E 2966

ASSEMBLÉE NATIONALE

DOUZIÈME LÉGISLATURE

SÉNAT

SESSION EXTRAORDINAIRE DE 2004-2005

Reçu à la Présidence de l'Assemblée nationale
le 30 septembre 2005

Enregistré a la Présidence du Sénat le 30 septembre 2005

TEXTE SOUMIS EN APPLICATION DE L'ARTICLE 88-4 DE LA CONSTITUTION

PAR LE GOUVERNEMENT,

À L'ASSEMBLÉE NATIONALE ET AU SÉNAT.

Proposition de directive du Parlement européen et du Conseil sur la conservation des 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) 438 final

FICHE DE TRANSMISSION DES PROJETS D'ACTES DES COMMUNAUTES EUROPEENNES ET DE L'UNION EUROPEENNE

- article 88-4 de la Constitution -

INTITULE

COM (2005) 438 final
Proposition de directive du Parlement européen et du Conseil sur la conservation des données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, et modifiant la directive 2002/58/CE.

NATURE	
	S.O. Sans Objet
	L Législatif
	N.L. Non Législatif

Date d'arrivée au Conseil d'Etat :

27/09/2005

Date de départ du Conseil d'Etat :

29/09/2005

Observations :

La proposition de directive a pour objet l'harmonisation des obligations imposées aux fournisseurs de services de télécommunications électroniques accessibles au public en matière de traitement et de conservation de certaines données techniques relatives aux communications. Les dispositions de ce projet, en sus d'imposer des obligations aux fournisseurs de services, touchent au secret des correspondances (lors même qu'elles ne s'appliquent pas au contenu des communications) et, d'une manière générale, aux droits de la personne. Elle relèveraient de la loi en droit interne.

COMMISSION DES COMMUNAUTÉS EUROPÉENNES

Bruxelles, le 21.9.2005
COM(2005) 438 final

2005/0182 (COD)

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

(présentée par la Commission)

{SEC(2005) 1131}

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

- **Motivations et objectifs de la proposition**

Les activités et transactions quotidiennes des citoyens impliquent un recours sans cesse croissant aux réseaux et services de communications électroniques. Ces communications génèrent des «données relatives au trafic» ou des «données de localisation», qui renseignent par exemple sur l'endroit où se trouve l'appelant, sur le numéro appelé ainsi que sur la date, l'heure et la durée de l'appel. Lorsque les données relatives au trafic sont associées à des données permettant l'identification de l'abonné ou de l'utilisateur du service, la disponibilité de ces données relatives au trafic est importante pour l'accomplissement des missions des services répressifs et de sécurité, comme la prévention, la recherche, la détection et la poursuite d'infractions graves, telles que les actes terroristes et la criminalité organisée.

Toutefois, en raison de l'évolution des stratégies commerciales et des offres de services, et notamment du développement des tarifs forfaitaires et des services de communications électroniques prépayés ou gratuits, il arrive que les données relatives au trafic ne soient pas stockées par tous les opérateurs dans la même mesure que ces dernières années, selon les services qu'ils proposent. Cette tendance est accentuée par les offres récentes de services de communication vocale sur Internet (*Voice over IP*), voire de services forfaitaires de téléphonie fixe. Pour les services de ce type, les opérateurs ne devraient plus avoir besoin de stocker les données relatives au trafic à des fins de facturation. Si ces données ne sont pas stockées pour établir les factures ou à d'autres fins commerciales, elles ne pourront plus être mises à la disposition des pouvoirs publics lorsque ceux-ci auront des motifs légitimes d'y accéder. En d'autres termes, du fait de ces évolutions, il devient de plus en plus difficile pour les pouvoirs publics de remplir leurs missions de prévention de la criminalité organisée et du terrorisme et de lutte contre ces phénomènes, et de plus en plus facile pour les criminels de communiquer entre eux, sans craindre que les données concernant leurs communications puissent être utilisées par les services répressifs pour déjouer leurs plans.

