**CONSEIL DE L'UNION EUROPÉENNE**

**Bruxelles, le 19 avril 2011 (20.04)**
**(OR. en)**

**9324/11**

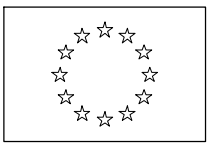
**DAPIX 38**
**TELECOM 47**
**COPEN 85**

**NOTE DE TRANSMISSION**

| | |
|---|---|
| Origine: | Pour le Secrétaire général de la Commission européenne,<br>Monsieur Jordi AYET PUIGARNAU, Directeur |
| Date de réception: | 18 avril 2011 |
| Destinataire: | Monsieur Pierre de BOISSIEU,<br>Secrétaire général du Conseil de l'Union européenne |
| N° doc. Cion: | COM(2011) 225 final |
| Objet: | Rapport de la Commission au Conseil et au Parlement européen<br>- Rapport d'évaluation concernant la directive sur la conservation des données (directive 2006/24/EC) |

Les délégations trouveront ci-joint le document de la Commission - COM(2011) 225 final.

p.j.: COM(2011) 225 final



COMMISSION EUROPÉENNE

Bruxelles, le 18.4.2011
COM(2011) 225 final

# RAPPORT DE LA COMMISSION AU CONSEIL ET AU PARLEMENT EUROPÉEN

## Rapport d'évaluation concernant la directive sur la conservation des données (directive 2006/24/CE)

**RAPPORT DE LA COMMISSION AU CONSEIL ET AU PARLEMENT EUROPÉEN**

**Rapport d'évaluation concernant la directive sur la conservation des données (directive 2006/24/CE)**

## 1. INTRODUCTION

La directive sur la conservation des données[1] (ci-après «la directive») impose aux États membres de contraindre les fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications (ci-après «les opérateurs») 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 de la Commission présente, conformément à l'article 14 de la directive, une évaluation de l'application de celle-ci par les États membres et de ses effets sur les opérateurs économiques et les consommateurs, compte tenu de l'évolution de la technologie des communications électroniques et des statistiques transmises à la Commission, 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. Le présent rapport analyse également les effets de la directive sur les droits fondamentaux, compte tenu des critiques formulées, de manière générale, à l'encontre de la conservation des données 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[2].

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 contribution de la directive à l'harmonisation de la conservation des données a été restreinte en ce qui concerne, par exemple, la limitation des finalités et les durées de conservation, ainsi que pour le remboursement des coûts exposés par les opérateurs, qui ne relève pas de son champ d'application. Eu égard aux conséquences et aux risques pour le marché intérieur et pour le respect du droit à la vie privée et à la protection des données à caractère personnel, l'UE devrait continuer, grâce à des règles communes, à veiller à ce que des normes élevées soient constamment imposées au stockage, à l'extraction et à l'utilisation des données relatives au trafic et des données de localisation. Sur la base de ces conclusions, la Commission a l'intention de proposer des modifications de la directive après avoir procédé à une étude d'impact.

---

1 Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 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, JO L 105 du 13.4.2006, p. 54-63.

2 Conclusions du Conseil sur la lutte contre l'utilisation, à des fins criminelles, des communications électroniques et de leur anonymat, 2908e session du Conseil Justice et affaires intérieures, Bruxelles, 27-28 novembre 2008.

## 2. CONTEXTE DE L'EVALUATION

Le présent rapport d'évaluation repose sur des discussions approfondies avec les États membres, des experts et des parties prenantes, et sur des contributions qu'ils ont envoyées à la Commission.

En mai 2009, la Commission avait organisé une conférence intitulée «Towards the Evaluation of the Data Retention Directive» (Vers l'évaluation de la directive sur la conservation des données), à laquelle avaient participé des autorités chargées de la protection des données, le secteur privé, la société civile et des universitaires. En septembre 2009, elle a envoyé un questionnaire aux acteurs de ces différents groupes et a reçu près de 70 réponses[3]. La Commission a organisé une seconde conférence en décembre 2010 sur le thème «Taking on the Data Retention Directive» (le point sur la directive sur la conservation des données), à laquelle a assisté un éventail similaire de parties prenantes, en vue d'échanger des évaluations préliminaires de la directive et de discuter des défis à venir dans ce domaine.

Au cours de la période comprise entre octobre 2009 et mars 2010, la Commission a rencontré des représentants de chacun des États membres et pays associés de l'Espace économique européen afin d'examiner de façon plus approfondie des questions liées à l'application de la directive. Les États membres ont commencé à appliquer la directive plus tard que prévu, notamment en ce qui concerne les données liées à l'internet. Les retards intervenus dans la transposition de la directive ont fait que neuf États membres ont été en mesure de fournir à la Commission, pour l'année 2008 ou 2009, toutes les statistiques visées à l'article 10 de la directive, alors que dans l'ensemble, dix-neuf États membres n'ont fourni que des statistiques partielles (voir la section 4.7). La Commission a écrit aux États membres en juillet 2010, pour leur demander d'autres informations quantitatives et qualitatives sur la nécessité de conserver les données pour obtenir des résultats au niveau répressif. Dix États membres ont répondu en précisant les affaires pour lesquelles les données s'étaient révélées nécessaires[4].

Le présent rapport prend appui sur les documents de synthèse adoptés par la «Plateforme sur la conservation de données électroniques pour la recherche, la détection et la poursuite d'infractions pénales graves» depuis sa création en 2008[5]. La Commission a tenu compte des rapports du groupe de travail «Article 29» sur la protection des données[6], et notamment du rapport sur la deuxième action de contrôle de l'application de la législation, c'est-à-dire son

---

3 Les réponses ont été publiées sur le site internet de la Commission (http://ec.europa.eu/home-affairs/news/consulting_public/consulting_0008_en.htm - en anglais).

4 Belgique, République tchèque, Chypre, Lituanie, Hongrie, Pays-Bas, Pologne, Slovénie, Royaume-Uni. La Suède a également signalé plusieurs cas d'infractions graves dans lesquels l'historique des données relatives au trafic, qui étaient disponibles malgré l'absence d'obligation de conservation des données, a été déterminant pour faire condamner les auteurs.

5 Ce groupe d'experts a été établi en vertu de la décision 2008/324/CE de la Commission, JO L 111 du 23.04.2008, p. 11-14. La Commission a régulièrement rencontré ce groupe. Ses documents de synthèse sont publiés à l'adresse: http://ec.europa.eu/justice_home/doc_centre/police/doc_police_intro_en.htm(en anglais).

6 Le groupe de travail sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel a été établi en vertu de l'article 29 de la directive relative à la protection des données (directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, 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, JO L 281 du 23.11.1995, p. 31).

évaluation du respect des exigences de la directive en matière de protection et de sécurité des données par les États membres[7].

## 3. LA CONSERVATION DES DONNEES DANS L'UNION EUROPEENNE

### 3.1. La conservation des données à des fins judiciaires et policières

Dans le cadre de leur activité, les prestataires de services et les fournisseurs de réseaux (ci-après «les opérateurs») traitent des données à caractère personnel aux fins de la transmission d'une communication, de la facturation, des paiements pour interconnexion, de la prospection, et de certains autres services à valeur ajoutée. Ce traitement porte sur des données mentionnant la source, la destination, la date, l'heure, la durée et le type de communication, ainsi que le matériel de communication des utilisateurs et, dans le cas de la téléphonie mobile, des données relatives à la localisation de l'équipement. Conformément à la directive 2002/58/CE sur la vie privée et les communications électroniques (ci-après «la directive sur la vie privée»)[8], ces données relatives au trafic générées par l'utilisation des services de communication électronique doivent, en principe, être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication, hormis si et uniquement aussi longtemps qu'elles sont nécessaires à la facturation, ou si le consentement de l'abonné ou de l'utilisateur a été obtenu. Les données de localisation ne peuvent être traitées qu'après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés, dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée.

Avant l'entrée en vigueur de la directive, sous réserve de certaines conditions, les autorités nationales demandaient l'accès à ces données aux opérateurs, par exemple pour identifier des abonnés utilisant une adresse IP, analyser l'historique des communications et localiser un téléphone portable.

Au niveau de l'UE, la conservation et l'utilisation des données à des fins répressives ont d'abord été régies par la directive 97/66/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications. Dans un premier temps, la directive prévoyait que les États membres pouvaient prendre des mesures législatives lorsqu'elles sont nécessaires pour sauvegarder la sûreté de l'État, la défense ou l'ordre public, y compris la prospérité économique de l'État lorsque les activités concernaient la sûreté de l'État ou l'application du droit pénal[9].

---

7 Rapport 01/2010 sur la deuxième action commune de contrôle de l'application de la législation UE: Respect au niveau national par les fournisseurs de télécommunications et les fournisseurs de services Internet (FSI) des obligations découlant de la législation nationale sur la conservation des données relatives au trafic, sur la base juridique des articles 6 et 9 de la directive 2002/58/CE «vie privée et communications électroniques» et de la directive 2006/24/CE sur la conservation des données la modifiant (WP 172), 13 juillet 2010, disponible sur: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_fr.pdf.

8 Directive 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, JO L 201 du 31.7.2002, p. 37-47).

9 Article 14, paragraphe 1, de la directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications (JO L 24 du 30.1.1998, p. 1-8).

Cette disposition a été développée dans la directive sur la vie privée, qui permet aux États membres d'adopter des mesures législatives dérogeant au principe de confidentialité des communications, y compris, sous certaines conditions, la conservation, l'accès et l'utilisation de données à des fins répressives. Son article 15, paragraphe 1, autorise les États membres à restreindre les droits et les obligations en matière de vie privée, notamment par la conservation de données pendant une durée limitée, lorsque cela constitue une mesure «nécessaire, appropriée et proportionnée, au sein d'une société démocratique, 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 du système de communications électroniques».

Le rôle que jour les données conservées dans le système de justice pénale et le système répressif est discuté plus en détail à la section 5.

### 3.2. L'objectif et la base juridique de la directive sur la conservation des données

La directive 97/66/CE et la directive sur la vie privée, qui permettent aux États membres d'adopter des mesures législatives sur la conservation des données, ont eu pour conséquence que, dans certains États membres, les opérateurs ont dû acquérir des équipements pour conserver les donnés et affecter du personnel à la recherche de données pour le compte des autorités répressives, tandis que les opérateurs d'autres États membres n'avaient pas ces contraintes, ce qui a créé des distorsions sur le marché intérieur. De plus, en raison de l'évolution des modèles commerciaux et des offres de services, comme la multiplication des services de communications électroniques à forfait, prépayés et gratuits, les opérateurs ont progressivement cessé de stocker les données relatives au trafic et les données de localisation à des fins de facturation, réduisant ainsi la disponibilité de ces données à des fins judiciaires ou répressives. Les attentats terroristes de Madrid en 2004 et de Londres en 2005 ont accentué l'urgence de discuter au niveau de l'Union européenne des moyens de résoudre ces problèmes.

