

Procédure file

Informations de base		
CNS - Procédure de consultation Acte JAI	2004/0813(CNS)	Procédure caduque ou retirée
Lutte contre la criminalité: prévention des délits des infractions pénales et du terrorisme, rétention de données traitées ou transmises via des réseaux de communications publics. Décision-cadre. Initiative France, Irlande, Suède et Royaume-Uni		
Sujet 7.30.20 Lutte contre le terrorisme 7.40.04 Coopération judiciaire en matière pénale		

Acteurs principaux			
Parlement européen	Commission au fond	Rapporteur(e)	Date de nomination
	LIBE Libertés civiles, justice et affaires intérieures	ALDE PICKART ALVARO Alexander Nuno	25/11/2004
	Commission pour avis	Rapporteur(e) pour avis	Date de nomination
	ITRE Industrie, recherche et énergie	La commission a décidé de ne pas donner d'avis.	
	Commission pour avis sur la base juridique	Rapporteur(e) pour avis	Date de nomination
	JURI Affaires juridiques	PSE MEDINA ORTEGA Manuel	21/09/2004
Conseil de l'Union européenne	Formation du Conseil	Réunion	Date
	Justice et affaires intérieures(JAI)	2683	12/10/2005
	Justice et affaires intérieures(JAI)	2664	02/06/2005
	Justice et affaires intérieures(JAI)	2626	02/12/2004
Commission européenne	DG de la Commission	Commissaire	
	Justice et consommateurs	FRATTINI Franco	

Evénements clés			
28/04/2004	Publication de la proposition législative	08958/2004	Résumé
01/12/2004	Annonce en plénière de la saisine de la commission		
02/12/2004	Débat au Conseil	2626	Résumé

26/05/2005	Vote en commission		Résumé
01/06/2005	Dépôt du rapport de la commission, 1ère lecture/lecture unique	A6-0174/2005	
02/06/2005	Débat au Conseil	2664	Résumé
07/06/2005	Débat en plénière		Résumé
07/06/2005	Décision du Parlement		
27/09/2005	Décision du Parlement	T6-0348/2005	Résumé
12/10/2005	Débat au Conseil	2683	Résumé

Informations techniques

Référence de procédure	2004/0813(CNS)
Type de procédure	CNS - Procédure de consultation
Sous-type de procédure	Législation
Instrument législatif	Acte JAI
Base juridique	Traité sur l'Union européenne (après Amsterdam) M 038; Traité sur l'Union européenne (après Amsterdam) M 034-p2; Traité sur l'Union européenne (après Amsterdam) M 031-p1-aa
Etape de la procédure	Procédure caduque ou retirée
Dossier de la commission parlementaire	LIBE/6/25028

Portail de documentation

Document de base législatif		08958/2004	28/04/2004	CSL	Résumé
Avis de la commission	JURI	PE355.785	08/04/2005	EP	
Rapport déposé de la commission, 1ère lecture/lecture unique		A6-0174/2005	01/06/2005	EP	
Texte adopté du Parlement, 1ère lecture/lecture unique		T6-0348/2005 JO C 220 21.09.2006, p. 0018-0045 E	27/09/2005	EP	Résumé

Informations complémentaires

Commission européenne	EUR-Lex
-----------------------	-------------------------

Lutte contre la criminalité: prévention des délits des infractions pénales et du terrorisme, rétention de données traitées ou transmises via des réseaux de communications publics. Décision-cadre. Initiative France, Irlande, Suède et Royaume-Uni

OBJECTIF : prévoir un mécanisme de rétention des données stockées par les fournisseurs de communications accessibles au public en vue de prévenir les infractions pénales, y compris le terrorisme.

ACTE PROPOSÉ : Décision-cadre (initiative des gouvernements français, irlandais, suédois et britannique).