Il est désormais urgent d'adopter des dispositions harmonisées au niveau de l'UE 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. Des disparités sur le plan des dispositions législatives, réglementaires et techniques dans les États membres concernant la conservation de données relatives au trafic font obstacle au marché intérieur des communications électroniques, puisque les fournisseurs de services doivent satisfaire à des exigences différentes pour ce qui est des types de données à conserver ainsi que des conditions de conservation. Il convient donc de poursuivre l'harmonisation de ces dispositions, conformément à l'article 14 du traité CE.

- **Contexte général**

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'UE 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. Dans les conclusions du Conseil européen des 16 et 17 juin, ainsi que lors de la réunion spéciale du Conseil JAI du 13 juillet 2005, organisée à la suite des attentats de Londres, il a récemment été réaffirmé qu'il était prioritaire d'adopter un instrument législatif adapté dans ce domaine.

- **Dispositions en vigueur dans le domaine de la proposition**

La directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) harmonise, au moyen de ses articles 6 et 9, les règles de protection des données à caractère personnel applicables au traitement 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. Son article 15, paragraphe 1, dispose que les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus (notamment) aux articles 5, 6 et 9 lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, 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.

- **Cohérence avec les autres politiques et les objectifs de l'Union**

La présente proposition est conforme au droit communautaire et à la Charte des droits fondamentaux. Même si, de toute évidence, la proposition aura des conséquences sur le droit au respect de la vie privée des citoyens, tel qu'il est garanti par l'article 7 de la Charte, ainsi que sur le droit à la protection des données à caractère personnel, tel qu'il est garanti par l'article 8 de la Charte, les limitations de ces droits se justifient conformément à l'article 52 de la Charte. En particulier, les limitations prévues par la présente proposition sont proportionnées et nécessaires pour atteindre les objectifs, généralement reconnus, de prévention de la criminalité et du terrorisme et de lutte contre ces phénomènes.

En outre, la présente proposition encadre les incidences qu'elle aura sur la vie privée des citoyens: premièrement, en définissant avec précision la finalité pour laquelle les données conservées peuvent être utilisées, deuxièmement, en circonscrivant les catégories de données qui doivent être conservées et, troisièmement, en limitant la

durée de conservation des données. Autre garantie importante, la présente directive n'est pas applicable au contenu des communications – cela équivaudrait à prévoir l'interception de télécommunications, ce qui échappe au champ d'application du présent instrument législatif.

Les dispositions générales et spécifiques en matière de protection de données établies par les directives 95/46/CE et 2002/58/CE s'appliquent au traitement des données à caractère personnel conservées en vertu des dispositions de la présente directive par les fournisseurs de services et de réseaux – ce qui signifie qu'en pratique, il est inutile de prévoir des dispositions supplémentaires spécifiques relatives aux principes généraux en matière de protection des données et à la sécurité des données. Cela implique aussi que le traitement de données de ce type se fera sous le contrôle exclusif des autorités chargées de la protection des données, instituées dans tous les États membres.

2. CONSULTATION DES PARTIES INTERESSEES ET ANALYSE D'IMPACT

- **Consultation des parties intéressées**

Méthodes de consultation utilisées, principaux secteurs visés et profil général des répondants

Dès 2001 dans le cadre des réunions du Forum sur la cybercriminalité, la question de la conservation des données relatives au trafic a fait l'objet de consultations avec les représentants des services répressifs, le secteur des communications électroniques et les experts en matière de protection de données.