Dans ce contexte, la directive sur la conservation des données a imposé aux États membres de contraindre les prestataires de services de communications électroniques accessibles au public et de réseaux publics de communication à conserver les données relatives aux communications «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» et a tenté d'harmoniser certains problèmes connexes au niveau de l'UE.

La directive a modifié l'article 15, paragraphe 1, de la directive sur la vie privée, en ajoutant un paragraphe précisant que l'article 15, paragraphe 1, n'est pas applicable aux données dont la conservation est exigée par la directive sur la conservation des données[10]. Ainsi, les États membres (ainsi que le mentionne le considérant 12 de la directive) continuent de pouvoir déroger au principe de confidentialité des communications. La directive (sur la conservation

[10] L'article 11 de la directive est libellé comme suit: «À l'article 15 de la directive 2002/58/CE, le paragraphe suivant est inséré: "1 bis. Le paragraphe 1 n'est pas applicable aux données dont la conservation est spécifiquement exigée par la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques ou de réseaux publics de communication aux fins visées à l'article 1er, paragraphe 1, de ladite directive"».

des données) régit uniquement la conservation des données aux fins, plus limitées, de recherche, de détection et de poursuite d'infractions graves.

Cette relation juridique compliquée entre la directive et la directive sur la vie privée, à laquelle s'ajoute l'absence de définition, dans les deux instruments, de la notion d'«infraction grave», rend malaisée toute distinction entre, d'une part, les mesures prises par les États membres pour transposer les obligations relatives à la conservation des données énoncées dans la directive et, d'autre part, la pratique plus générale de conservation des données dans les États membres qu'autorise l'article 15, paragraphe 1, de la directive sur la vie privée[11]. Cet aspect est discuté plus en détail à la section 4.

La base juridique de la directive est l'article 95 du traité instituant la Communauté européenne (remplacé par l'article 114 du traité sur le fonctionnement de l'Union européenne) concernant l'établissement et le fonctionnement du marché intérieur. Après l'adoption de la directive, sa base juridique a été contestée devant la Cour de justice de l'Union européenne (ci-après la «Cour de justice») au motif que l'objectif premier était la recherche, la détection et la poursuite des infractions graves. La Cour de justice a jugé que la directive réglementait des opérations indépendantes de la mise en œuvre de toute éventuelle action de coopération policière et judiciaire en matière pénale et qu'elle n'harmonisait ni la question de l'accès aux données par les autorités nationales compétentes en matière répressive ni celle relative à l'utilisation et à l'échange de ces données entre ces autorités. Elle a dès lors conclu que la directive visait pour l'essentiel les activités des opérateurs dans le secteur concerné du marché intérieur et a donc confirmé la base juridique[12].

### 3.3. La conservation des données a posteriori

La simple conservation des données (*data retention*) se distingue de la conservation des données a posteriori (*data preservation*, également appelée «gel immédiat»), dans le cadre de laquelle des opérateurs ayant reçu une injonction judiciaire sont tenus de conserver des données portant uniquement sur des personnes déterminées soupçonnées d'une activité criminelle, à compter de la date de l'injonction de conservation. La conservation de données a posteriori est l'un des moyens d'enquête envisagés et utilisés par les États parties à la convention du Conseil de l'Europe sur la cybercriminalité[13]. La quasi-totalité des États parties ont désigné un point de contact, dont le rôle consiste à fournir une assistance immédiate dans les enquêtes ou procédures relatives à la cybercriminalité. Toutefois, toutes les parties à la convention ne semblent pas avoir prévu la conservation des données a posteriori, et l'efficacité de ce modèle dans la lutte contre la cybercriminalité n'a pas encore été évaluée[14]. Récemment, un mode de conservation des données a posteriori appelé «quick freeze plus» ou «gel immédiat plus» a été mis au point: sa nouveauté est que le juge peut également accorder

---

11 Le groupe de travail «Article 29» s'interroge: «la directive [sur la conservation des données] a-t-elle pour objet de permettre de déroger à l'obligation générale d'effacer les données relatives au trafic dès qu'elles ne sont plus nécessaires à la transmission d'une communication, ou bien de rendre obligatoire la conservation de toutes les données que les fournisseurs sont déjà autorisés à stocker pour leurs propres finalités commerciales».

12 Arrêt de la Cour de justice dans l'affaire C-301/6, Irlande/Parlement et Conseil, Recueil 2009, p. I-00593.

13 Article 16 de la convention sur la cybercriminalité (http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm) .

14 Source: Conseil de l'Europe.

l'accès à des données qui n'ont pas encore été effacées par les opérateurs. De plus, il comporterait une exemption légale très limitée de l'obligation d'effacer, pendant une courte période, certaines données de communication qui ne sont normalement pas stockées, telles que les données de localisation, celles concernant les connexions à l'internet, et les adresses IP dynamiques pour les utilisateurs ayant un abonnement forfaitaire ainsi que lorsqu'il n'est pas nécessaire de stocker des données pour la facturation.

Les partisans de la conservation des données a posteriori jugent ce mode moins intrusif que la simple conservation des données. En revanche, la plupart des États membres contestent que la conservation des données a posteriori, quelle que soit sa forme, puisse valablement remplacer la simple conservation des données, estimant que cette dernière met à disposition des données historiques, alors que la première ne garantit pas la possibilité de remonter en amont de l'injonction de conservation, pas plus qu'elle ne permet de recueillir des preuves sur les mouvements des victimes ou des témoins d'une infraction, par exemple[15].

## 4. LA TRANSPOSITION DE LA DIRECTIVE SUR LA CONSERVATION DES DONNEES

Les États membres étaient tenus de transposer la directive avant le 15 septembre 2007, avec la possibilité de reporter jusqu'au 15 mars 2009 la mise en œuvre des obligations de conservation relatives à l'accès à l'internet, au courrier électronique par l'internet et à la téléphonie par l'internet.

L'analyse développée ci-après repose sur les notifications de transposition envoyées à la Commission par 25 États membres, y compris la Belgique qui n'a que partiellement transposé la directive[16]. En Autriche et en Suède, les projets législatifs sont en cours d'examen. Dans ces deux États membres, il n'existe pas d'obligation de conserver les données, mais les autorités répressives ont la faculté de demander et d'obtenir des opérateurs des données relatives au trafic dans la mesure où ces données sont disponibles. Après que la République tchèque, l'Allemagne et la Roumanie ont notifié leurs mesures nationales de transposition de la directive, celles-ci ont été annulées par leurs cours constitutionnelles respectives[17], et les trois pays examinent maintenant comment procéder à une nouvelle transposition.

La présente section analyse la façon dont les États membres ont transposé les dispositions pertinentes de la directive dans leur droit interne. Elle se penche également sur la question de savoir si les États membres ont choisi de rembourser les opérateurs pour les coûts qu'ils

---

15 Ce fait a également été reconnu par la cour constitutionnelle allemande dans son arrêt annulant la loi transposant la directive (voir section 4.9) (Bundesverfassungsgericht, 1 BvR 256/08 du 2 mars 2010, point 208).

16 Les vingt-cinq États membres qui ont notifié la transposition de la directive à la Commission sont les suivants: Belgique, Bulgarie, République tchèque, Danemark, Allemagne, Grèce, Estonie, Irlande, Espagne, France, Italie, Chypre, Lettonie, Lituanie, Luxembourg, Hongrie, Malte, Pays-Bas, Pologne, Portugal, Roumanie, Slovénie, Slovaquie, Finlande et Royaume-Uni. La Belgique a informé la Commission que le projet de loi achevant la transposition est en cours d'examen au Parlement.

17 Décision n° 1258 du 8 octobre 2009 de la cour constitutionnelle roumaine, journal officiel roumain n° 789 du 23 novembre 2009; arrêt du Bundesverfassungsgericht 1 BvR 256/08 du 2 mars 2010; journal officiel du 1er avril 2011, arrêt de la cour constitutionnelle du 22 mars relatif aux dispositions de l'article 97, paragraphes 3 et 4, de la loi n° 127/2005 Coll. sur les communications électroniques et modifiant certaines lois connexes telles que modifiées, et décret n° 485/2005 Coll. sur la conservation et la transmission des données aux autorités compétentes.

supportent en conservant et en permettant l'extraction des données, un aspect que la directive ne prévoit pas, et elle étudie l'importance des arrêts des cours constitutionnelles allemande, roumaine et tchèque pour la directive.

### 4.1. Objet de la conservation des données (article premier)

La directive oblige les États membres à prendre des mesures en vue de garantir la conservation et la disponibilité des 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. Or, les finalités mentionnées dans la législation nationale pour la conservation des données et/ou l'accès à ces dernières varient toujours à l'intérieur de l'UE. Ainsi, dix États membres (Bulgarie, Estonie, Irlande, Grèce, Espagne, Lituanie, Luxembourg, Hongrie, Pays-Bas, Finlande) ont défini les «infractions graves» par référence à une peine minimale d'emprisonnement, à la possibilité d'une peine privative de liberté ou à une liste d'infractions pénales définies par ailleurs dans la législation nationale. Huit États membres (Belgique, Danemark, France, Italie, Lettonie, Pologne, Slovaquie, Slovénie) exigent que les données soient conservées non seulement à des fins de recherche, de détection et de poursuite d'infractions pénales graves, mais aussi pour toutes les infractions pénales et pour la prévention de la criminalité, ou pour des raisons générales de sécurité nationale, de sûreté de l'État et/ou de sécurité publique. La législation de quatre États membres (Chypre, Malte, Portugal et Royaume-Uni) fait référence à des «infractions pénales graves» ou à des «délits graves» sans les définir. Le tableau 1 présente le détail de la situation par pays.

| **Tableau 1: Limitation des finalités de la conservation des données dans le droit national** | |
|---|---|
| Belgique | Pour la poursuite et la répression d'infractions pénales, la répression d'appels malveillants vers les services d'urgence, la poursuite de l'utilisation malveillante d'un réseau ou d'un service de communications électroniques, et en vue de l'accomplissement des missions de renseignement des services de renseignement et de sécurité[18]. |
| Bulgarie | En vue de «découvrir et de poursuivre des infractions graves et les infractions relevant de l'article 319a à 319f du code pénal, et en vue de la recherche de personnes»[19]. |
| République tchèque | Directive non transposée. |
| Danemark | Pour la recherche et la poursuite d'infractions pénales[20]. |
| Allemagne | Directive non transposée. |

[18] Article 126, paragraphe 1, de la loi du 13 juin 2005 sur les communications électroniques. .

[19] Article 250 bis, paragraphe 2, de la loi sur les communications électroniques (modifiée) de 2010.

