Procedure file

Informations de base

COD - Procédure législative ordinaire (ex-procedure codécision) Directive	2005/0182(COD)	Procédure terminée
Communications électroniques: données personnelles, protection de la vie privée et accès aux données relatives au trafic à des fins antiterroristes Modification Directive 2002/58/EC 2000/0189(COD) Sujet 1.20.09 Protection de la vie privée et des données 3.30.05 Communications électroniques et mobiles, services cryptés 7.30.20 Lutte contre le terrorisme		

Acteurs principaux

Parlement européen	Commission au fond	Rapporteur(e)	Date de nomination
	LIBE Libertés civiles, justice et affaires intérieures	ALDE PICKART ALVARO Alexander Nuno	26/09/2005
	Commission pour avis	Rapporteur(e) pour avis	Date de nomination
	ITRE Industrie, recherche et énergie	PPE-DE NIEBLER Angelika	05/10/2005
	IMCO Marché intérieur et protection des consommateurs	PPE-DE CEDERSCHIÖLD Charlotte	24/10/2005
Conseil de l'Union européenne	Formation du Conseil	Réunion	Date
	Justice et affaires intérieures(JAI)	2709	21/02/2006
	Justice et affaires intérieures(JAI)	2696	01/12/2005
Commission européenne	DG de la Commission	Commissaire	
	Justice et consommateurs		

Evénements clés

21/09/2005	Publication de la proposition législative	COM(2005)0438	Résumé
15/11/2005	Annonce en plénière de la saisine de la commission, 1ère lecture		
24/11/2005	Vote en commission,1ère lecture		Résumé
28/11/2005	Dépôt du rapport de la commission, 1ère lecture	A6-0365/2005	

01/12/2005	Débat au Conseil	2696	Résumé
13/12/2005	Débat en plénière		
14/12/2005	Résultat du vote au parlement		
14/12/2005	Décision du Parlement, 1ère lecture	T6-0512/2005	Résumé
21/02/2006	Adoption de l'acte par le Conseil après la 1ère lecture du Parlement		Résumé
15/03/2006	Signature de l'acte final		
15/03/2006	Fin de la procédure au Parlement		
13/04/2006	Publication de l'acte final au Journal officiel		

Informations techniques

Référence de procédure	2005/0182(COD)
Type de procédure	COD - Procédure législative ordinaire (ex-procedure codécision)
Sous-type de procédure	Législation
Instrument législatif	Directive
	Modification Directive 2002/58/EC 2000/0189(COD)
Base juridique	Traité CE (après Amsterdam) EC 095
Etape de la procédure	Procédure terminée
Dossier de la commission parlementaire	LIBE/6/30671

Portail de documentation

Document de base législatif		COM(2005)0438	21/09/2005	EC	Résumé
Document annexé à la procédure		SEC(2005)1131	21/09/2005	EC	
Pour information		N6-0029/2005 JO C 298 29.11.2005, p. 0001-0012	26/09/2005	OS	
Amendements déposés en commission		PE364.849	27/10/2005	EP	
Amendements déposés en commission		PE364.972	17/11/2005	EP	
Avis de la commission	ITRE	PE364.724	23/11/2005	EP	
Rapport déposé de la commission, 1ère lecture/lecture unique		A6-0365/2005	28/11/2005	EP	
Texte adopté du Parlement, 1ère lecture/lecture unique		T6-0512/2005	14/12/2005	EP	Résumé
Réaction de la Commission sur le texte adopté en plénière		SP(2006)0053	12/01/2006	EC	
Comité économique et social: avis, rapport		CES0035/2006 JO C 069 21.03.2006, p. 0016-0021	19/01/2006	ESC	
Projet d'acte final		03677/12/2005	15/03/2006	CSL	
Document de suivi		COM(2011)0225	18/04/2011	EC	Résumé

Document annexé à la procédure		N7-0088/2011 JO C 279 23.09.2011, p. 0001	31/05/2011	EDPS	Résumé

Informations complémentaires

Commission européenne	EUR-Lex

Acte final

Directive 2006/24
JO L 105 13.04.2006, p. 0054-0063 Résumé

Communications électroniques: données personnelles, protection de la vie privée et accès aux données relatives au trafic à des fins antiterroristes

OBJECTIF : 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.

ACTE PROPOSÉ : Directive du Parlement européen et du Conseil.