CONTENU : Afin d'offrir un niveau élevé de protection dans un Espace européen de liberté, de sécurité et de justice, il est apparu important pour les services répressifs des États membres, d'enquêter sur des actes criminels à partir de données utilisées par les systèmes de communications. Dans ses conclusions du 19 décembre 2002, le Conseil avait indiqué qu'avec l'accroissement des possibilités offertes par les communications électroniques, les données relatives à leur utilisation constituaient un instrument utile pour la prévention et la détection des infractions pénales liées à la criminalité organisée et au terrorisme. Parallèlement, le 25 mars 2004, le Conseil européen a appelé de ses vœux l'établissement, d'ici juin 2005, de règles relatives à la rétention des données générées par les fournisseurs de services, conscient que les télécommunications modernes ouvraient de nouvelles voies à la criminalité internationale et au terrorisme, en particulier.

En réponse à la demande du Conseil et pour contrer les disparités juridiques existant entre les États membres, il est proposé, à l'initiative de 4 États membres (France, Irlande, Royaume-Uni et Suède) de prévoir un mécanisme efficace et harmonisé de rétention "a priori" d'une liste de données stockées et générées par les fournisseurs de services de communications accessibles au public. Ces données seraient retenues dans le respect des prescriptions internationales applicables à la protection des données et de manière proportionnée par rapport l'objectif poursuivi qui est la protection des citoyens dans une société démocratique.

CHAMP D'APPLICATION : le projet de décision-cadre ne porte que sur les données générées par une communication et non sur le contenu proprement dit des informations communiquées. Il ne s'agit donc pas d'accéder à des données obtenues par la surveillance, l'interception ou l'enregistrement de télécommunications. L'objectif est d'utiliser certains types de données recueillies "a priori" afin de remonter à la source des contenus illégaux, tels que des matériaux à caractère pédophile, raciste et xénophobe, ainsi qu'à l'origine des attaques informatiques, et d'identifier ainsi les individus utilisant des réseaux de communications électroniques pour mener à bien des activités illicites relevant de la criminalité organisée et du terrorisme. Il ne s'agit pas non plus de fixer des règles pour la rétention de données dans le contexte de la sécurité nationale ou de la sûreté de l'État.

Le projet de décision-cadre entend faciliter la coopération judiciaire pénale par le rapprochement des législations en matière de rétention de données et fixer une liste de données à retenir en vue d'une utilisation ultérieure.

LISTE DE DONNÉES À RETENIR : le projet de décision-cadre délimite le type de données à retenir : il s'agit de données nécessaires pour :

.retrouver et identifier la source d'une communication, y compris des informations à caractère personnel, des informations sur les contacts et des informations permettant d'identifier les services pour lesquels un abonnement a été souscrit (ex.: données traitées et stockées à des fins de facturation, à des fins commerciales ou à toute autre fin légitime);

.déterminer l'acheminement et la destination d'une communication;

.déterminer l'heure, la date et la durée d'une communication;

.identifier la télécommunication, le dispositif de communication ou encore localiser la communication,...

à partir des modes de communications suivants :

- téléphonie classique et GSM;

- SMS, services de médias électroniques (EMS) et MMS;

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

Il est également prévu d'inclure tout autre développement technologique futur destiné à faciliter la transmission de données relevant du champ d'application de la décision-cadre.

DURÉE DE LA RÉTENTION DES DONNÉES : ces données seraient retenues pendant une période allant de 12 à 36 mois après leur création. Des périodes plus longues pourraient être prévues d'un commun accord entre États membres à condition que cette durée soit légitime et proportionnée par rapport à l'objectif poursuivi. La durée de la période de rétention serait fonction de l'utilité des données pour la prévention et la détection des infractions mais aussi du coût de la rétention.

PRINCIPE DE COOPÉRATION : le projet de décision-cadre prévoit expressément l'accès mutuel aux données retenues dans le cadre de la coopération judiciaire en matière pénale telle que visée au titre VI du traité sur l'Union européenne et en accord avec les procédures applicables à la coopération judiciaire en matière pénale. Toute transmission de données pourra toutefois être subordonnée à un certain nombre de conditions édictées par l'État membre qui émet l'information.