[20] Article 1er de l'ordonnance sur la conservation des données.

| Tableau 1: Limitation des finalités de la conservation des données dans le droit national | |
|---|---|
| Estonie | Autorisée si la recherche de preuves par d'autres actes de procédure est exclue ou particulièrement compliquée et si l'objet d'une procédure pénale est une infraction pénale [de premier degré, ou une infraction pénale de second degré commise intentionnellement et passible d'une peine privative de liberté d'au moins trois ans][21]. |
| Irlande | Pour la prévention d'infractions graves [c'est-à-dire des infractions passibles d'une peine d'emprisonnement de cinq ans ou plus, ou une infraction citée dans l'annexe de la loi de transposition], la sauvegarde de la sécurité de l'État et la préservation de la vie humaine.[22] |
| Grèce | Pour la détection des infractions particulièrement graves[23]. |
| Espagne | Pour la détection, la recherche et la poursuite des infractions pénales graves prévues par le code pénal ou par des lois pénales spécifiques[24]. |
| France | Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre la mise à disposition de l'autorité judiciaire des informations nécessaires, ainsi que pour la prévention d'actes de terrorisme et la protection de la propriété intellectuelle[25]. |
| Italie | Pour la détection et la répression d'infractions pénales[26]. |
| Chypre | Pour la recherche d'infractions pénales graves[27]. |
| Lettonie | Pour protéger l'État et la sécurité publique, ou aux fins de la recherche d'infractions pénales, de poursuites pénales ou de procédures pénales[28]. |
| Lituanie | Pour la recherche, la détection et la poursuite des infractions pénales graves et très graves, telles qu'elles sont définies dans le code pénal lituanien[29]. |

21 Article 110, paragraphe 1, du code de procédure pénale.

22 Article 6 de la *Communications (Retention of Data Act*) (loi sur les communications (conservation des données) de 2011.

23 Ces infractions sont définies à l'article 4 de la loi 2225/1994 et à l'article 1er de la loi 3917/2011.

24 Article 1er, paragraphe 1, de la loi n° 25/2007.

25 Les lois qui régissent l'utilisation des données conservées, respectivement, pour les infractions pénales, la prévention des actes de terrorisme et la protection de la propriété intellectuelle sont les suivantes: article L 34-1(II) du CPCE, loi n° 2006-64 du 23 janvier 2006 et loi n° 2009-669 du 12 juin 2009.

26 Article 132, paragraphe 1, du code de protection des données.

27 Article 4, paragraphe 1, de la loi 183(I)/2007.

28 Article 71, paragraphe 1, de la loi sur les communications électroniques.

29 Article 65 de la loi X-1835.

| Tableau 1: Limitation des finalités de la conservation des données dans le droit national | |
|---|---|
| Luxembourg | Pour les besoins de la recherche, de la constatation et de la poursuite d'infractions pénales qui emportent une peine criminelle dont le maximum est égal ou supérieur à un an d'emprisonnement[30]. |
| Hongrie | Pour permettre aux organismes d'enquête, au ministère public, aux cours et tribunaux et aux agences de sécurité nationale de remplir leur mission, et permettre à la police et à l'Office national des douanes d'enquêter sur les infractions intentionnelles passibles d'une peine d'emprisonnement égale ou supérieure à deux ans[31]. |
| Malte | Pour la recherche, la détection et la poursuite d'infractions graves[32]. |
| Pays-Bas | Pour la recherche et la poursuite des infractions graves passibles d'une peine privative de liberté[33]. |
| Autriche | Directive non transposée. |
| Pologne | Pour la prévention ou la recherche d'infractions, la prévention et la détection de délits fiscaux, pour les procureurs et juges si c'est nécessaire à la procédure en cours, pour l'exécution de la mission de l'agence de sécurité intérieure, de l'agence de renseignement étranger, du bureau central de lutte contre la corruption, des services de contre-espionnage militaire et des services de renseignement militaires[34]. |
| Portugal | Pour la recherche, la détection et la poursuite d'infractions graves[35]. |
| Roumanie | Directive non transposée. |
| Slovénie | Pour garantir la sécurité nationale, l'application de la constitution et la sécurité, les intérêts politiques et économiques de l'État … et pour la défense nationale[36]. |
| Slovaquie | Pour la prévention, la recherche, la détection et la poursuite des infractions pénales[37]. |

30 Article 1er, paragraphe 1, de la loi du 24 juillet 2010.

31 Pour la finalité générale de la conservation des données, article 159/A de la loi C/2003, modifiée par la loi CLXXIV/2007; en ce qui concerne l'accès accordé à la police, article 68 de la loi XXXIV/1994; en ce qui concerne l'accès accordé à l'Office national des douanes, article 59 de la loi CXXII/2010.

32 Article 20, paragraphe 1, de la loi modificative (*Avviż Legali*) 198 de 2008.

33 Article 126 du code de procédure pénale.

34 Article 180 bis de la loi du 16 juillet 2004 sur les télécommunications, tel que modifié par l'article 1er de la loi du 24 avril 2009.

35 Articles 1er et 3, paragraphe 1, de la loi n° 32/2008.

36 Article 170 bis, paragraphe 1, de la loi sur les communications électroniques.

| Tableau 1: Limitation des finalités de la conservation des données dans le droit national | |
|---|---|
| Finlande | Pour la recherche, la détection et la poursuite des infractions graves visées au chapitre 5a, article 3, paragraphe 1, de la loi sur les mesures coercitives[38]. |
| Suède | Directive non transposée. |
| Royaume-Uni | Pour la recherche, la détection et la poursuite d'infractions graves[39]. |

La plupart des États membres qui ont transposé la directive autorisent, dans leur législation, l'accès aux données conservées et leur utilisation pour des finalités dépassant celles couvertes par la directive, comme la prévention et la répression de la criminalité en général et les risques pour la vie humaine. Si la directive sur la vie privée autorise ce dépassement, le degré d'harmonisation obtenu par la législation de l'UE à cet égard demeure limité. Or, si les finalités de la conservation des données diffèrent d'un pays à l'autre, cela risque d'affecter le volume et la fréquence des demandes et, par conséquent, les coûts qu'implique le respect des obligations fixées par la directive. De plus, cette situation ne répondrait pas suffisamment à l'exigence de prévisibilité à laquelle est soumise toute mesure législative qui restreint le droit à la vie privée[40]. La Commission évaluera la nécessité d'une harmonisation plus poussée dans ce domaine et les options pour y parvenir[41].

### 4.2. Les opérateurs tenus de conserver les données (article premier)

La directive s'applique aux «fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications» (article 1er, paragraphe 1). Deux États membres (Finlande et Royaume-Uni) n'imposent pas aux petits opérateurs l'obligation de conserver les données parce que, selon eux, les coûts que cela représente tant pour le fournisseur que pour l'État dépasseraient les bénéfices pour les services répressifs et la justice pénale. Quatre États membres (Lettonie, Luxembourg, Pays-Bas et Pologne) déclarent avoir mis en place d'autres modalités administratives. Tandis que les grands opérateurs présents dans plusieurs États membres bénéficient d'économies d'échelle au niveau des coûts, les opérateurs de taille plus réduite ont tendance à créer des coentreprises ou à «externaliser» la conservation et l'extraction de données à des entreprises spécialisées afin de réduire leurs coûts. Cette externalisation de fonctions techniques ne remet pas en cause l'obligation des fournisseurs de contrôler comme il se doit les opérations de traitement et de veiller à ce que

---

37 Article 59 bis, paragraphe 6, de la loi sur les communications électroniques.

38 Article 14 bis, paragraphe 1, de la loi sur les communications électroniques.

39 *Data Retention (EC Directive) Regulations 2009* (Règlements de 2009 sur la conservation des données (directive CE) (2009 n° 859).

40 Arrêt de la Cour de justice du 20 mai 2003 dans les affaires jointes C-465/00, C-138/01 et C-139/01 (demande de décision préjudicielle du Verfassungsgerichtshof et l'Oberster Gerichtshof): Rechnungshof (C-465/00) contre Österreichischer Rundfunk et autres, et Christa Neukomm (C-138/01), Joseph Lauermann (C-139/01) contre Österreichischer Rundfunk (Protection des personnes physiques à l'égard du traitement de données à caractère personnel - Directive 95/46/CE - Protection de la vie privée - Divulgation des données sur les revenus de salariés d'entités soumises au contrôle du Rechnungshof).

41 Lors de l'adoption de la directive, la Commission avait publié une déclaration suggérant de retenir la liste des infractions figurant dans le mandat d'arrêt européen (décision-cadre 2002/584/JAI du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres).

les mesures de sécurité requises soient en place, ce qui peut poser des problèmes notamment aux opérateurs de taille plus modeste. La Commission examinera les questions relatives à la sécurité des données, et leur incidence sur les petites et moyennes entreprises, lorsqu'elle se penchera sur les possibilités envisageables pour modifier le cadre régissant la conservation des données.

### 4.3. Accès aux données: autorités compétentes, procédures et conditions (article 4)

Les États membres ont l'obligation de «veiller à ce que les données conservées […] ne soient transmises qu'aux autorités nationales compétentes, dans des cas précis et conformément au droit interne». Les États membres ont toute latitude pour définir dans leur droit national «la procédure à suivre et les conditions à remplir pour avoir accès aux données conservées dans le respect des exigences de nécessité et de proportionnalité, […] sous réserve des dispositions du droit de l'Union européenne ou du droit international public applicable en la matière, en particulier la Convention européenne des droits de l'homme telle qu'interprétée par la Cour européenne des droits de l'homme».