CONTEXTE : dans sa déclaration du 25 mars 2004 sur la lutte contre le terrorisme, le Conseil européen a confirmé la nécessité de prévoir des règles au niveau de l?Union garantissant l?accès aux données relatives au trafic à des fins antiterroristes dans les 25 États membres. À la suite des attentats de Madrid, le Conseil européen a chargé le Conseil d?envisager des « propositions en vue de l?établissement de règles relatives à la conservation, par les fournisseurs de services, des données relatives au trafic des communications» dans la perspective de leur adoption en 2005. Enfin après les attentats de Londres, le Conseil européen a réaffirmé qu'il était prioritaire d'adopter un instrument législatif adapté dans ce domaine.

Plusieurs États membres ont arrêté, ou envisagent d?arrêter, des dispositions nationales obligeant certains opérateurs ou l?ensemble de ceux-ci à conserver tel ou tel type de données de sorte qu?elles puissent être utilisées si nécessaire pour les finalités décrites ci-dessus. Afin d?éviter toute disparité sur le plan des dispositions législatives, réglementaires et techniques dans les États membres, il est nécessaire de poursuivre l?harmonisation de ces dispositions au niveau de l?Union européenne.

CONTENU : la directive proposée 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.

En application de la directive, les États membres devraient veiller à ce que soient conservées les données nécessaires pour :

- retrouver et identifier la source d?une communication;
- retrouver et identifier la destination d?une communication;
- déterminer la date, l?heure et la durée d?une communication; déterminer le type de communication;
- déterminer le dispositif de communication utilisé ou ce qui est censé avoir été utilisé comme dispositif de communication;
- localiser le matériel de communication mobile.

S?appuyant sur une analyse d?impact, la proposition adopte une approche équilibrée, à savoir des durées de conservation d?un an pour les données relatives au trafic concernant la téléphonie mobile et la téléphonie fixe, et de six mois pour les données relatives au trafic concernant l?utilisation d?Internet. Les données conservées ainsi que toute autre information nécessaire concernant ces données devront pouvoir, à leur demande, être transmises sans délai aux autorités compétentes.

À noter que la présente proposition porte sur la même thématique que le projet de décision-cadre portant sur la rétention des données (initiative des gouvernements français, irlandais, suédois et britannique) proposé en 2004 (se reporter à la fiche de procédure CNS/2004/0813) et rejetée par le Parlement européen.

Communications électroniques: données personnelles, protection de la vie privée et accès aux données relatives au trafic à des fins antiterroristes

La commission a adopté le rapport de Alexander Nuno ALVARO (ADLE, DE) modifiant la proposition en première lecture de la procédure de codécision:

- l?article 1 (objectif de la directive) est modifié de sorte à ce que puissent être conservées à des fins de recherche, de détection et de poursuite, mais pas de «prévention», de formes d'infractions graves, au motif qu?il s?agit d?un concept vague rendant les données conservées plus vulnérables aux abus. En outre, alors que la proposition donne simplement des exemples d?infractions graves («comme le terrorisme et la criminalité organisée»), la commission préfère renvoyer à la définition visée à l?article 2, paragraphe 2, du mandat d?arrêt européen;

- de nouvelles dispositions à l?article 1 précisent qu?un des objectifs de la directive doit être d'assurer que soient pleinement respectés les droits au respect de la vie privée et à la protection des données à caractère personnel lorsque ces données sont conservées. La présente directive s?applique uniquement aux données relatives au trafic et aux données de localisation, ainsi qu?aux données nécessaires pour identifier l'abonné ou l'utilisateur enregistré. Elle ne s?applique pas aux données «connexes»;

- les données conservées conformément à la présente directive ne sont transmises qu?aux autorités nationales compétentes à des fins de recherche, de détection et de poursuite des infractions pénales graves «après approbation des autorités judiciaires et des autres autorités compétentes conformément à la législation nationale»;

- deux nouveaux articles introduisent des dispositions régissant l?accès aux données conservées, à la protection des données et à la sécurité des données. Ces dispositions veillent notamment à garantir que l?accès aux données conservées ne soit autorisé qu?à des fins spécifiques, au cas par cas, et soit limité aux données nécessaires «pertinentes et proportionnées» dans le contexte d'une enquête spécifique. Il 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. Les données sont effacées dès qu'elles ne sont plus nécessaires et lorsqu?elles sont inexactes. Tout accès aux données est enregistré. Enfin, les autorités nationales ne peuvent transmettre ces données à des pays tiers (tels que les États-Unis) 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;