Le 14 juin 2004, une table ronde ad hoc organisée sous les auspices du Forum européen de la prévention du crime organisé a rassemblé des représentants des services répressifs, du secteur des communications électroniques et des organisations de protection des données. Le 30 juillet 2004, un document de consultation conjoint sur la conservation de données relatives au trafic a été présenté par la DG INSFO et la DG JLS, en préparation d'un atelier public sur la question, qui s'est tenu le 21 septembre 2004. Le document de consultation conjoint a suscité des contributions et des réactions de diverses parts – notamment du secteur industriel concerné et des associations de défense des droits de l'homme. L'atelier public du 21 septembre a fourni des éléments de réflexion supplémentaires à la Commission.

Pour préparer la présente proposition, la Commission s'est aussi inspirée du débat public de grande ampleur consacré à ce sujet, notamment des discussions qui se sont tenues au Parlement européen.

Synthèse des réponses reçues et de la façon dont elles ont été prises en compte

La procédure de consultation a confirmé que la conservation de données relatives au trafic des communications constitue un outil essentiel utilisé par les services répressifs pour prévenir la criminalité et le terrorisme et lutter contre ces phénomènes. Selon les services répressifs, il convient, pour leur permettre de s'acquitter des missions qui sont les leurs, de prévoir des durées de conservation aussi longues que nécessaire et de conserver autant de données que nécessaire. En

particulier pour des enquêtes complexes portant sur des infractions graves, dont la conclusion peut exiger plusieurs années, des données relatives au trafic plus anciennes sont encore régulièrement nécessaires. Les répondants ont cité plusieurs exemples dans lesquels des données de ce type s'étaient avérées décisives pour des enquêtes pénales, la plupart du temps concernant des infractions comme des attentats à la bombe ou des meurtres.

Les délégués d'organisations européennes représentant le secteur des télécommunications et d'Internet, ainsi que diverses entreprises fournissant des services de communications électroniques, ont fait valoir que, s'ils étaient certes disposés à collaborer avec les services répressifs, ce qu'ils faisaient déjà, de longues périodes de conservation engendreraient des coûts considérables et que le stockage des données serait suffisant. Ils ont en tout état de cause plaidé pour des durées de conservation ne dépassant pas six mois, puisque la plupart des données demandées par les services répressifs ne remontent pas plus loin, et en faveur de mécanismes de compensation des coûts supplémentaires qu'ils supporteraient.

Les représentants des autorités chargées de la protection des données et des associations de défense des droits de l'homme ont soutenu que la conservation de données constitue une atteinte à la vie privée des citoyens, raison pour laquelle les durées de conservation doivent être les plus courtes possible. D'une manière générale, ils ont émis des doutes quant au fait que des durées de conservation supérieures à six mois puissent être qualifiées de proportionnées. Ils ont également fait part de leurs préoccupations au sujet de la finalité et des objectifs de la conservation, qui devraient être définis clairement et précisément.

La présente proposition adopte une approche équilibrée et s'appuie sur l'analyse d'impact ci-jointe. Les 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, permettront de répondre aux principaux besoins des services répressifs, tout en limitant les coûts qui y sont liés pour l'industrie, ainsi que l'ingérence dans la vie privée des citoyens. Une période de conservation de six mois pour toutes les données aurait été trop courte car bien qu'un nombre considérable de demandes des autorités de poursuites soit lié aux données de moins de six mois, les données de plus de six mois sont en général requises dans le cadre d'actes criminels plus sérieux tel que le terrorisme, le crime organisé ou le meurtre.

- **Obtention et utilisation d'expertise**

Il n'a pas été nécessaire de faire appel à des experts extérieurs.

- **Analyse d'impact**

Plusieurs options ont été envisagées. En 2002, le Conseil avait expressément prôné un dialogue au niveau de l'UE et au niveau national afin de trouver des solutions au problème de la conservation de données relatives au trafic, permettant de répondre à la nécessité de disposer d'outils efficaces de prévention, de recherche, de détection et de poursuite d'infractions pénales, mais aussi de garantir la protection des libertés et droits fondamentaux des personnes physiques, notamment de leurs droits à la vie privée, à la protection des données et au secret de la correspondance. En dépit des

nombreux débats et consultations publics consacrés à la question, et notamment des discussions au Parlement européen, il n'a pas été possible de dégager une solution commune.