Dans tous les États membres, les forces nationales de police et, à l'exception des pays appliquant la *common law* (Irlande et Royaume-Uni), les procureurs peuvent avoir accès aux données conservées. Quatorze États membres citent les services de sécurité ou de renseignement ou l'armée parmi les autorités compétentes. Six États membres mentionnent les autorités fiscales et/ou douanières, et trois, les autorités frontalières. Un État membre accepte que d'autres autorités publiques aient accès aux données si elles y sont autorisées par le droit dérivé dans un but spécifique. Onze États membres soumettent à une autorisation judiciaire chaque demande d'accès à des données conservées. Dans trois États membres, l'autorisation du juge est requise dans la plupart des cas. Quatre autres États membres soumettent l'accès à l'autorisation d'une haute autorité, mais pas d'un juge. Dans deux États membres, la seule condition mise à l'accès semble être que la demande soit faite par écrit.

| **Tableau 2: Accès aux données de télécommunications conservées** | | |
|---|---|---|
| | *Autorités nationales compétentes* | *Procédures et conditions* |
| Belgique | Unité de coordination judiciaire, juges d'instruction, procureur, police judiciaire | L'accès doit être autorisé par un juge ou un procureur. Sur demande, les opérateurs doivent fournir les données sur l'abonné et les données de trafic et de localisation «en temps réel» pour les appels réalisés au cours du mois écoulé.<br>Les données concernant des communications plus anciennes doivent être fournies dans les meilleurs délais. |
| Bulgarie[42] | Directions et départements spécifiques de l'agence pour la sécurité nationale, ministère de l'intérieur, service du renseignement militaire, service de la police militaire, ministère de la défense, agence nationale d'enquête ; autorités judiciaires sous conditions. | Accès possible uniquement sur ordre du président d'une cour régionale. |
| République tchèque | Directive non transposée. | |

[42] Article 250b, paragraphe 1, de la loi sur les communications électroniques (modifiée) de 2010 (autorités); article 250b, paragraphe 1, et article 250c, paragraphe 1, de la loi sur les communications électroniques (modifiée) de 2010 (accès).

| Tableau 2: Accès aux données de télécommunications conservées | | |
|---|---|---|
| | *Autorités nationales compétentes* | *Procédures et conditions* |
| | | |
| Danemark[43] | Police. | Accès soumis à une autorisation judiciaire; une ordonnance du tribunal est rendue lorsque la demande répond à des critères stricts de suspicion, de nécessité et de proportionnalité. |
| Allemagne | Directive non transposée. | |
| Estonie[44] | Conseil national de la police et des gardes-frontières Conseil national de la police de sécurité et, pour les objets et les communications électroniques, Administration fiscale et douanière. | Accès soumis à l'autorisation d'un juge d'instruction.<br>Les opérateurs doivent «fournir [les données conservées], dans les cas urgents, au plus tard dans les 10 heures et, dans les autres cas, dans les 10 jours ouvrables [suivant la réception d'une demande]». |
| Irlande[45] | Membres de la Garda Síochána (police) ayant rang de Chief Superintendant ou un grade supérieur ; officiers de la *Permanent Defence Force* ayant rang de colonel ou un grade supérieur; fonctionnaires de l'administration fiscale (*Revenue Commissioners*) ayant rang de fonctionnaire en chef ou un grade supérieur | Les demandes doivent être écrites. |
| Grèce[46] | Autorités publiques judiciaires, militaires ou policières. | Accès soumis à une décision judiciaire déclarant que l'enquête par d'autres moyens est impossible ou extrêmement difficile. |
| Espagne[47] | Forces de police chargées de la détection, la recherche et la poursuite des infractions pénales graves, centre national du renseignement, et agence des douanes. | Accès à ces données par les autorités nationales compétentes soumis à une autorisation judiciaire préalable. |
| France[48] | Parquet, officiers de police et gendarmes désignés | La police doit motiver chaque demande d'accès à des données conservées et demander l'autorisation de la personne du ministère de l'intérieur désignée par la Commission nationale de contrôle des interceptions de sécurité.<br>Les demandes d'accès sont traitées par un responsable désigné travaillant pour l'opérateur. |
| Italie[49] | Procureur; police; avocat de la personne poursuivie ou visée par l'enquête. | Accès soumis à un «ordre motivé» délivré par le ministère public. |
| Chypre[50] | Juges, procureurs, police. | L'accès doit être autorisé par un procureur s'il estime qu'il pourrait apporter des preuves de la commission d'une infraction grave.<br>Un juge peut rendre une telle ordonnance s'il existe une suspicion raisonnable qu'une infraction pénale grave a été commise et si les données sont susceptibles d'avoir un lien avec |

43 Chapitre 71 de la loi sur l'administration de la justice.

44 Article 112, paragraphes 2 et 3, du code de procédure pénale (autorités et procédure); article 111, paragraphe 9, de la loi sur les communications électroniques.

45 Article 6 du *Communications (Retention of Data) Bill* de 2009 (projet de loi de 2009 sur les communications (conservation des données)).

46 Articles 3 et 4 de la loi 2225/94.

47 Articles 6 et 7 de la loi 25/2007.

48 Articles 60-1 et 60-2 du code de procédure pénale (autorités); article L.31-1-1 (conditions).

49 Article 132, paragraphe 3, du code de protection des données.

| Tableau 2: Accès aux données de télécommunications conservées | | |
|---|---|---|
| *Autorités nationales compétentes* | | *Procédures et conditions* |
| | | celle-ci. |
| Lettonie[51] | Agents autorisés des autorités chargées de l'instruction; enquêteurs; agents autorisés des organismes de sécurité nationale; parquet; cours et tribunaux. | Les agents autorisés, le parquet et les cours et tribunaux sont tenus d'évaluer «l'adéquation et la pertinence» de la demande, de l'enregistrer et de garantir la protection des données obtenues. Les instances autorisées peuvent conclure un accord avec un opérateur, pour le cryptage des données, par exemple. |
| Lituanie[52] | Autorités chargées de l'instruction, procureurs, cours et tribunaux (juges) et agents de renseignement | Les autorités publiques habilitées doivent demander les données conservées par écrit.<br>Pour l'accès aux données dans le cadre d'une instruction, un mandat judiciaire est requis. |
| Luxembourg[53] | Autorités judiciaires (juges d'instruction, procureurs), autorités chargées de la protection de la sûreté de l'État, de la défense, de la sécurité publique et de la prévention, de la recherche, la détection et la poursuite des infractions pénales | Accès soumis à une autorisation judiciaire. |
| Hongrie[54] | Police, administration fiscale et douanière nationale, agences de sécurité nationale, procureurs, cours et tribunaux. | La police et l'administration fiscale et douanière nationale doivent demander l'autorisation du procureur.<br>Les procureurs et les agences de sécurité nationale peuvent avoir accès à ces données sans présenter d'ordonnance d'un tribunal. |
| Malte[55] | police maltaise; service de sécurité. | Les demandes doivent être introduites par écrit. |
| Pays-Bas[56] | Enquêteurs | L'accès est soumis à une ordonnance d'un procureur ou d'un juge d'instruction. |
| Autriche | Directive non transposée. | |
| Pologne[57] | Police, gardes-frontières, inspection des impôts, agence de sécurité intérieure, agence de renseignements étrangers, bureau central de lutte contre la corruption, services de contre-espionnage militaires, services de renseignement militaires, cours et tribunaux, et procureurs. | Les demandes doivent être faites par écrit et, dans le cas de la police, des gardes-frontières et de l'inspection des impôts, elles doivent être autorisées par le fonctionnaire du rang le plus élevé de l'organisation. |
| Portugal[58] | Police judiciaire, garde nationale républicaine, office de sécurité publique, police judiciaire militaire, service d'immigration et des frontières, police maritime. | La transmission de données est subordonnée à une autorisation judiciaire constatant que l'accès est indispensable à la manifestation de la vérité ou que les preuves seraient impossibles ou très difficiles à obtenir de toute |

50 Article 4, paragraphes 2 et 4, de la loi 183(I)/2007.

51 Article 71, paragraphe 1, de la loi sur les communications électroniques (autorités); règlement n° 820 (procédures).

52 Article 77, paragraphes 1 et 2, de la loi X-1835; rapport oral à la Commission.

53 Article 5-2, paragraphe 1, et article 9, paragraphe 2, de la loi du 24 juillet 2010 (autorités); article 67-1 du code d'instruction criminelle (conditions).

54 Article 68, paragraphe 1, et article 69, paragraphe 1, points c) et d), de la loi XXXIV de 1994; article 9/A(1) de la loi V de 1972; article 71, paragraphes 1, 3, et 4, article 178/A, paragraphe 4, articles 200 et 201, et article 268, paragraphe 2, de la loi XIX de 1998; article 40, paragraphes 1 et 2, article 53, paragraphe 1, et article 54, paragraphe 1, point j), de la loi CXXV de 1995.

55 Article 20, paragraphes 1 et 3, de la loi modificative (*Avviż Legali*) 198 de 2008.

56 Article 126ni du code de procédure pénale.

57 Article 179, paragraphe 3, de la loi du 16 juillet 2004 sur les télécommunications, tel que modifié par l'article 1er de la loi du 24 avril 2009.

| Tableau 2: Accès aux données de télécommunications conservées | | |
|---|---|---|
| *Autorités nationales compétentes* | | *Procédures et conditions* |
| | | autre manière. La délivrance de l'autorisation judiciaire est soumise à des critères de nécessité et de proportionnalité. |
| Roumanie | Directive non transposée. | |
| Slovénie[59] | Police, agences de renseignement et de sécurité, agences de défense chargées du renseignement et du contre-espionnage et de missions de sécurité | Accès soumis à une autorisation judiciaire. |
| Slovaquie[60] | Autorités répressives, cours et tribunaux | Les demandes doivent être introduites par écrit. |
| Finlande[61] | Police, gardes-frontières, autorités douanières (pour les données conservées relatives à l'abonné, au trafic et à la localisation).<br>Centre d'intervention d'urgence, services de sauvetage en mer, sous-centre de sauvetage en mer (pour les données d'identification et de localisation en cas d'urgence) | Les données relatives à l'abonné peuvent être obtenues par toutes les autorités compétentes sans autorisation judiciaire.<br>Les autres données nécessitent une ordonnance d'un tribunal. |
| Suède | Directive non transposée. | |
| Royaume-Uni[62] | Police, services de renseignement, autorités fiscales et douanières, autres autorités publiques désignées dans le droit dérivé. | L'accès est autorisé, sous réserve d'une autorisation délivrée par une «personne désignée» et du respect des critères de nécessité et de proportionnalité, dans des cas spécifiques et dans des circonstances où la divulgation des données est autorisée ou requise par la loi. Des procédures spécifiques ont été convenues avec les opérateurs. |

La Commission évaluera la nécessité d'une harmonisation plus poussée, ainsi que les options pour y parvenir, en ce qui concerne les autorités ayant accès aux données conservées et la procédure à cet effet. Les options pourraient inclure des listes définissant plus clairement les autorités compétentes, un contrôle indépendant et/ou juridictionnel des demandes de données, et des procédures standards minimales pour l'octroi de l'accès aux autorités compétentes par les opérateurs.

### 4.4. Champ d'application de la conservation des données et catégories de données couvertes (article premier, paragraphe 2, article 3, paragraphe 2, et article 5)

La directive est applicable aux domaines de la téléphonie du réseau fixe, de la téléphonie mobile, de l'accès à l'internet, du courrier électronique par l'internet et de la téléphonie par

---

58 Article 2, paragraphe 1, article 3, paragraphe 2, et article 9 de la loi 32/2008.

59 Article 107c de la loi sur les communications électroniques; article 149b du code de procédure pénale; article 24(b) de la loi sur l'agence de renseignement et de sécurité; article 32 de la loi sur la défense.

60 Article 59a, paragraphe 8, de la loi sur les communications électroniques.

61 Article 35, paragraphe 1, et article 36 de la loi sur les communications électroniques; articles 31 à 33 de la loi sur la police; article 41 de la loi sur les services de surveillance des frontières.