- un autre nouvel article prévoit que les États membres imposent des sanctions effectives, proportionnées et dissuasives pour infractions aux dispositions nationales adoptées en vue de la mise en ?uvre de la présente directive;

- Les députés européens veulent que toutes les données (c?est-à-dire la téléphonie et l?internet) soit conservées pour une période de 6 à 12 mois puis effacées, alors que la proposition prévoit simplement que les données pour la téléphonie soient conservées un an et pour l?internet 6 mois;

- la commission restructure la proposition de manière à placer l?annexe (liste des catégories de données à conserver) dans le corps principal du texte (à l?article 4);

- tout en soutenant l?enregistrement des données de localisation pour les conversations téléphoniques, les sms et les protocoles internet, les députés européens préfèrent laisser aux États membres la possibilité d'imposer aux entreprises de télécommunications une rétention des appels infructueux. Ils introduisent une nouvelle définition - «tentatives infructueuses de communication» - dans la directive;

- les entreprises de télécommunications obtiennent le remboursement des surcoûts qu?ils justifient avoir supportés pour s?acquitter des obligations leur incombant en vertu de la présente directive, y compris les investissement et les frais de fonctionnement, ainsi que des surcoûts de toute future modification de ladirective, alors que la proposition ne prévoit que le remboursement inclut les coûts «prouvés»;

- enfin, la directive est révisée après 2 ans, et tous les 3 ans par la suite, en accordant une attention particulière sur les types de données conservées et les périodes de rétention.

Communications électroniques: données personnelles, protection de la vie privée et accès aux données relatives au trafic à des fins antiterroristes

Le Conseil est convenu de parvenir d'ici la fin de l'année à un accord en première lecture avec le Parlement européen sur le projet de directive portant sur la conservation des données, sur base d'un texte de compromis approuvé ce 1er décembre 2005. M. FRATTINI, vice-président de la Commission, a annoncé qu'il pouvait appuyer l'approche retenue et le texte approuvé par le Conseil. L'Irlande, la Slovaquie et la Slovénie ont, en revanche, émis des réserves.

Les éléments sur lesquels un accord a pu être dégagé sont les suivants:

- infractions pénales graves : le texte de la proposition de directive mentionne des infractions pénales graves, telles que définies par chaque État membre dans leur droit interne. Les États membres devront tenir dûment compte des infractions énumérées à l'article 2, par. 2, de la décision-cadre relative au mandat d'arrêt européen (2002/584/JAI) ainsi que des infractions ayant pour objet les télécommunications ;
- durée de conservation : les États membres devraient veiller à ce que les catégories de données visées dans le projet de directive soient conservées pour une durée de 6 mois minimum et de 2 ans maximum à compter de la date de la communication ;
- données Internet : le Conseil se dit favorable à une obligation de conservation des données sur l'accès à Internet, le courrier électronique par Internet et la téléphonie par Internet ;
- appels infructueux : le Conseil souhaiterait inclure la conservation des données relatives aux appels infructueux lorsque ces données sont générées ou traitées et stockées (en ce qui concerne les données de la téléphonie) ou journalisées (en ce qui concerne les données Internet) par des fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications dans le cadre de la fourniture des services de communication concernés, lorsque ces fournisseurs relèvent de leur compétence. La directive n'impose pas la conservation des données relatives aux appels non connectés ;
- souplesse : l'article 15, par. 1, de la directive 2002/58/CE continuerait à s'appliquer aux données qu'il n'y a pas spécifiquement lieu de conserver en vertu de la directive, y compris les données relatives aux appels infructueux, et qui ne relèvent donc pas du champ d'application de la présente directive, ainsi qu'à la conservation de données à d'autres fins que celle visée par la présente directive.

Communications électroniques: données personnelles, protection de la vie privée et accès aux données relatives au trafic à des fins antiterroristes

En adoptant par 378 voix pour, 197 contre et 30 abstentions, le rapport de M. Alexander Nuno ALVARO(ALDE, DE), le Parlement européen a approuvé en première lecture la directive sur la rétention des données.

Le texte final a fait l'objet d'un accord avec le Conseil. Les amendements adoptés par compromis entre le PPE-DE et le PSE avec le Conseil diffèrent sur plusieurs points clefs de la proposition de directive soutenue par la commission des Libertés civiles. Le GUE, les Verts et l'UEN, ainsi que certains membres de l'ADLE, ont ainsi finalement voté contre.