À défaut d'initiative dans le domaine de la conservation des données, la mosaïque actuelle de dispositions en la matière demeurera en place. L'idée d'un acte législatif non contraignant a été écartée, car un tel acte n'offre pas le niveau suffisant de sécurité juridique. De même, une initiative dans le domaine de la conservation de données fondée sur le troisième pilier a été repoussée en raison de son incompatibilité avec la législation communautaire actuelle. Dans sa déclaration sur la lutte contre le terrorisme, le Conseil européen a aussi plaidé pour une approche législative.

L'option retenue, une proposition de directive, offre le niveau d'harmonisation nécessaire dans le marché intérieur. Par rapport à un règlement, elle laisse, dans un domaine sensible, une certaine marge de manœuvre aux États membres pour ce qui est de la mise en œuvre. Un règlement aurait été trop contraignant, notamment compte tenu des divergences entre les architectures techniques utilisées par les divers opérateurs dans les différents pays. La directive laissera suffisamment de latitude aux États membres pour leur permettre de prendre en considération les contraintes nationales. En tout état de cause, le statu quo n'est plus tenable en raison des entraves à la libre fourniture de services que créent les dispositions nationales divergentes dans ce domaine. Le choix de cet instrument juridique et de la base juridique spécifique de l'article 95 CE découle également de l'analyse juridique figurant dans le document de travail des services de la Commission SEC(2005) 420 du 22 mars 2005. La Commission a effectué une analyse d'impact, dont le rapport peut être consulté à l'adresse suivante: http://europa.eu.int/comm/dgs/justice_home/evaluation/dg_coordination_evaluation_annexe_en.htm.

3. ÉLEMENTS JURIDIQUES DE LA PROPOSITION

- **Résumé des mesures proposées**

La directive proposée a pour objectif d'harmoniser les obligations, pour les fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications, de conserver certaines données relatives au trafic, de sorte qu'elles puissent être transmises aux autorités compétentes des États membres en vue de la prévention, de la recherche, de la détection et de la poursuite d'infractions graves, comme les actes terroristes et la criminalité organisée.

- **Base juridique**

Article 95 du traité CE.

- **Principe de subsidiarité**

Le principe de subsidiarité s'applique dès lors que la proposition ne relève pas de la compétence exclusive de la Communauté.

Les objectifs de la proposition ne peuvent être réalisés de manière suffisante par les États membres pour la ou les raisons suivantes.

L'harmonisation des durées de conservation des données relatives au trafic ne peut être réalisée par les États membres eux-mêmes. L'action de l'UE – prônée par le Conseil européen – permettra de garantir que les données relatives au trafic seront conservées à travers l'Union européenne et pourront être mises à la disposition des services répressifs.

L'efficacité des enquêtes des services répressifs étant fortement tributaire de la coopération internationale, et les divergences entre les solutions choisies au niveau national ayant des retombées négatives sur le marché des communications électroniques, une harmonisation à l'échelle européenne des régimes de conservation de données relatives au trafic constitue le choix politique le plus approprié. Le principe du remboursement des coûts permettra de maintenir des conditions équivalentes en matière de concurrence entre les fournisseurs de communications électroniques dans le marché intérieur.

Grâce à l'action communautaire, il sera possible de mieux réaliser les objectifs de la proposition pour la ou les raisons suivantes:

L'action de l'UE permettra de mieux atteindre les objectifs de la proposition en garantissant que les données relatives au trafic seront conservées à travers l'Union européenne et pourront être mises à la disposition des services répressifs dans les mêmes conditions. La présente mesure sera également bénéfique pour le secteur des communications électroniques, notamment les entreprises proposant des services dans plusieurs États membres, puisqu'elles pourront standardiser leur technologie.