62 Article 25, annexe 1, de la *Regulation of Investigatory Powers Act de 2000* (RIPA ou loi réglementant les pouvoirs d'enquête); article 7 du *Data Retention Regulation* (règlement sur la conservation des données). L'article 22, paragraphe 2, de la RIPA détermine les finalités pour lesquelles ces autorités peuvent obtenir des données.

l'internet. Elle précise, en son article 5, les catégories de données à conserver, à savoir celles nécessaires pour identifier:

(a) la source d'une communication;

(b) la destination d'une communication;

(c) la date, l'heure et la durée d'une communication;

(d) le type de communication;

(e) le matériel de communication des utilisateurs ou ce qui est censé être leur matériel ; et

(f) la localisation du matériel de communication mobile.

La directive (article 3, paragraphe 2) couvre également les appels téléphoniques infructueux, c'est-à-dire toute communication au cours de laquelle un appel téléphonique a été transmis mais est resté sans réponse ou a fait l'objet d'une intervention de la part du gestionnaire du réseau, et lorsque les données sur ces appels infructueux sont générées ou traitées, et stockées ou journalisées par les opérateurs. En vertu de la directive, aucune donnée révélant le contenu de la communication ne peut être conservée. Il a également été précisé ultérieurement que les requêtes de recherche, c'est-à-dire les journaux de serveurs générés par la fourniture d'un service de moteur de recherche, sont également exclues du champ d'application de la directive, car elles sont considérées comme des contenus plutôt que comme des données relatives au trafic[63].

Vingt-et-un États membres prévoient la conservation de chacune de ces catégories de données dans leur législation de transposition. La Belgique, elle, n'a pas précisé les types de données de téléphonie à conserver, pas plus qu'elle n'a prévu de dispositions concernant les données liées à l'internet. Les États qui ont répondu au questionnaire de la Commission n'ont pas jugé nécessaire de modifier les catégories de données à conserver, bien que le Parlement européen ait adressé une déclaration écrite à la Commission appelant à étendre la directive aux moteurs de recherche «pour contrer avec rapidité la pédopornographie et le harcèlement sexuel en ligne»[64]. Dans son rapport sur la deuxième action de contrôle de l'application de la législation de l'UE, le groupe "Article 29" soutenait que les catégories fixées dans la directive devraient être considérées comme exhaustives, et qu'il ne faudrait pas imposer aux opérateurs d'obligations supplémentaires de conservation des données. La Commission évaluera la nécessité de chacune de ces catégories de données.

### 4.5. Durées de conservation (articles 6 et 12)

Les États membres doivent veiller à ce que les catégories de données visées à l'article 5 soient conservées pendant une durée minimale de six mois et maximale de deux ans. La durée

---

63 Avis du groupe de travail «Article 29» sur les aspects de la protection des données liés aux moteurs de recherche, 4 avril 2008.

64 Déclaration écrite déposée conformément à l'article 123 du règlement sur la création d'un système d'alerte rapide européen (SARE) conte les pédophiles et les auteurs de harcèlements sexuels, 19.4.2010, 0029/2010.

maximale de conservation peut être prolongée par un État membre «confronté à des circonstances particulières justifiant une prolongation, pour une période limitée»; cette prolongation doit être notifiée à la Commission, laquelle peut, dans un délai de six mois suivant la notification, approuver ou rejeter la prolongation. Si la durée maximale peut être prolongée, aucune disposition ne prévoit la réduction de la durée de conservation en deçà de six mois. Tous les États membres qui ont transposé la directive, sauf un, appliquent une ou des durées de conservation comprises dans cette fourchette et la Commission n'a reçu aucune notification de prolongation. Toutefois, l'approche n'est pas harmonisée au sein de l'UE.

Quinze États membres prévoient une durée unique pour toutes les catégories de données: l'un d'eux (Pologne) prévoit une durée de deux ans, un autre fixe un an et demi (Lettonie), dix États prévoient un an (Bulgarie, Danemark, Estonie, Grèce, Espagne, France, Pays-Bas, Portugal, Finlande, Royaume-Uni) et trois États membres fixent six mois (Chypre, Luxembourg, Lituanie). Cinq États membres ont défini différentes durées de conservation selon les catégories de données: deux États membres (Irlande et Italie) prévoient deux ans pour les données de téléphonie fixe et mobile, et un an pour les données relatives à l'accès à l'internet, au courrier électronique par l'internet et à la téléphonie par l'internet; un État membre (Slovénie) prévoit 14 mois pour les données de téléphonie et 8 mois pour les données relatives à l'internet; un État membre (Slovaquie) prévoit un an pour les données de téléphonie fixe et mobile, et six mois pour les données relatives à l'internet ; un État membre (Malte) a fixé une durée de conservation d'un an pour les données de téléphonie fixe, mobile et par l'internet, et de six mois pour l'accès à l'internet et le courrier électronique par l'internet. Un État membre (Hongrie) conserve toutes les données pendant un an, à l'exception des données sur les appels téléphoniques infructueux, qui ne sont conservées que six mois. Un État (Belgique) n'a prévu aucune durée de conservation des données pour les catégories énumérées dans la directive. Le tableau 3 présente la situation en détail.

| **Tableau 3: Durées de conservation fixées dans la législation nationale** | |
|---|---|
| Belgique[65] | Entre 1 an et 36 mois pour les services téléphoniques «accessibles au public». Aucune disposition n'est prévue pour les données relatives à l'internet. |
| Bulgarie | 1 an. Les données auxquelles l'accès a été accordé peuvent être conservées six mois de plus sur demande. |
| République tchèque | Directive non transposée. |
| Danemark | 1 an |
| Allemagne | Directive non transposée. |
| Estonie | 1 an |
| Irlande | 2 ans pour les données de téléphonie fixe et mobile, 1 an pour les données relatives à l'accès à l'internet, au courrier électronique par l'internet et à la téléphonie par l'internet. |
| Grèce | 1 an |
| Espagne | 1 an |
| France | 1 an |
| Italie | 2 ans pour les données de téléphonie fixe et mobile, 1 an pour les données relatives à l'accès à l'internet, au courrier électronique par l'internet et à la téléphonie par l'internet. |
| Chypre | 6 mois |
| Lettonie | 18 mois |
| Lituanie | 6 mois |

[65] Article 126, paragraphe 2, de la loi du 13 juin 2005 sur les communications électroniques.

| Tableau 3: Durées de conservation fixées dans la législation nationale | |
|---|---|
| Luxembourg | 6 mois |
| Hongrie | 6 mois pour les appels téléphoniques infructueux et 1 an pour toutes les autres données |
| Malte | 1 an pour les données relatives à la téléphonie fixe, mobile et par l'internet, 6 mois pour les données relatives à l'accès à l'internet et au courrier électronique par l'internet |
| Pays-Bas | 1 an |
| Autriche | Directive non transposée. |
| Pologne | 2 ans |
| Portugal | 1 an |
| Roumanie | Directive non transposée (6 mois en vertu de la loi de transposition antérieure qui a été annulée) |
| Slovénie | 14 mois pour les données de téléphonie et 8 mois pour les données relatives à l'internet |
| Slovaquie | 1 an pour les données de téléphonie fixe et mobile, 6 mois pour les données relatives à l'accès à l'internet, au courrier électronique par l'internet et à la téléphonie par l'internet |
| Finlande | 1 an |
| Suède | Directive non transposée. |
| Royaume-Uni | 1 an |

Cette diversité d'approche est certes autorisée par la directive, mais celle-ci n'apporte dès lors qu'une sécurité et une prévisibilité juridiques limitées dans l'UE pour les opérateurs présents dans plusieurs États membres et pour les citoyens dont les données de communication sont susceptibles d'être stockées dans différents États membres. Compte tenu de l'internationalisation croissante du traitement des données et de l'externalisation de leur stockage, il conviendrait d'envisager des options pour harmoniser les durées de conservation des données dans l'UE. Afin de respecter le principe de proportionnalité, compte tenu des chiffres et des faits attestant l'utilité des données conservées dans les États membres, et eu égard à l'évolution des communications et des technologies, d'une part, et à celle de la criminalité et du terrorisme, d'autre part, la Commission envisagera de fixer différentes durées selon les catégories de données ou les catégories d'infractions graves, ou une combinaison de ces deux critères[66]. Les chiffres fournis à ce jour par les États membres concernant l'ancienneté des données conservées indiquent qu'environ 90 % d'entre elles datent de six mois ou moins et 70 % datent de trois mois ou moins lorsque la demande (initiale) d'accès est introduite par les autorités répressives (voir section 5.2).

### 4.6. Protection et sécurité des données et autorités de contrôle (articles 7 et 9)

La directive fait obligation aux États membres de veiller à ce que les opérateurs respectent, au minimum, quatre principes en matière de sécurité des données, à savoir que:

(a) les données conservées doivent être de la même qualité et soumises aux mêmes exigences de sécurité et de protection que les données sur le réseau [public de communications];

[66] La proposition de directive sur la conservation des données présentée par la Commission en 2005 prévoyait une durée de conservation d'un an pour les données relatives à la téléphonie et de six mois pour celles relatives à l'internet.

(b) les données fassent l'objet de mesures techniques et organisationnelles appropriées afin de les protéger contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle, ou le stockage, le traitement, l'accès ou la divulgation non autorisés ou illicites;

(c) les données fassent l'objet de mesures techniques et organisationnelles appropriées afin de garantir que seul un personnel spécifiquement autorisé y ait accès; et

(d) les données soient détruites lorsque leur durée de conservation prend fin, à l'exception des données auxquelles on a pu accéder et qui ont été conservées a posteriori [pour la finalité visée par la directive].

Conformément à la directive sur la protection des données et à la directive sur la vie privée, il est interdit aux opérateurs de traiter des données conservées au titre de la directive à d'autres fins, à condition que les données n'aient pas été conservées par ailleurs[67]. Les États membres doivent désigner une autorité publique chargée de surveiller, en toute indépendance, l'application de ces principes. Ces autorités peuvent être les mêmes que celles imposées par la directive sur la protection des données[68].

Quinze États membres ont transposé tous ces principes dans la législation pertinente. Quatre États membres (Belgique, Estonie, Espagne et Lettonie) ont transposé deux ou trois principes, mais ne prévoient pas explicitement la destruction des données à l'expiration de la période de conservation. Deux États membres (Italie et Finlande) prévoient la destruction des données. Il n'est toutefois pas clairement précisé quelles mesures de sécurité techniques et organisationnelles spécifiques, telles que l'authentification forte et une gestion détaillée du registre d'accès[69], ont été appliquées. Vingt-deux États membres ont désigné une autorité de contrôle chargée de surveiller l'application de ces principes. Dans la plupart des cas, ce rôle est dévolu à l'autorité chargée de la protection des données. Le tableau 4 présente la situation en détail.