Dans le texte adopté, le Parlement européen a inséré un certain nombre d'amendements afin de restreindre l'utilisation des données retenues, et d'assurer que la future loi respecte la vie privée des citoyens. En particulier, aucune donnée révélant le contenu de la communication ne pourra être conservée au titre de la présente directive. De plus, la conservation des données devra être effectuée de manière à éviter que les données soient conservées plus d?une fois.

S'agissant de l'objectif de la directive, les députés sont d'avis que la conservation des données doit s'appliquer pour la prévention, la recherche, la détection et la poursuite d'infractions graves telles que définies par chaque État membre dans sa législation nationale. (terrorisme et criminalité organisée) mais pas pour la prévention de toutes sortes de crimes. Les députés ont estimé que le concept de prévention était trop vague et pouvait conduire à des abus de la part des autorités nationales. Ils ont par ailleurs précisé les définitions des termes « service téléphonique », « numéro d?identifiant », « identifiant cellulaire » et « appel téléphonique infructueux ».

La directive prévoit que les données soient conservées par les opérateurs de télécommunication pendant une période minimale de 6 mois pouvant aller jusqu'à deux ans. Les députés ont en outre ajouté une disposition qui prévoit des sanctions pénales "effectives, proportionnées et dissuasives" pour les opérateurs qui auraient manqué - délibérément ou par négligence - à leurs obligations de stockage et de protection des informations. Un État membre confronté à des circonstances particulières justifiant une prolongation, pour une période limitée, de la conservation des données, pourra prendre les mesures nécessaires. Il devra notifier les mesures prises à la Commission et aux autres États membres, et les motiver. La Commission pourra approuver ou rejeter les mesures nationales concernées dans un délai de six mois suivant la notification.

Seules les autorités compétentes désignées par États membres seraient autorisées à accéder aux données conservées par les opérateurs de téléphonie et fournisseurs Internet, affirment les députés. Chaque État membre devra en outre veiller à ce que le contrôle de l'application, sur son territoire, des dispositions adoptées soit confié à une autorité publique désignée.

En outre, les députés souhaitent que l'accès aux données soit accordé au cas par cas et dans un but précis : en clair, les autorités devraient demander chaque fois à l'opérateur de télécommunication de consulter les données d'un suspect identifié mais ne pourraient pas avoir accès à toute la base de données.

S'agissant des données qui seraient conservées, les députés sont favorables à l'enregistrement des données de localisation pour les appels reçus, messages courts et protocoles Internet, y compris pour les appels infructueux (restés sans réponse). Les États membres auront dix-huit mois pour se conformer à la directive.

Les députés ont en outre décidé d'éliminer le paragraphe qui prévoyait que les compagnies de télécommunications devraient être intégralement remboursées par les États membres pour les frais occasionnés par la rétention, le stockage et la transmission de données. Le projet de directive soutenu par la commission parlementaire appelait à un remboursement total des coûts.

Communications électroniques: données personnelles, protection de la vie privée et accès aux données relatives au trafic à des fins antiterroristes

Le Conseil a adopté la directive du Parlement européen et du Conseil sur la conservation de données, modifiant la directive 2002/58/CE. La décision fait suite à l'accord dégagé par le Conseil lors de sa session des 1er et 2 décembre 2005.

Les délégations irlandaise et slovaque ont voté contre.

Pour rappel, cette 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 de réseaux publics de communications en matière de conservation de certaines données qui sont générées ou traitées par ces fournisseurs, en vue de garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne.

La directive s'applique aux données relatives au trafic et aux données de localisation concernant tant les entités juridiques que les personnes physiques, 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.

Les États membres disposeront généralement de 18 mois pour se conformer à ces dispositions.

Communications électroniques: données personnelles, protection de la vie privée et accès aux données relatives au trafic à des fins antiterroristes

OBJECTIF : harmoniser les dispositions des États membres relatives aux obligations des fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications en matière de conservation de certaines données.

ACTE LÉGISLATIF : Directive 2006/24/CE du Parlement européen sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE.

CONTENU : le Conseil a adopté une directive sur la conservation de données. Les délégations irlandaise et slovaque ont voté contre.

Cette 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 de réseaux publics de communications en matière de conservation de certaines données qui sont générées ou traitées par ces fournisseurs, en vue de garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne.

La directive s'applique aux données relatives au trafic et aux données de localisation concernant tant les entités juridiques que les personnes physiques, 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.