PROTECTION ET SÉCURITÉ DES DONNÉES: le principe de rétention des données devra respecter un certain nombre de principes de protection des données énoncés par le projet de décision-cadre mais aussi par la directive 95/46/CE sur la protection des données (notamment, voies de recours juridiques, responsabilité et sanctions en cas de non-respect).

De même, des dispositions sont prévues afin que la rétention des données s'effectue dans le respect de principes minimaux de sécurité tels que la protection contre la destruction accidentelle ou illicite de données, la perte, l'altération, la diffusion ou l'accès non autorisés, ainsi que contre toute autre forme de traitement illicite, etc.

À noter enfin que des dérogations sont prévues aux principaux articles du projet de décision-cadre (rapprochement des législations applicables à la rétention des données, durée de rétention, etc.). Dans ce cas, les États concernés devraient en avvertir le Conseil et la Commission.

Lutte contre la criminalité: prévention des délits des infractions pénales et du terrorisme, rétention de données traitées ou transmises via des réseaux de communications publics. Décision-cadre. Initiative France, Irlande, Suède et Royaume-Uni

Le Conseil a examiné le champ d'application du projet de décision-cadre sur la rétention de données. La proposition part du principe où les fournisseurs de services de communications électroniques accessibles au public retiennent un certain type de données permettant d'établir la source, l'acheminement, la destination, l'heure, la date et la durée de communications, ainsi que pour localiser les dispositifs de télécommunication utilisés.

Dans sa forme initiale, cette proposition se limitait aux données déjà traitées et stockées à des fins de facturation, à des fins commerciales ou toute autre fin légitime. Toutefois, cette approche sous-entend que les possibilités d'accès aux données à des fins de répression dépendent de la manière dont chaque fournisseur de services fonctionne sur les plans technique et commercial. Certains fournisseurs de services appliquent, par exemple, des systèmes forfaitaires. En conséquence, des données pertinentes, qui sont traitées afin de fournir la télécommunication concernée, sont effacées dès que celle-ci a cessé.

Le Conseil a donc chargé ses instances préparatoires d'examiner une autre approche qui suppose l'obligation pour les fournisseurs de services de retenir les données pertinentes définies dans une liste commune figurant dans le dispositif, à condition que les données soient traitées/générées par le fournisseur de services dans le cadre de la fourniture du service de télécommunications concerné.

Une attention particulière devrait être accordée à la proportionnalité de la mesure en matière de coûts, de protection de la vie privée (protection des données) et d'efficacité.

Pour le Conseil, l'approche pourrait conduire à un plus haut degré de garantie quant à la rétention des données concernées et serait moins exposée au comportement commercial du fournisseur de services et aux évolutions techniques. Le fournisseur de services serait tenu de retenir les données même si, a priori elles ne revêtent pas d'intérêt pour ce dernier. Le niveau d'harmonisation de la législation des États membres serait relativement élevé.

Cette proposition a été élaborée à la lumière de la déclaration sur la lutte contre le terrorisme qui a été adoptée par le Conseil européen lors de sa réunion du 25 mars 2004. Cette déclaration prévoyait qu'un instrument sur la rétention des données devait être adopté pour juin 2005.

Lutte contre la criminalité: prévention des délits des infractions pénales et du terrorisme, rétention de données traitées ou transmises via des réseaux de communications publics. Décision-cadre. Initiative France, Irlande, Suède et Royaume-Uni

La commission a adopté le rapport de M. Alexander Nuno ALVARO (ADLE, DE) qui rejette la proposition en procédure de consultation. La commission émet de grandes réserves quant à la base juridique choisie et la proportionnalité de la mesure. En outre, elle souligne la possibilité d'une violation de l'article 8 de la Convention européenne des droits de l'homme.