**Tableau 4: Protection et sécurité des données et autorités de contrôle**

| *État membre* | *Dispositions relatives à la protection et à la sécurité des données en droit interne* | *Autorité de contrôle* |
|---|---|---|
| Belgique | Les opérateurs doivent garantir que la transmission de données ne puisse pas être interceptée par un tiers et se conformer aux normes ETSI en matière de sécurité des télécommunications et d'interception licite[70].<br>Le principe de destruction obligatoire à la fin de la période de conservation ne semble pas pris en compte. | Institut des services postaux et des télécommunications |

67 Article 13, paragraphe 1, de la directive 95/46/CE.

68 Article 28 de la directive 95/46/CE.

69 Une authentification forte repose sur un double mécanisme d'authentification, comme un mot de passe associé à de la biométrique ou un mot de passe doublé d'un code, afin de garantir la présence physique de la personne responsable du traitement des données relatives au trafic. La gestion détaillée du registre d'accès implique le suivi détaillé des accès et des traitements grâce à la conservation des registres mentionnant l'identité de l'utilisateur, l'heure d'accès et les fichiers auxquels l'utilisateur a eu accès.

70 Article 6 de l'arrêté royal du 9 janvier 2003.

| Tableau 4: Protection et sécurité des données et autorités de contrôle | | |
|---|---|---|
| *État membre* | *Dispositions relatives à la protection et à la sécurité des données en droit interne* | *Autorité de contrôle* |
| Bulgarie | La loi de transposition contient l'obligation d'appliquer les quatre principes[71]. | La commission chargée de la protection des données à caractère personnel surveille le traitement et le stockage des données afin de veiller au respect des obligations ; la commission parlementaire de l'assemblée nationale surveille les procédures d'autorisation et d'accès aux données. |
| République tchèque[72] . | Directive non transposée. | |
| Danemark | Les quatre principes sont prévus[73]. | L'agence nationale des TI et des télécommunications contrôle le respect de l'obligation faite aux fournisseurs de réseaux et de services de communications électroniques de veiller à ce que les équipements et systèmes techniques permettent à la police d'accéder aux informations sur le trafic des télécommunications. |
| Allemagne | Directive non transposée. | |
| Estonie | La loi de transposition contient trois des quatre principes. Aucune disposition ne mentionne explicitement le quatrième principe, mais toute personne ayant subi une atteinte à la vie privée par des activités liées à la surveillance peut demander en justice la destruction des données[74]. | L'instance responsable est l'autorité de surveillance technique. |
| Irlande[75] | La loi de transposition contient l'obligation d'appliquer les quatre principes. | Le juge désigné est habilité à enquêter et à faire un rapport sur le respect des dispositions de la loi de transposition par les autorités nationales compétentes. |
| Grèce[76] | La loi de transposition contient l'obligation d'appliquer les quatre principes, et impose en outre aux opérateurs d'établir et d'appliquer un plan assurant le respect des principes sous le contrôle d'un gestionnaire de la sécurité des donnés désigné. | Autorité chargée de la protection des données à caractère personnel et autorité chargée de la protection du secret des communications. |
| Espagne[77] | Les dispositions relatives à la sécurité des données contiennent trois des quatre principes (qualité et la sécurité des données conservées, accès par des personnes autorisées et protection contre un traitement illicite). | L'instance responsable est l'agence de la protection des données. |

71 Article 4, paragraphe 1, de la loi sur les communications électroniques (modifiée) de 2010.

72 Article 87, paragraphe 3, et article 88 de la loi 127/2005, telle que modifiée par la loi 247/2008; article 2 de la loi 336/2005; article 3, paragraphe 4, de la loi 485/2005; article 28, paragraphe 1, de la loi 101/2000.

73 Loi sur le traitement des données à caractère personnel ; arrêté n° 714 du 26 juin 2008 sur la fourniture de réseaux et services de communications électroniques.

74 Article 111, paragraphe 9, de la loi sur les communications électroniques; article 122, paragraphe 2, du code de procédure pénale.

75 Articles 4, 11 et 12 de la *Communications (Retention of Data) Act* de 2009 (loi sur les communications (conservation des données)).

76 Article 6 de la loi 3917/2011.

| Tableau 4: Protection et sécurité des données et autorités de contrôle | | |
|---|---|---|
| *État membre* | *Dispositions relatives à la protection et à la sécurité des données en droit interne* | *Autorité de contrôle* |
| France[78] | La loi de transposition contient l'obligation d'appliquer les quatre principes. | La Commission nationale de l'informatique et des libertés contrôle le respect de ces obligations. |
| Italie | Pas de dispositions explicites sur la sécurité des données conservées, bien qu'il existe une obligation générale de destruction ou d'anonymisation des données relatives au trafic et de traitement consensuel des données de localisation[79]. | L'autorité chargée de la protection des données contrôle le respect des dispositions de la directive par les opérateurs. |
| Chypre[80] | La loi de transposition consacre chacun des quatre principes. | Le commissaire chargé de la protection des données à caractère personnel surveille l'application de la loi de transposition. |
| Lettonie[81] | La loi de transposition consacre deux des quatre principes: confidentialité des données conservées et accès autorisé aux données conservées, ainsi que la destruction des données à la fin de la période de conservation. | L'inspection nationale des données contrôle la protection des données à caractère personnel dans le secteur des communications électroniques, mais pas l'accès aux données conservées ni leur traitement. |
| Lituanie[82] | La loi de transposition consacre les quatre principes. | L'inspection nationale de la protection des données contrôle l'application de la loi de transposition et est chargée de fournir des statistiques à la Commission européenne. |
| Luxembourg[83] | La loi de transposition consacre les quatre principes. | Autorité de protection des données. |
| Hongrie[84] | La loi de transposition consacre les quatre principes. | Commissaire parlementaire chargé de la protection des données et de la liberté de l'information. |
| Malte[85] | La loi de transposition consacre les quatre principes. | Commissaire à la protection des données. |
| Pays-Bas[86] | La loi de transposition consacre les quatre principes. | L'agence des radiocommunications contrôle le respect des obligations des fournisseurs de télécommunications et d'accès à l'internet; l'autorité de protection des données contrôle le traitement général des données à caractère personnel; un protocole détaille les modalités de la coopération entre les deux autorités. |

77 Article 8 de la loi 25/2007; article 38, paragraphe 3, de la loi générale sur les télécommunications. La loi (article 9) fait référence à la dérogation aux droits d'accès et de suppression énoncés dans la loi organique 15/1999 sur la protection des données à caractère personnel (articles 22 et 23).

78 Article D.98-5 du CPCE; article L-34-1(V) du CPCE; article 34 de la loi n° 78-17; article 34-1 du CPCE; article 11 de la loi n° 78-17 du 6 janvier 1978.

79 Articles 123 et 126 du code de protection des données.

80 Articles 14 et 15 de la loi 183(I)/2007.

81 Article 4, paragraphe 4, et article 71, paragraphes 6 à 8, de la loi sur les communications électroniques.

82 Article 12, paragraphe 5, et article 66, paragraphes 8 et 9, de la loi sur les communications électroniques, telle que modifiée le 14 novembre 2009.

83 Article 1er, paragraphe 5, de la loi du 24 juillet 2010.

84 Article 157 de la loi C/2003, telle que modifiée par la loi CLXXIV/2007; article 2 du décret 226/2003; loi LXIII/1992 sur la protection des données.

85 Articles 24 et 25 de la loi modificative 198/2008; article 40(b) de la loi sur la protection des données (Cap. 440).

86 Article 13, paragraphe 5, de la loi sur les télécommunications; Le titre complet du protocole de coopération est "Samenwerkingsovereenkomst tussen Agentschap Telecom en het College bescherming

| Tableau 4: Protection et sécurité des données et autorités de contrôle | | |
|---|---|---|
| *État membre* | *Dispositions relatives à la protection et à la sécurité des données en droit interne* | *Autorité de contrôle* |
| Autriche | Directive non transposée. | |
| Pologne | La loi de transposition consacre les quatre principes[87]. | Autorité de protection des données. |
| Portugal | La loi de transposition consacre les quatre principes[88]. | Autorité portugaise de protection des données. |
| Roumanie | Directive non transposée. | |
| Slovénie[89] | La loi de transposition consacre les quatre principes. | Commissaire à l'information. |
| Slovaquie[90] | La loi de transposition consacre les quatre principes. | Le régulateur national et l'autorité de fixation des prix dans le domaine des communications électroniques contrôlent la protection des données à caractère personnel. |
| Finlande | La loi de transposition n'impose explicitement que l'obligation de détruire les données à la fin de la période de conservation[91]. | L'autorité finlandaise de régulation des communications contrôle le respect de la réglementation sur la conservation des données par les opérateurs.<br>Le médiateur de la protection des données contrôle la légalité générale du traitement des données à caractère personnel. |
| Suède | Directive non transposée. | |
| Royaume-Uni | La loi de transposition consacre les quatre principes[92]. | Le commissaire à l'information contrôle la conservation et/ou le traitement des données relatives aux communications (et de toute autre donnée à caractère personnel) et procède aux contrôles appropriés en matière de protection des données.<br>Le commissaire à l'interception des communications (un juge de haut rang en exercice ou à la retraite) contrôle l'acquisition de données sur les communications par les autorités publiques au titre de la RIPA.<br>Le Investigatory Powers Tribunal traite les plaintes pour utilisation abusive de données acquises au titre de la législation de transposition (RIPA). |

La transposition de l'article 7 est inégale. Or, les données conservées pouvant revêtir un caractère extrêmement personnel et sensible, des normes strictes de protection et de sécurité doivent leur être appliquées tout au long du processus, pour le stockage, l'extraction et l'utilisation, de façon cohérente et transparente, afin de réduire au minimum le risque de violation de la vie privée et de préserver la confiance des citoyens. La Commission étudiera les options disponibles pour renforcer la sécurité des données et les normes assurant leur protection, notamment l'introduction de solutions respectant la vie privée dès la conception

---

persoonsgegevens met het oog op de wijzigingen in de Telecommunicatiewet naar aanleiding van de Wet bewaarplicht telecommunicatiegegevens".

87 Articles 180a et 180e de la loi sur les télécommunications.

88 Article 7, paragraphes 1 et 5, et article 11 de la loi 32/2008; articles 53 et 54 de la loi sur la protection des données à caractère personnel.

89 Article 107a, paragraphe 6, et article 107c de la loi sur les communications électroniques.

90 Article 59a de la loi sur les communications électroniques; article S33 de la loi n° 428/2002 sur la protection des données à caractère personnel.

91 Article 16, paragraphe 3, de la loi sur les communications électroniques;

92 Article 6 du règlement sur la conservation des données.

(«privacy by design») afin que ces critères soient respectés dans le cadre du stockage et de la transmission. Elle tiendra également compte des recommandations formulées par le groupe de travail «Article 29» dans son rapport sur la deuxième action de contrôle de l'application de la législation de l'UE[93], qui préconisent l'adoption de garanties minimales et de mesures de sécurité techniques et organisationnelles.

### 4.7. Statistiques (Article 10)

Les États membres doivent fournir à la Commission des statistiques annuelles sur la conservation des données. Ces statistiques comprennent notamment:

– les cas dans lesquels des informations ont été transmises aux autorités compétentes conformément à la législation nationale applicable,

– le délai 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 (c'est-à-dire l'ancienneté des données), et

– les cas dans lesquels des demandes de données n'ont pu être satisfaites.