En ce qui concerne la téléphonie fixe en réseau, la téléphonie mobile, l?accès à l?Internet, le courrier électronique par l?Internet et la téléphonie par l?Internet, les États membres veillent à ce que soient conservées en application de la directive les catégories de données suivantes:

- les données nécessaires pour retrouver et identifier la source d?une communication ;
- les données nécessaires pour identifier la destination d?une communication ;
- les données nécessaires pour déterminer la date, l?heure et la durée d?une communication ;
- les données nécessaires pour déterminer le type de communication ;
- les données nécessaires pour identifier le matériel de communication des utilisateurs ou ce qui est censé être leur matériel ;
- les données nécessaires pour localiser le matériel de communication mobile.

Les données conservées ne sont transmises qu'aux autorités nationales compétentes, dans des cas précis et conformément à la législation nationale. Elles sont conservées pour une durée minimale de six mois et maximale de deux ans à compter de la date de la communication. Les États membres doivent prendre les mesures nécessaires pour faire en sorte que l'accès intentionnel aux données conservées ou le transfert de ces données soient passibles de sanctions, y compris de sanctions administratives ou pénales, qui sont efficaces, proportionnées et dissuasives. Chaque État membre désigne une autorité publique qui est chargée de surveiller l'application, sur son territoire, des dispositions adoptées pour ce qui concerne la sécurité des données conservées.

Un État membre confronté à des circonstances particulières justifiant une prolongation, pour une période limitée, de la durée de conservation maximale prévue par la directive, peut prendre les mesures nécessaires. Il doit notifier immédiatement à la Commission et communiquer aux autres États membres les mesures prises.

Le 15/09/2010 au plus tard, la Commission présentera au Parlement européen et au Conseil une évaluation de l?application de la directive et de ses effets sur les opérateurs économiques et les consommateurs.

ENTRÉE EN VIGUEUR : 03/05/2006.

TRANSPOSITION : 15/09/2007. Chaque État membre peut, jusqu?au 15/03/2009, différer l?application de la directive en ce qui concerne la conservation de données de communication concernant l?accès à l?Internet, la téléphonie par l?Internet et le courrier électronique par l?Internet, à condition de le notifier au Conseil et à la Commission au moyen d?une déclaration. Plusieurs États membres ont fait une déclaration, se réservant ainsi le droit de différer l?application de la directive : Pays-Bas, Autriche, Royaume-Uni, Estonie, Chypre, Grèce, Luxembourg, Slovénie, Suède, Lituanie, Lettonie, République tchèque, Belgique, Pologne, Finlande, Allemagne.

Communications électroniques: données personnelles, protection de la vie privée et accès aux données relatives au trafic à des fins antiterroristes

La Commission présente un rapport d?évaluation concernant la directive sur la conservation des données (directive 2006/24/CE). La directive impose aux États membres de contraindre les fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications à conserver les données relatives au trafic et les données de localisation pendant une durée comprise entre six mois et deux ans aux fins de la recherche, de la détection et de la poursuite d?infractions pénales graves.

Ce rapport évalue l?application de la directive par les États membres et ses effets sur les opérateurs économiques et les consommateurs afin de déterminer s?il y a lieu de modifier ses dispositions, notamment en ce qui concerne la couverture des données et les durées de conservation. Il analyse également les effets de la directive sur les droits fondamentaux et se penche sur la question de savoir si des mesures doivent être prises pour répondre aux préoccupations liées à l?utilisation de cartes SIM anonymes à des fins criminelles.

Dans l?ensemble, l?évaluation a montré que la conservation de données est très utile aux systèmes de justice pénale et aux services répressifs de l?UE. La Commission a l?intention de proposer des modifications de la directive après avoir procédé à une étude d?impact. L?étude d?impact évaluera la conservation des données dans l?UE à l?aune des critères de nécessité et de proportionnalité, compte tenu et dans l?intérêt de la sécurité intérieure, du bon fonctionnement du marché intérieur et du renforcement du respect de la vie privée et du droit à la protection des données à caractère personnel.

La proposition de la Commission visant à réviser le cadre qui régit la conservation des données devrait s?inspirer des conclusions et recommandations suivantes :

1) Encourager et réglementer la conservation des données en tant que mesure de sécurité : les États membres estiment pour la plupart que les règles de l'Union relatives à la conservation des données demeurent nécessaires à la mission des services répressifs, à la protection des victimes et aux systèmes de justice pénale. Même si elles sont limitées sur certains points, les données conservées jouent un rôle capital dans les enquêtes judiciaires.

