l'objet d'une rétention, le volume de données en question représenterait, en l'état actuel du trafic, entre 20 et 40 000 téraoctets sur le réseau d'un grand fournisseur d'accès à Internet. Ce volume de données correspond à 4 millions de kilomètres linéaires de classeurs - soit dix montagnes de dossiers allant chacune de la terre à la lune. Face à ce gigantesque volume de données, le temps d'une seule recherche demanderait, en utilisant les techniques actuelles et sans investissements supplémentaires, entre 50 et 100 ans. On peut dès lors mettre en doute une disponibilité rapide des données demandées.

Une rétention au cas par cas pourrait être une option aussi pertinente et, au demeurant, plus douce que la proposition actuelle de rétention généralisée. C'est d'ailleurs la formule prescrite par la convention du Conseil de l'Europe sur la cybercriminalité[1].

À la lecture de la motivation retenue par le Conseil pour rejeter cette solution[2], on ne peut s'empêcher de s'interroger sur la compatibilité de la rétention des données proposées avec le principe de présomption d'innocence.

La proposition à l'examen met de côté les contraintes susceptibles de peser sur les intéressés. Outre les graves atteintes à la protection des données individuelles à caractère personnel, l'industrie européenne des télécommunications, notamment les petites et moyennes entreprises de télécommunication, doit s'attendre à être confrontée à des charges énormes.

Dans ce contexte, les charges en question sont notamment imputables:
- à la mise à niveau de la technologie système pour générer et conserver les données,
- à l'adaptation des cycles d'exploitation à l'archivage sécurisé des données et
- au traitement et à l'analyse des demandes adressées par les services de sécurité.

Le montant des investissements annuels nécessaires à cet effet dans le domaine de la téléphonie filaire traditionnelle s'élève, au sein des États membres et selon les estimations de sociétés très diverses et relativement importantes quant à leur taille, à 180 millions d'euros par entreprise, les coûts annuels d'exploitation pouvant atteindre les 50 millions d'euros. L'avenir commercial des petites et moyennes entreprises serait certainement hypothéqué. D'après certaines estimations, les charges dans le domaine de l'Internet seraient plusieurs fois supérieures au montant des investissements nécessaires en matière de téléphonie filaire traditionnelle. Le comité de l'article 36 propose en conséquence de continuer à n'enregistrer que les données déjà pertinentes[3].

La proposition du Conseil ne prévoit pas de réglementation harmonisée ventilant sur le plan

[1] STE n° 185, 8 novembre 2001; la convention n'a pas encore été transposée dans tous les États membres.
[2] Document du Conseil 8958/04 ADD 1. L'exposé des motifs de la décision-cadre sur la rétention des données se borne à constater que la rétention au cas par cas «ne présentera jamais aucune utilité dans une enquête au sujet d'une personne qui n'est pas encore soupçonnée de participation à une organisation criminelle ou terroriste. [...] Par conséquent, [elle] ne suffit pas à satisfaire les besoins des services de sécurité, des services de renseignement et des services répressifs dans la lutte contre la criminalité moderne, y compris le terrorisme».
[3] 15098/04 du 23 novembre 2004.

européen les coûts générés par le dispositif. Il en résulte des distorsions de concurrence qui menacent à long terme des structures compétitives viables et, partant, font obstacle à l'accomplissement d'un marché unique intérieur européen.

3. Compatibilité avec l'article 8 de la convention européenne des droits de l'homme
De l'avis du rapporteur, l'article 8 de la convention européenne des droits de l'homme n'est pas respecté.

Il y a lieu de rejeter un contrôle et une rétention des données, dès lors que ces mesures ne répondent pas à trois critères fondamentaux conformément à l'article 8, paragraphe 2, de la convention européenne et à l'interprétation par la Cour européenne des droits de l'homme de cette disposition: une base légale, la nécessité de la mesure dans une société démocratique et la conformité à l'un des buts légitimes énumérés dans la convention[1]. Sur la base de l'examen effectué en l'espèce, le respect de tous les critères nécessaires apparaît pour le moins douteux dans le cas du présent document du Conseil[2].

III. Conclusion

Partant, le rapporteur rejette la proposition de décision-cadre et invite les États membres à retirer leur initiative.

Le rapporteur invite les États membres à présenter une étude prouvant de manière incontestable la nécessité de la rétention de données prévue. De plus, il propose de traiter les questions de l'obligation de rétention des données, de la définition des données à stocker et de la durée de rétention dans une directive distincte. Il invite la Commission à élaborer une proposition en ce sens. Le rapporteur indique que les objectifs de la proposition à l'examen pourraient déjà être atteints au travers de la mise en œuvre de la convention du Conseil de l'Europe sur la cybercriminalité et d'une amélioration de la coopération transfrontalière dans le domaine concerné. Par conséquent, avant de pouvoir décider de nouvelles mesures, les résultats de l'étude susmentionnée doivent obligatoirement être pris en compte. Si, contre toute attente, la proposition du Conseil recueillait la majorité des voix, le texte devra prévoir un examen des mesures après trois ans sur la base d'une évaluation, afin de déterminer l'efficacité réelle de ces mesures et de justifier ainsi la rétention des données.

[1] Groupe de travail "Article 29" sur la protection des données, 11885/04 du 9 novembre 2004.
[2] La Cour européenne des droits de l'homme a rappelé que les États contractants ne disposent pas pour autant d'une latitude illimitée pour assujettir à des mesures de surveillance secrète les personnes soumises à leur juridiction. Consciente du danger, inhérent à pareille loi, de saper, voire de détruire, la démocratie au motif de la défendre, elle affirme qu'ils ne sauraient prendre, au nom de la lutte contre l'espionnage et le terrorisme, n'importe quelles mesures jugées par eux appropriées.