En demandant des statistiques au titre de cette disposition, la Commission a invité les États membres à détailler les exemples de «demandes» individuelles de données. Néanmoins, les statistiques fournies variaient quant à leur portée et leur niveau de détail : dans leurs réponses, certains États membres ont établi une distinction entre différents types de communication, d'autres ont indiqué l'ancienneté des données au moment de la demande, tandis que d'autres encore n'ont fourni que des statistiques annuelles, sans la moindre ventilation. Dix-neuf États membres[94] ont transmis des statistiques sur le nombre de demandes de données en 2009 et/ou en 2008; parmi eux figuraient l'Irlande, la Grèce et l'Autriche, où des données ont été demandées malgré l'absence d'une législation de transposition à cette époque, ainsi que la République tchèque et l'Allemagne, dont la loi sur la conservation des données a été annulée. Sept États membres qui ont transposé la directive n'ont pas fourni de statistiques, la Belgique ayant toutefois communiqué une estimation du volume annuel de demandes de données sur la téléphonie (300 000).

Il est indispensable de disposer de données quantitatives et qualitatives fiables pour démontrer la nécessité et l'utilité de mesures de sécurité telles que la conservation des données. Le plan d'action de 2006 visant à établir des statistiques sur la criminalité et la justice pénale[95] a reconnu ce fait et il mentionnait parmi ses objectifs l'élaboration d'une méthodologie de collecte régulière des données, dans le respect de la directive, et l'inclusion des statistiques dans la base de données d'Eurostat (pour autant qu'elles satisfassent aux normes de qualité). Cet objectif n'a cependant pas pu être atteint car la plupart des États membres n'ont pleinement transposé la directive qu'au cours des deux dernières années et ont retenu des interprétations différentes de la source statistique. Dans sa future proposition visant à réviser

---

93 Avis 3/2006 du groupe de travail «Article 29» sur la protection des données (WP 119); rapport 01/2010.

94 République tchèque, Danemark, Allemagne, Estonie, Irlande, Grèce, Espagne, France, Chypre, Lettonie, Lituanie, Malte, Pays-Bas, Autriche, Pologne, Slovénie, Slovaquie, Finlande et Royaume-Uni.

95 Communication de la Commission, Élaboration d'une stratégie globale et cohérente de l'UE en vue de l'établissement de statistiques sur la criminalité et la justice pénale: Plan d'action de l'UE 2006 – 2010, COM(2006) 437.

le cadre régissant la conservation des données, ainsi que le plan d'action relatif aux statistiques, la Commission suggérera d'établir des critères de mesure réalistes et des procédures de rapport qui permettent un contrôle transparent et effectif de la conservation des données et qui n'imposent pas des charges indues aux systèmes de justice pénale et aux services répressifs.

### 4.8. La transposition dans les pays de l'EEE

Une législation sur la conservation des données existe en Islande, au Liechtenstein et en Norvège[96].

### 4.9. Les décisions des cours constitutionnelles sur les lois de transposition

Les cours constitutionnelles roumaine, allemande et tchèque ont annulé, respectivement en octobre 2009, mars 2010 et mars 2011, les lois transposant la directive en droit interne au motif qu'elles étaient inconstitutionnelles. La cour constitutionnelle roumaine[97] a admis qu'une ingérence dans l'exercice des droits fondamentaux pouvait être autorisée à condition que certaines règles soient respectées et que des garanties adéquates et suffisantes soient prévues pour protéger les citoyens contre une éventuelle action arbitraire de l'État. Toutefois, s'appuyant sur la jurisprudence de la Cour européenne des droits de l'homme[98], elle a jugé que le champ d'application et l'objet de la loi de transposition étaient ambigus et que les garanties étaient insuffisantes, et elle a déclaré qu'une «obligation juridique continue» de conserver toutes les données relatives au trafic pendant six mois était compatible avec le droit au respect de la vie privée et à la liberté d'expression consacré à l'article 8 de la convention européenne des droits de l'homme.

La cour constitutionnelle allemande[99] a déclaré que la conservation des données créait un sentiment de surveillance, qui pouvait entraver le libre exercice des droits fondamentaux. Elle a expressément reconnu que la conservation de données à des fins strictement limitées, assortie d'une sécurité des données suffisamment élevée, n'enfreindrait pas nécessairement la loi fondamentale allemande. Mais elle a souligné que la conservation de ces données constituait une grave restriction du droit à la vie privée et devait donc n'être admise que dans des circonstances extrêmement limitées, et qu'une durée de conservation de six mois était la limite maximale (*'an der Obergrenze')* de ce qui pouvait être considéré comme proportionné (point 215). Les données ne devaient être demandées que lorsqu'il existait déjà une suspicion d'infraction pénale grave ou une preuve d'un danger pour la sécurité publique, et l'extraction des données devrait être interdite pour certaines communications privilégiées (c'est-à-dire celles liées à un besoin affectif ou social), qui reposent sur la confidentialité. Les données devaient en outre être codées, avec un contrôle transparent de leur utilisation.

La cour constitutionnelle tchèque[100] a annulé la loi de transposition au motif que sa formulation n'était pas suffisamment claire et précise, ce qui constituait une atteinte aux droits

---

96 La loi transposant la directive en Islande est la loi sur les télécommunications 81/2003 (telle que modifiée en avril 2005); au Liechtenstein, la loi sur les télécommunications de 2006. En Norvège, la loi de transposition a été votée le 5 avril 2011 et attend actuellement la sanction royale.

97 Arrêt n° 1258 du 8 octobre 2009 de la cour constitutionnelle roumaine.

98 CEDH, Rotaru c. Roumanie 2000, Sunday Times c. Royaume-Uni 1979, et Prince Hans-Adam de Liechtenstein c. Roumanie 2001.

99 Bundesverfassungsgericht, 1 BvR 256/08, points 1 à 345.

100 Arrêt de la cour constitutionnelle tchèque du 22 mars relatif à la loi n° 127/2005 et au décret n° 485/2005; voir notamment les points 45 à 48, 50 à 51 et 56.

fondamentaux. La cour reprochait à la limitation de la finalité d'être insuffisante, eu égard à l'ampleur et à la portée de l'obligation de conservation des données. Elle estimait que la définition des autorités compétentes pour avoir accès aux données conservées et les utiliser, et les procédures à cet effet n'étaient pas assez claires dans la loi de transposition pour garantir l'intégrité et la confidentialité des données Dès lors, le citoyen ne disposait pas de garanties suffisantes contre d'éventuels abus de pouvoir des autorités publiques. Elle ne critiquait pas la directive en soi, estimant que cette dernière laissait suffisamment de latitude à la République tchèque pour la transposer dans le respect de sa constitution. Néanmoins, dans une opinion incidente, la cour exprimait ses doutes quant à la nécessité, à l'efficacité et au caractère approprié de la conservation des données relatives au trafic, en raison des nouvelles formes de criminalité telles que l'utilisation de cartes SIM anonymes.

Ces trois États membres examinent actuellement comment procéder à une nouvelle transposition de la directive. Des affaires relatives à la conservation des données ont également été portées devant la cour constitutionnelle bulgare, ce qui a entraîné une révision de la loi de transposition, devant la cour constitutionnelle chypriote, qui a jugé inconstitutionnelles les ordonnances des tribunaux rendues en vertu de la loi de transposition, et devant la cour constitutionnelle hongroise, où une affaire concernant l'absence de mention, dans la loi de transposition, des finalités juridiques du traitement des données, est pendante[101].

La Commission examinera les questions soulevées par la jurisprudence nationale dans sa future proposition visant à réviser le cadre régissant la conservation des données.

### 4.10. La mise en œuvre actuelle de la directive

La Commission entend que les États membres qui n'ont pas encore intégralement transposé la directive, ou qui n'ont pas encore adopté de législation remplaçant la loi de transposition annulée par les juridictions nationales, le fassent dès que possible. À défaut, elle se réserve le droit d'exercer les pouvoirs que lui confèrent les traités. À ce jour, deux États membres qui n'ont pas transposé la directive (l'Autriche et la Suède) ont été déclarés coupables de manquement aux obligations qui leur incombent en vertu du droit de l'UE par la Cour de justice[102]. En avril 2011, la Commission a décidé d'intenter un second recours contre la Suède devant la Cour pour inexécution de l'arrêt rendu dans l'affaire C-185/09, en demandant l'imposition de sanctions financières au titre de l'article 260 du traité sur le fonctionnement de l'Union européenne, à la suite d'une décision du parlement suédois de retarder de 12 mois l'adoption de la loi de transposition. La Commission continue de suivre de près la situation en Autriche, qui a communiqué un calendrier prévoyant l'adoption imminente de la loi de transposition.

## 5. LE ROLE DES DONNEES CONSERVEES DANS LA JUSTICE PENALE ET LA REPRESSION

Cette section résume les fonctions remplies par les données conservées, telles qu'elles ont été décrites par les États membres dans leurs contributions à l'évaluation.

---

101 Cour administrative suprême de Bulgarie, arrêt n° 13627 du 11 décembre 2008; cour suprême de Chypre, affaires n° 65/2009, 78/2009, 82/2009 et 15/2010-22/2010, 1er février 2011; le recours constitutionnel en Hongrie a été introduit par l'union hongroise pour le libertés civiles, le 2 juin 2008.

102 Affaires C-189/09 et C-185/09, respectivement.

### 5.1. Volume des données conservées auxquelles les autorités nationales compétentes ont eu accès

Le volume du trafic des télécommunications et des demandes d'accès à des données y afférentes ne cesse d'augmenter. Les statistiques transmises par 19 États membres pour 2008 et/ou 2009 indiquent que, dans l'ensemble de l'UE, plus de deux millions de demandes de données ont été introduites chaque année, avec des fluctuations sensibles selon les États, le nombre de demandes variant de moins d'une centaine par an (Chypre) à plus d'un million (Pologne). Selon les informations sur le type de données demandées qui ont été communiquées par douze États membres pour 2008 ou 2009, le type le plus fréquemment demandé concernait la téléphonie mobile (voir les tableaux 5, 8 et 12). Ces statistiques n'indiquent toutefois pas le but précis dans lequel chaque demande a été introduite. La République tchèque, la Lettonie et la Pologne ont mentionné que, pour les données relatives à la téléphonie mobile, les autorités compétentes devaient adresser la même demande à chacun des grands opérateurs concernés, de sorte que le nombre réel de demandes par affaire était donc considérablement inférieur à celui indiqué par les statistiques.

Il n'existe pas d'explication évidente à ces variations, bien que la taille de la population, les tendances dans la prévalence des infractions, les limitations imposées aux finalités, les conditions d'accès et les coûts d'acquisition des données soient autant de facteurs à prendre en compte.