L?harmonisation des règles dans ce domaine devrait faire de la conservation des données un moyen efficace de lutte contre la criminalité, apporter aux entreprises une sécurité juridique sur un marché intérieur qui fonctionne bien, et assurer l?application cohérente dans toute l?Union d?un niveau élevé de respect de la vie privée et de protection des données à caractère personnel.

2) Transposition de la directive inégale : la latitude considérable laissée aux États membres de la directive 2002/58/CE sur la vie privée pour adopter des mesures relatives à la conservation des données rend toute évaluation de la directive extrêmement délicate. Il existe en effet des différences sensibles entre les mesures de transposition régissant la limitation des finalités, l'accès aux données, les durées de conservation, la protection et la sécurité des données, et les statistiques.

Une législation de transposition est en vigueur dans vingt-deux États membres. Trois États membres (République tchèque, Allemagne, Roumanie) sont en situation de manquement depuis que leur loi de transposition a été annulée par leur cour constitutionnelle. Deux autres États membres (Autriche, Suède) doivent encore transposer la directive. La Commission poursuivra sa collaboration avec les États membres pour garantir la bonne mise en ?uvre de la directive et recourra, s?il le faut, à la procédure d?infraction.

3) La directive n?a pas pleinement harmonisé l?approche de la conservation des données ni créé des conditions de concurrence égales pour les opérateurs : si la conservation des données est une réalité dans la plupart des États membres, la directive ne garantit pas en soi que les données conservées seront stockées, extraites et utilisées dans le strict respect du droit à la vie privée et à la protection des données à caractère personnel. La responsabilité de faire respecter ces droits incombe aux États membres.

La directive ne visait qu?une harmonisation partielle des approches en matière de conservation des données. Aussi, il n?existe pas d?approche commune dans des domaines tels que la limitation des finalités ou les durées de conservation, ou sur des aspects tels que le remboursement des coûts. Les divergences dans l?application nationale de la conservation des données ont créé des difficultés considérables pour les opérateurs.

4) Les opérateurs devraient bénéficier d?un remboursement homogène des coûts qu?ils supportent : l?obligation de conserver et d?extraire des données représente un coût substantiel pour les opérateurs, en particulier pour ceux de taille plus modeste. En outre, les opérateurs sont affectés et remboursés à des degrés divers selon les États membres. La Commission envisagera des moyens de proposer un remboursement homogène aux opérateurs.

5) Garantir la proportionnalité dans le processus intégré de stockage, d?extraction et d?utilisation : la Commission veillera à ce que toute proposition future relative à la conservation des données respecte le principe de proportionnalité et soit apte à atteindre l?objectif de lutte contre les infractions graves et le terrorisme, et n?aille pas au-delà de ce qui est nécessaire pour y parvenir. Elle reconnaîtra que les exceptions et limitations ayant trait à la protection des données à caractère personnel ne doivent s?appliquer que dans la mesure où elles sont nécessaires. Elle évaluera en détail les conséquences d?une réglementation plus stricte du stockage, de l?accès et de l?utilisation des données de trafic sur l?efficacité et l?efficience du système de justice pénale et des services répressifs, sur la vie privée et sur les coûts pour l?administration publique et les opérateurs. Les domaines suivants devraient notamment être examinés dans l?étude d?impact:

- la cohérence entre la limitation des finalités de la conservation des données et les types d?infractions pénales pour lesquels l?accès aux données conservées et leur utilisation peuvent être autorisés;
- une meilleure harmonisation, et éventuellement la réduction, des durées de conservation obligatoire des données ;
- un contrôle indépendant des demandes d?accès et du régime général d?accès et de conservation des données appliqué dans tous les États membres;
- la limitation des autorités autorisées à accéder aux données;
- la réduction des catégories de données à conserver;
- l?élaboration d?orientations sur les mesures de sécurité techniques et organisationnelles pour l?accès aux données, y compris des procédures de transfert;
- l?élaboration d?orientations sur l?utilisation des données, y compris la prévention de la recherche aléatoire de données («data mining »); et
- l?établissement de critères de mesure réalistes et de procédures de rapport afin de faciliter les comparaisons sur l?application d?un futur instrument et son évaluation.

La Commission déterminera par ailleurs si une approche européenne de la conservation des données a posteriori peut compléter la conservation des données et, dans l?affirmative, selon quelles modalités.