Lutte contre la criminalité: prévention des délits des infractions pénales et du terrorisme, rétention de données traitées ou transmises via des réseaux de communications publics. Décision-cadre. Initiative France, Irlande, Suède et Royaume-Uni

Le Conseil a eu un échange de vues sur certaines questions clés dans l'optique d'une mise au point rapide du projet de décision-cadre, notamment la liste des données à retenir, la durée de la période de rétention, et la base juridique de l'acte.

Suite au débat, la Présidence luxembourgeoise a conclu qu'un accord pourrait se dégager parmi les délégations sur une ligne de conduite et certains éléments clés de la décision-cadre:

- la rétention de données est un élément important dans la lutte contre le crime et le terrorisme et il est nécessaire d'avoir un acte législatif au sein de l'UE;
- afin d'aboutir à un accord rapide sur cette décision-cadre, une approche progressive dans le traitement du dossier serait préférable, en commençant par la rétention des données de communication de téléphonie fixe et mobile;
- en ce qui concerne la rétention de données d'Internet et s'agissant de la téléphonie, des appels sortant n'ayant pas abouti, les États membres qui ne sont pas en mesure de collecter les données immédiatement pourraient bénéficier d'une période transitoire d'application de la décision-cadre, limitée dans le temps, dont la durée resterait à déterminer ;
- les fournisseurs des services de communications et les services d'enquête judiciaire seraient consultés afin d'examiner, entre autres, les coûts liés à la mise en œuvre de cette décision-cadre.

En ce qui concerne la liste des données de communication qui doivent être retenues, d'une manière générale, les délégations ont été en mesure d'accepter l'approche de la Présidence, laquelle prévoit une liste minimum de données à retenir. Cette liste devrait avoir une finalité essentiellement fonctionnelle, tout en étant assortie de certaines spécifications techniques pour différents types de télécommunications.

La plupart des délégations seraient en mesure d'accepter la durée des périodes prévues dans le texte de compromis de la Présidence: la durée normale de la période de rétention des données serait de 12 mois. Les États membres seraient autorisés à prévoir une période plus courte dans des circonstances exceptionnelles, qui ne pourrait toutefois pas être inférieure à 6 mois.

Pour ce qui est de la base juridique, la majorité des délégations ont estimé que le Titre VI du TUE (article 31, par. 1, point c), et article 34, par 2, point b)) devrait être la base juridique de la proposition. Ce point sera traité à nouveau lors de la réunion informelle des ministres de la Justice et de l'Intérieur qui aura lieu en septembre sous Présidence britannique.

Lutte contre la criminalité: prévention des délits des infractions pénales et du terrorisme, rétention de données traitées ou transmises via des réseaux de communications publics. Décision-cadre. Initiative France, Irlande, Suède et Royaume-Uni

Conformément à la position de sa commission au fond, le Parlement a rejeté le projet de décision-cadre présenté sur initiative française, irlandaise, suédoise et britannique sur la rétention des données transmises via des réseaux de communications publics.

Pour rappel, cette initiative portait sur la conservation des données traitées par les fournisseurs de téléphone et d'Internet aux fins de la prévention, de la recherche et de la poursuite des actes terroristes et visait à faciliter la coopération judiciaire en matière pénale en modifiant

la législation des États membres sur la conservation des données traitées par les fournisseurs de service public.

Sur la base d'un rapport rédigé par Alexandre Nuno ALVARO (ADLE, DE), le Parlement a rejeté en Plénière la proposition en raison des incertitudes qui régnaient autour du choix de la base juridique et de la proportionnalité des mesures. Le rapport exigeait notamment que les États membres mandatent une étude pour prouver la nécessité de dispositions sur la conservation de données et suggérait de vérifier si les objectifs de la décision-cadre ne pouvaient pas être réalisés par la mise en oeuvre de la convention du Conseil de l'Europe sur le Cybercrime.

Pendant le débat, le Commissaire à la JAI, M. FRATTINI a annoncé que la Commission entendait proposer un nouveau texte avec une base juridique différente d'ici l'été. Le ministre SCHMIT ayant déclaré que le Conseil maintenait son texte, ce dernier a été renvoyé en commission des Libertés civiles.