Les indicateurs qualitatifs qui permettent de démontrer que l'objectif peut être mieux réalisé par l'Union sont l'efficacité des services répressifs s'agissant de prévenir et de combattre la criminalité et le terrorisme, en particulier les actes terroristes et la criminalité organisée, qui ont souvent un caractère transfrontalier.

La proposition se limite aux objectifs que les États membres ne peuvent réaliser de manière satisfaisante et à ce que l'Union peut mieux faire en restreignant l'étendue des obligations de conservation qui pèsent sur les fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications. La proposition laisse aux États membres le choix des autorités devant avoir accès aux données conservées et des conditions de cet accès. L'accès des services répressifs concernés aux informations et l'échange de ces informations entre ces services sont des questions qui ne relèvent pas du champ d'application du traité CE.

Dans ce contexte, il y a lieu de mentionner que la Commission prépare actuellement des projets de propositions législatives fondées sur le traité sur l'Union européenne et concernant le principe de disponibilité des informations à des fins répressives et l'adoption de principes en matière de protection des données pour le troisième pilier. Il convient en outre de relever qu'aucun accès ne sera accordé aux «données conservées» en application de la présente directive à des finalités autres que répressives, c'est-à-dire que les fournisseurs de services de communications électroniques ne pourront y avoir accès.

Par conséquent, la proposition respecte le principe de subsidiarité.

- **Principe de proportionnalité**

La proposition respecte le principe de proportionnalité car son effet sur les citoyens et les entreprises a été limité dans toute la mesure du possible. Il convient de rappeler que cet instrument ne porte que sur les données relatives au trafic qui sont traitées par les fournisseurs de communications électroniques. Le contenu des communications électroniques est exclu du champ d'application de la présente directive.

La recherche de l'équilibre le plus approprié entre tous les intérêts en jeu, comme le contexte social et économique, les exigences en matière de sécurité et les préoccupations concernant la vie privée a été guidée essentiellement par le respect des libertés et droits fondamentaux, et notamment du droit à la vie, et par la limitation stricte de l'ingérence dans la vie privée.

La présente proposition de directive a par conséquent tenu compte des questions de proportionnalité et, plus spécifiquement, des durées de conservation proposées, de la distinction entre données téléphoniques et données Internet, de la limitation des catégories de données à conserver et du mécanisme de remboursement des coûts. En particulier, la proposition limite strictement les finalités pour lesquelles les données conservées peuvent être transmises aux services répressifs. La législation en matière de protection de données sera pleinement applicable aux données conservées, tandis que l'incidence sur les droits fondamentaux et les retombées pour les opérateurs économiques seront limitées grâce au choix d'un ensemble restreint de données relatives au trafic à conserver. En outre, la période de conservation plus courte prévue pour les données relatives au trafic générées par l'utilisation d'Internet, par opposition aux données relatives au trafic générées par l'utilisation de la téléphonie fixe ou mobile «traditionnelle», tient compte des pratiques commerciales actuelles en réduisant sensiblement le volume de données à conserver.

La charge financière et administrative incombant aux administrations nationales, aux opérateurs économiques et aux citoyens a été minimisée de plusieurs façons. Premièrement, la directive prévoit une harmonisation, ce qui se traduira par une réduction des coûts de mise en conformité pour les fournisseurs de services de communications électroniques ou d'un réseau public de communications. Deuxièmement, les coûts ont été réduits au minimum en limitant strictement les durées de conservation, ainsi que les catégories de données à conserver. Eu égard à l'importance de la mesure sur le plan de la prévention de la criminalité et du terrorisme et de la lutte contre ces phénomènes, les frais supplémentaires que les États membres devront supporter en raison du remboursement des coûts sont considérés comme proportionnés (voir l'analyse d'impact).

Il convient aussi de souligner que la présente directive ne porte nullement atteinte à la possibilité des États membres de demander des mesures spécifiques de conservation de données, par exemple si un suspect ou une organisation criminelle ont déjà été identifiés ou en cas d'événements particuliers comme des attentats.