En ce qui concerne la « check-list » des droits fondamentaux établie par la Commission pour toutes les propositions législatives et l?approche de la gestion de l?information dans le domaine de la liberté, de la sécurité et de la justice, la Commission examinera chacun de ces domaines à l?aune du principe de proportionnalité et de l?exigence de prévisibilité. Elle veillera également à assurer la cohérence avec la révision actuelle du cadre européen de la protection des données.

Á partir de la présente évaluation, la Commission proposera une révision du cadre actuel régissant la conservation des données. Elle élaborera plusieurs options en consultation avec les autorités répressives, judiciaires et celles chargées de la protection des données, les groupes représentant le secteur et les consommateurs, et la société civile. Elle étudiera de manière approfondie la perception qu?a le public de la conservation des données et son incidence sur les comportements. Ces conclusions alimenteront une étude de l?impact des possibilités d?action recensées, qui servira de base à la proposition de la Commission.

Communications électroniques: données personnelles, protection de la vie privée et accès aux données relatives au trafic à des fins antiterroristes

Avis du Contrôleur européen de la protection des données sur le rapport d?évaluation de la Commission au Conseil et au Parlement européen concernant la directive sur la conservation des données (directive 2006/24/CE)

Le CEPD rappelle que la Commission a présenté le 18 avril 2011 un rapport d?évaluation concernant la directive sur la conservation des données, envoyé à titre d?information au Contrôleur à cette même date.

Il rappelle également que la directive sur la conservation des données constituait une réponse de l?UE à des défis de sécurité urgents, après les attentats terroristes de Madrid en 2004 et de Londres en 2005. Malgré la finalité légitime de la mise en place d?un système de conservation des données, des voix se sont élevées contre l'impact considérable que la mesure pouvait avoir sur la vie privée des citoyens.

Depuis 2005, le CEPD suit de près la création, la mise en ?uvre et l?évaluation de la directive de différentes manières. Le CEPD a rendu un avis critique en 2005, après la publication de la proposition par la Commission.

De manière générale, le Contrôleur estime que la directive sur la conservation des données constitue un exemple frappant d?une mesure de l?UE visant à assurer la disponibilité pour des activités répressives des données générées et traitées dans le contexte des communications électroniques. Maintenant que la mesure est en place depuis plusieurs années, une évaluation de son application pratique devrait véritablement prouver la nécessité et la proportionnalité de la mesure à la lumière des droits au respect de la vie privée et de la protection des données à caractère personnel.

Le CEPD estime que la procédure d?évaluation actuelle devrait être utilisée pour guider l?évaluation d?autres instruments de l?UE et pour assurer que seules les mesures véritablement justifiées restent en place. Il présente dès lors son avis en cherchant à analyser la directive afin de déterminer si la conservation des données satisfait aux exigences du respect des droits fondamentaux. L?analyse tentera également de

déterminer si la nécessité de la conservation des données telle qu?arrêtée par la directive, a été suffisamment démontrée.

L?avis présente le contenu principal de la directive sur la conservation des données et son lien avec la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques. Il expose également les changements apportés par le traité de Lisbonne, contient l?analyse de la validité de la directive sur la conservation des données, à la lumière des droits à la vie privée et à la protection des données à caractère personnel et présente les éventuelles pistes à suivre.

La directive ne répond pas aux exigences : le rapport d?évaluation met en évidence plusieurs faiblesses de la présente directive. Les informations fournies dans le rapport montrent que la directive n?a pas réussi à atteindre son objectif principal, à savoir harmoniser les législations nationales en matière de conservation des données. La Commission note des différences «sensibles» entre les mesures de transposition régissant la limitation des finalités, l'accès aux données, les durées de conservation, la protection et la sécurité des données, et les statistiques. Un tel manque d?harmonisation ne peut qu?être préjudiciable à toutes les parties concernées: les citoyens, les chefs d?entreprise ainsi que les autorités répressives.

Sur la base du rapport d?évaluation, la directive ne satisfait pas aux exigences établies par les droits à la vie privée et à la protection des données à caractère personnel, pour les motifs suivants:

- la nécessité de la conservation des données telle qu?arrêtée par la directive sur la conservation des données n?a pas été suffisamment démontrée ;
- la conservation des données aurait pu être réglementée d?une manière moins intrusive dans la vie privée ;
- la directive sur la conservation des données manque de prévisibilité.

Dans ce contexte, le CEPD appelle la Commission à envisager sérieusement la possibilité d?abroger purement et simplement la directive, de façon exclusive ou combinée avec une proposition de mesure alternative de l?UE plus ciblée.