Lutte contre la criminalité: prévention des délits des infractions pénales et du terrorisme, rétention de données traitées ou transmises via des réseaux de communications publics. Décision-cadre. Initiative France, Irlande, Suède et Royaume-Uni

Le Parlement a définitivement rejeté le projet de décision-cadre sur la rétention des données, confirmant ainsi sa position exprimée le 7 juin 2005 (se reporter au résumé du débat en Plénière du 7 juin 2005) avant le renvoi du rapport ALVARO (ALDE, DE) en commission des libertés publiques.

Par le vote du 27 septembre 2005, le Parlement confirme le rejet de cette initiative. La procédure est de ce fait, close. À compter de cette date les députés se pencheront sur un nouveau projet de directive de la Commission portant sur le même sujet qui impliquera le Parlement en codécision, cadre qui lui sera beaucoup plus favorable (se reporter à la fiche de procédure COD/2005/0182)

La proposition de décision-cadre soutenue par la Présidence britannique de l'Union était devenue l'une des priorités depuis les attentats de Londres. Le vote des députés n'ayant pas dans le cas présent, force de loi, deux projets parallèles sont désormais en route et la Présidence pourrait à nouveau peser en faveur de la proposition des 4 États membres dans les semaines qui viennent.

Lutte contre la criminalité: prévention des délits des infractions pénales et du terrorisme, rétention de données traitées ou transmises via des réseaux de communications publics. Décision-cadre. Initiative France, Irlande, Suède et Royaume-Uni

Le Conseil a eu un échange de vues sur la base d'un document de la présidence britannique : un grand nombre de délégations pouvaient accepter les éléments figurant dans le document de la présidence comme base pour la suite des travaux, pour autant que la dérogation prévue à l'article 15, par 1 de la directive "télécommunications" de 2002 soit maintenue et que son futur champ d'application soit clarifié.

Au cours de la prochaine étape, la décision-cadre, qui est une option à laquelle un grand nombre de délégations sont favorables, restera sur la table. Toutefois, une majorité des délégations n'écartaient pas non plus l'idée d'adopter une directive.

Un large accord existait pour considérer que toute mesure devait tenir compte des éléments figurant dans le document de la présidence, notamment en ce qui concerne les dispositions relatives aux durées de conservation, au champ d'application et aux coûts.

Le Conseil a été d'accord pour estimer que les travaux devraient se poursuivre d'urgence. Il a chargé le COREPER de dégager dans les meilleurs délais un accord définitif sur toutes les questions en suspens et est convenu qu'il y avait lieu de poursuivre les contacts informels avec le Parlement européen (qui a rejeté cette proposition) afin de parvenir à un terrain d'entente aussi large que possible avec cette institution sur les questions de fond, tout en respectant la position du Conseil telle qu'elle est exposée ci-dessus.

Le Conseil est convenu de revenir sur cette question lors de sa prochaine session en vue d'arrêter une décision définitive d'ici à la fin de l'année.

À noter que cette proposition de décision-cadre, fondée sur les articles 31 et 34 du traité sur l'Union européenne, a été faite sur initiative de la France, de l'Irlande, de la Suède et du Royaume-uni en avril 2004, dans le cadre du "troisième pilier". Une telle proposition requiert l'unanimité au niveau du Conseil pour pouvoir être adoptée. Toutefois, la Commission a estimé que les catégories de données à conserver et la durée de leur conservation relevaient de la compétence de la CE ("premier pilier") et que les dispositions y relatives devaient être adoptées par le Conseil et le Parlement européen suivant la procédure de codécision, sur la base d'une proposition de directive de la Commission. En conséquence, le 21 septembre 2005, la Commission a adopté une proposition de directive concernant la conservation des données relatives au trafic des communications qui fait maintenant l'objet d'un avis devant le PE (voir COD/2005/0182).