- **Choix des instruments**

Instrument proposé: directive.

Le recours à d'autres moyens n'aurait pas été adéquat pour les motifs suivants:

Le problème de la base juridique à choisir pour une proposition sur la conservation de données relatives au trafic a récemment été examiné dans un document de travail des services de la Commission. En bref, la position exposée dans ce document est la suivante: la question de la conservation de données relatives au trafic a déjà fait l'objet d'instruments législatifs précédents fondés sur une base juridique du premier pilier, comme les directives 2002/58/CE et 95/46/CE précitées. Toujours selon cette analyse, ce n'est que parce qu'il a été impossible de trouver un accord politique sur la durée effective de la conservation que cette question n'a pas fait l'objet d'une harmonisation plus complète dans la directive 2002/58/CE; cette analyse conclut en indiquant que, par conséquent, tout nouvel instrument juridique sur la conservation de données relatives au trafic en tant que telle (au contraire des dispositions régissant l'échange de ce type de données entre services répressifs et l'accès à ces données par ces mêmes services) doit aussi se fonder sur une base juridique du premier pilier. Cette logique s'inscrit dans le droit fil de l'article 47 du traité sur l'Union européenne, qui établit le rapport entre les traités CE et UE et dispose qu'aucun instrument législatif adopté en application du traité sur l'Union européenne ne peut affecter le cadre législatif adopté en application du traité CE.

4. INCIDENCE BUDGETAIRE

La proposition n'a aucune incidence sur le budget de la Communauté.

5. INFORMATIONS SUPPLEMENTAIRES

- **Réexamen / révision / clause de suppression automatique**

La proposition inclut une clause de réexamen. Pour aider la Commission dans sa mission de réexamen, la création d'une Plateforme sur la conservation de données est envisagée. Cette plateforme pourrait rassembler des experts techniques des communications électroniques, ainsi que des représentants des services répressifs et des autorités chargées de la protection des données.

- **Tableau de correspondance**

Les États membres sont tenus de communiquer à la Commission le texte des dispositions nationales transposant la directive proposée ainsi qu'un tableau de correspondance entre lesdites dispositions et la directive.

2005/0182 (COD)

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

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité instituant la Communauté européenne, et notamment son article 95,

vu la proposition de la Commission[1],

vu l'avis du Comité économique et social européen[2],

vu l'avis du Comité des régions[3],

statuant conformément à la procédure visée à l'article 251 du traité,

considérant ce qui suit:

(1) La directive 95/46/CE du Parlement européen et du Conseil 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[4] oblige les États membres à assurer la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel, afin d'assurer la libre circulation de ces données dans la Communauté.

(2) La directive 2002/58/CE du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)[5] traduit les principes définis dans la directive 95/46/CE en règles spécifiques au secteur des communications électroniques.

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

---

1 JO C [...] du [...], p. [...].
2 JO C [...] du [...], p. [...].
3 JO C [...] du [...], p. [...].
4 JO L 281 du 23.11.1995, p. 31.
5 JO L 201 du 30.7.2002, p. 37.

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.

(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.

(5) Plusieurs États membres ont légiféré sur la conservation de données par les fournisseurs de services en vue de la prévention, de la recherche, de la détection et de la poursuite de délits et d'infractions pénales; les dispositions des différentes législations nationales varient considérablement.

(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.

(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.

(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.

(9) Dans sa déclaration du 25 mars 2004 sur la lutte contre le terrorisme, 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.

(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.

(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.

(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.

(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 Etats 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.

(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.

(15) Il convient de rappeler que la directive 95/46/CE et la directive 2002/58/CE sont applicables sans réserve aux données conservées conformément à la présente directive; l'article 30, paragraphe 1, point c), de la directive 95/46/CE exige la consultation du «groupe de travail article 29».