Nécessité : le CEPD estime que la Commission aurait dû être plus critique à l?égard des États membres pour qu?ils produisent des éléments suffisants démontrant la nécessité de la mesure. Les déclarations politiques de certains États membres sur la nécessité d?une telle mesure ne peuvent justifier à elles seules une action de l?UE.

Constatant que sous sa forme actuelle, la directive ne pouvait être maintenue, le CEPD affirme qu?avant de proposer une version révisée de la directive:

- la Commission devait, durant l?étude d?impact, s?atteler à collecter des preuves pratiques supplémentaires auprès des États membres afin de démontrer la nécessité de la conservation des données en tant que mesure au titre du droit de l?UE;
- si une majorité des États membres considère la conservation des données comme étant nécessaire, ces États membres doivent tous fournir des preuves quantitatives et qualitatives pour le démontrer;
- les États membres qui s?opposent à une mesure de conservation des données doivent fournir à la Commission les informations pertinentes pour permettre une évaluation plus large de la question.

Il convient de souligner que l?évaluation de la nécessité et l?examen des moyens alternatifs moins intrusifs dans la vie privée ne peuvent être menés équitablement que si toutes les options pour l?avenir de la directive sont laissées ouvertes. À cet égard, la Commission semble exclure la possibilité d?abroger purement et simplement la directive. Le CEPD appelle donc la Commission à considérer sérieusement cette option dans l?étude d?impact qu?elle présentera pour réviser la présente directive. Le CEPD estime par ailleurs que toute future directive sur la conservation des données ne pourra être envisagée que si tout le monde s?accorde sur la nécessité d?une réglementation de l?UE du point de vue du marché interne et de la coopération policière et judiciaire en matière pénale et si, durant l?étude d?impact, la nécessité de la conservation des données, encouragée et réglementée par l?UE, peut être suffisamment démontrée, avec un examen minutieux des mesures alternatives. Il ne nie toutefois pas la valeur des données conservées à des fins de répression ni le rôle capital qu?elles peuvent jouer dans des cas spécifiques.

Directive sur la vie privéeet les communications électroniques : conformément à l?article 15 par 1 de cette directive, il est possible pour les États membres de prendre des mesures législatives pour limiter la portée des obligations prévues lorsqu?il s?agit d?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 [?]». La question de la conservation des données est explicitement mentionnée à cet article. Or, de nombreux États membres ont utilisés les données conservées à d?autres finalités, ce qui, pour le CEPD, laisse entrevoir une forme de «vide juridique» dans ce domaine.

La conservation des données va au-delà de ce qui est nécessaire : il ressort de l?analyse du CEPD que la directive sur la conservation des données a réglementé la conservation des données bien au-delà de ce qui était nécessaire, ou, tout au moins, qu?elle a été incapable de garantir que la conservation des données n?avait pas été appliquée de manière abusive. Le CEPD affirme ainsi que :

- la finalité imprécise de la mesure et la notion plutôt large des «autorités nationales compétentes» a donné lieu à une utilisation des données conservées à des fins, et par des autorités, bien trop nombreuses ;
- la période de conservation maximale de 2 ans semble aller au-delà de ce qui est nécessaire. Les informations statistiques de certains États membres montrent qu?une grande majorité des demandes d?accès portent sur des données d?une ancienneté de 6 mois maximum. En outre, l?absence d?une période de conservation fixée pour l?ensemble des États membres a créé toute une série de législations nationales divergentes ;
- le niveau de sécurité n?est pas suffisamment harmonisé et donc une consultation plus large et un examen plus concret des cas d?abus s?avèrent nécessaires ;
- l?évaluation ne permet pas de déterminer si toutes les catégories de données conservées se sont avérées nécessaires (seules quelques distinctions générales sont établies entre données téléphoniques et internet).

Exigences minimales d?un futur instrument : pour le CEPD, toute future directive sur la conservation des données devra satisfaire aux exigences fondamentales suivantes:

- il doit être global et véritablement harmoniser les règles sur l?obligation de conservation des données, ainsi que sur l?accès et l?utilisation ultérieure des données par les autorités compétentes;
- il doit être exhaustif, ce qui signifie qu?il doit avoir une finalité claire et précise, et que le vide juridique existant à l?article 15,

paragraphe 1, de la directive sur la vie privé et les communications électroniques doit être comblé;

- il doit être proportionnel et ne pas aller au-delà de ce qui est nécessaire.