(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 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.

(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[6].

(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.

(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,

ONT ARRÊTÉ LA PRÉSENTE DIRECTIVE:

Article premier
Objet et champ d'application

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.

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.

Article 2
Définitions

1. Aux fins de la présente directive, les définitions contenues dans la directive 95/46/CE, la directive 2002/21/CE[7], ainsi que la directive 2002/58/CE s'appliquent.

---

6 JO L 184 du 17.7.1999, p. 23.

2. Aux fins de la présente directive, on entend par :

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.

b) «utilisateur» toute personne physique ou morale qui utilise un service de communications électroniques accessible au public à des fins privées ou professionnelles sans être nécessairement abonnée à ce service.

Article 3
Obligation de conservation de données

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.

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.

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.

---

[7] JO L 108 du 24.4.2002, p. 33.

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

Article 5
Révision de l'annexe

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

Article 6
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.

Article 7
Durées de conservation

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.

Article 8
Conditions à observer pour le stockage des données conservées

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.

Article 9
Statistiques

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.

Ces statistiques ne contiennent pas de données à caractère personnel.

Article 10
Coûts

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.

Article 11
Modification de la directive 2002/58/CE

À l'article 15 de la directive 2002/58/CE, le paragraphe 1 *bis* suivant est inséré:

«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 …. ».

Article 12
Évaluation

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.

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.

Article 13
Transposition

1. Les États membres mettent en vigueur les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive [quinze mois au

plus tard après son adoption]. Ils communiquent immédiatement à la Commission le texte de ces dispositions ainsi qu'un tableau de correspondance entre ces dispositions et la présente directive.

Lorsque les États membres adoptent ces dispositions, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication officielle. Les modalités de cette référence sont arrêtées par les États membres.

2. Les États membres communiquent à la Commission le texte des dispositions essentielles de droit interne qu'ils adoptent dans le domaine régi par la présente directive.

Article 14
Entrée en vigueur

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

Article 15
Destinataires

Les États membres sont destinataires de la présente directive.

Fait à Bruxelles, le

Par le Parlement européen	*Par le Conseil*
Le Président	*Le Président*

Annexe

Types de données à conserver pour chacune des catégories définies à l'article 4 de la présente directive:

a) 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, de courrier électronique par Internet et de téléphonie par 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) l'identité de connexion ou numéro de téléphone attribué à toute communication entrant dans le réseau téléphonique public;

(d) 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 retrouver et identifier la destination d'une communication:

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

(a) le ou les numéros de téléphone appelés;

(b) les nom et adresse du ou des abonnés ou utilisateurs enregistrés;

(2) En ce qui concerne la téléphonie mobile:

(a) le ou les numéros de téléphone appelés;

(b) les nom et adresse du ou des abonnés ou utilisateurs enregistrés;

(3) En ce qui concerne les services d'accès à Internet, de courrier électronique par Internet et de téléphonie par Internet:

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

(b) les nom et adresse du ou des abonnés ou utilisateurs enregistrés qui est/sont le ou les destinataires visés d'une communication;

c) 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, de courrier électronique par Internet et de téléphonie par Internet:

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

d) 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, conférence téléphonique, télécopie et services de messagerie.

(2) En ce qui concerne la téléphonie mobile:

(a) 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:

(1) En ce qui concerne la téléphonie mobile:

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

(b) l'identité internationale d'équipement mobile (IMEI) de l'appelant et de l'appelé.

(2) En ce qui concerne les services d'accès à Internet, de courrier électronique par Internet et de téléphonie par 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;

(c) l'adresse de contrôle d'accès au média (MAC) ou tout autre identifiant machine de l'auteur de la communication.

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

(1) l'identité de localisation (identifiant cellulaire) au début et à la fin de la communication;

(2) la mise en correspondance des identifiants cellulaires et de leur localisation géographique au début et à la fin de la communication.