### 5.2. Ancienneté des données conservées auxquelles un accès a été donné

Les chiffres ventilés fournis par neuf États membres[103] pour 2008 (voir le résumé dans le tableau 5 et d'autres détails à l'annexe) montrent qu'environ 90 % des données auxquelles les autorités compétentes ont eu accès cette année-là dataient de six mois ou moins, et que près de 70 % dataient de trois mois ou moins lorsque la demande (initiale) d'accès a été introduite.

**Tableau 5: Aperçu de l'ancienneté des données conservées auxquelles un accès a été donné dans neuf États membres ayant transmis une ventilation par type de données en 2008**

| *Ancienneté* | *Téléphonie fixe* | *Téléphonie mobile* | *Internet* | *Agrégat* |
|---|---|---|---|---|
| Moins de 3 mois | 61% | 70% | 56% | 67% |
| 3 à 6 mois | 28% | 18% | 19% | 19% |
| 6 à 12 mois | 8% | 11% | 18% | 12% |
| Plus d'un an | 3% | 1% | 7% | 2% |

Selon les États membres, l'utilisation de données conservées de plus de 3 mois, voire de 6 mois, est moins fréquente mais peut être cruciale; leur utilisation tend à se classer en trois catégories. Premièrement, les données relatives à l'internet sont généralement demandées plus tard que d'autres formes de preuve dans le cadre d'enquêtes judiciaires. L'analyse des données de téléphonie fixe et mobile aboutit souvent à des indices potentiels, qui entraînent de nouvelles demandes de données plus anciennes. Par exemple, si, au cours d'une enquête, un nom apparaît dans les données de téléphonie fixe ou mobile, les enquêteurs pourraient vouloir identifier l'adresse IP utilisée par cette personne et les individus avec lesquels elle a été en

[103] République tchèque, Danemark, Estonie, Irlande, Espagne, Chypre, Lettonie, Malte, Royaume-Uni.

contact pendant une période donnée, par le biais de cette adresse IP. Dans un tel cas, il est probable que les enquêteurs demanderont les données leur permettant de retracer également des communications avec d'autres adresses IP et l'identité des utilisateurs de ces dernières.

Deuxièmement, les enquêtes relatives à des infractions particulièrement graves, à une série de crimes, à la criminalité organisée et aux attentats terroristes s'appuient généralement sur des données conservées plus anciennes qui reflètent le temps pris à préparer ces infractions, afin de déceler des comportements délictueux et des liens entre les complices d'une infraction, et d'établir l'intention délictueuse. Les activités liées à des infractions financières sophistiquées ne sont souvent détectées qu'après plusieurs mois. Troisièmement, et à titre d'exception, des États membres ont demandé des données relatives au trafic détenues dans un autre État membre qui ne peut normalement publier ces données qu'avec l'autorisation d'un juge, en réponse à une commission rogatoire délivrée par un juge dans l'État membre requérant. Ce type d'entraide judiciaire peut prendre du temps, ce qui explique pourquoi certaines des données demandées avaient plus de six mois.

### 5.3. Les demandes transfrontalières de données conservées

Les enquêtes judiciaires et les poursuites pénales peuvent faire intervenir des événements survenus, ou des preuves et des témoins se trouvant, dans plusieurs États membres. D'après les statistiques fournies par les États membres, moins de 1 % des demandes de données conservées portait sur des données provenant d'autres États membres. Les services répressifs indiquaient qu'ils préféraient demander des données aux opérateurs nationaux susceptibles d'avoir stocké les données pertinentes plutôt que lancer une procédure d'entraide judiciaire qui peut durer longtemps sans aucune garantie d'obtenir l'accès aux données. La décision-cadre 2006/960/JAI relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres[104], qui fixe des délais pour la fourniture d'informations en réponse à une demande d'un autre État membre, n'est pas applicable parce que les données conservées sont considérées comme des informations obtenues par des moyens coercitifs ne relevant pas du champ d'application de cet instrument. Néanmoins, aucun État membre ou service répressif n'a demandé une nouvelle simplification de ces échanges transfrontaliers.

### 5.4. L'utilité des données conservées pour les enquêtes judiciaires et les poursuites pénales

Bien que le nombre absolu de demandes de données communiqué ne traduise pas nécessairement l'utilité des données dans les enquêtes judiciaires, les États membres ont généralement mentionné que la conservation des données était au moins utile et, dans certains cas, indispensable[105] à la prévention et à la répression des infractions, y compris pour protéger des victimes et faire acquitter des innocents dans les procédures pénales. Pour aboutir à des

---

104 Décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne, JO L 386 du 29.12.2006, p. 89-100, et JO L 200 du 1.8.2007, p. 637-648.

105 La République tchèque considérait la conservation des données «absolument indispensable dans un grand nombre de cas»; la Hongrie disait qu'elle était «indispensable aux activités régulières [des services répressifs]»; la Slovénie affirmait que l'absence de données conservées «paralyserait le fonctionnement des services répressifs»; un service de police britannique disait des données relatives au trafic qu'elles étaient «absolument déterminantes… pour les enquêtes sur les menaces terroristes et les infractions graves .

condamnations, il faut des aveux de culpabilité, des déclarations de témoins ou des preuves scientifiques. Il a été signalé que les données de trafic conservées s'étaient révélées nécessaires pour contacter des témoins d'un incident qui, sans cela, n'auraient pas été identifiés et pour apporter des preuves ou des indices permettant d'établir la complicité dans une infraction. Certains États membres[106] ont également affirmé que l'utilisation des données conservées avait permis de mettre hors de cause des personnes soupçonnées, sans devoir recourir à d'autres méthodes de surveillance, telles que l'interception de communications et la perquisition, susceptibles d'être jugées plus intrusives.

Comme il n'existe aucune définition générale des «infractions graves» dans l'Union, aucune statistique européenne n'est disponible sur leur incidence ou sur celle des enquêtes ou poursuites dont elles font l'objet, alors que des données sur la criminalité et la justice sont régulièrement publiées. Le nombre total de demandes de données conservées déclarées par les 19 États membres qui ont fourni des chiffres pour 2009 et/ou 2008 s'établissait à quelque 2,6 millions. Par rapport aux dernières statistiques disponibles sur la criminalité et la justice pénale pour ces 19 États membres (qui concernent toutes les infractions signalées, et non uniquement les infractions graves), on peut dire qu'il y a un peu plus de deux demandes par policier et par an, ou environ 11 demandes pour 100 infractions enregistrées[107].

Les statistiques et les exemples fournis, qui établissent un lien entre l'utilisation des données historiques conservées sur les communications et le nombre de condamnations, d'acquittements, d'affaires classées et d'infractions prévenues, permettent de tirer une série de conclusions sur le rôle et l'utilité des données conservées pour les enquêtes judiciaires.

*Établir des faisceaux de preuves*

Premièrement, les données conservées permettent d'établir des faisceaux de preuves qui conduisent à un délit. Elles servent à discerner les activités et les liens entre des suspects, ou à corroborer d'autres formes de preuves qui y ont trait. Les données de localisation, notamment, ont été utilisées par les services répressifs et les personnes poursuivies pour exclure des suspects des scènes de crime et vérifier des alibis. Ces preuves peuvent donc écarter des personnes d'une enquête judiciaire, éliminant ainsi la nécessité de procéder à des recherches plus intrusives, ou entraîner un acquittement dans un procès. La Belgique a ainsi cité la condamnation, en 2008, des preneurs d'otage d'un employé du tribunal d'Anvers; dans cette affaire, les données de localisation reliant les activités des malfrats dans trois villes différentes ont été déterminantes pour convaincre le jury de leur complicité. Dans une autre affaire concernant un meurtre lié à une bande de motards en 2007, les données de localisation des téléphones portables des auteurs ont prouvé qu'ils étaient dans la zone où le meurtre avait été commis et elles ont conduit à des aveux partiels[108]. La Belgique, l'Irlande et le Royaume-Uni affirment que les enquêtes sur certaines infractions impliquant des communications par l'internet *sont impossibles* si l'on ne recourt pas à la conservation des données : par exemple,

---

106 Allemagne, Pologne, Slovénie et Royaume-Uni.

107 En 2007, l'UE-27 comptait 1,7 million de policiers, dont 1,2 million dans les 19 États membres qui ont fourni des statistiques sur les demandes de données conservées. La même année, 29,2 millions d'infractions ont été enregistrées par les polices de l'UE, dont 24 millions dans les 19 États membres ayant fourni des statistiques. (Source: Eurostat 2009)

108 National Policing Improvement Agency (UK), *The Journal of Homicide and Major Incident Investigation*, Volume 5, Issue 1, Spring 2009, p. 39-51.

les menaces de violence dans les groupes de discussion ne laissent souvent pas d'autre trace que les données relatives au trafic dans le cyberespace. Il en est de même des infractions commises par voie téléphonique. La Hongrie et la Pologne citaient le cas d'une escroquerie perpétrée auprès de personnes âgées, fin 2009-début 2010, à l'occasion d'appels téléphoniques au cours desquels les auteurs se présentaient comme des membres de la famille ayant besoin d'emprunter de l'argent. Ils ont pu être identifiés grâce aux données de téléphonie conservées.

*Ouvrir une enquête judiciaire*

Deuxièmement, des cas ont été recensés où, en l'absence de toute preuve scientifique ou de témoin oculaire, le seul moyen d'ouvrir une enquête judiciaire résidait dans la consultation de données conservées. L'Allemagne a cité l'exemple du meurtre d'un policier, où l'assaillant s'était échappé dans le véhicule de la victime, pour ensuite l'abandonner. Il a été possible d'établir qu'il avait alors téléphoné pour trouver un autre moyen de transport. Il n'existait aucune preuve scientifique de l'identité du meurtrier ni aucun témoin oculaire, et les autorités dépendaient de la disponibilité de ces données de trafic pour pouvoir poursuivre leur enquête. Dans des affaires de pédopornographie infantile sur internet, la conservation des données a été indispensable au succès des enquêtes. En effet, parallèlement aux autres techniques d'enquête, les données conservées ont permis d'identifier des consommateurs de contenus pédopornographiques[109], ainsi que des enfants victimes, qui ont ainsi pu être sauvés. La République tchèque indiquait que, sans l'accès aux données relatives à l'internet conservées, il aurait été impossible de commencer les recherches dans le cadre de «l'opération Vilma» lancée contre un réseau d'utilisateurs et de diffuseurs de pornographie enfantine. Au niveau de l'Union, l'efficacité de l'opération Rescue (coordonnée par Europol) pour protéger les enfants contre les pédophiles a été freinée parce que le défaut de transposition de la législation sur la conservation des données a empêché certains États membres d'enquêter sur les membres d'un large réseau pédophile international utilisant des adresses IP, dont l'ancienneté pourrait remonter jusqu'à un an.

Dans les enquêtes sur la cybercriminalité, le premier indice est souvent une adresse IP. Les services répressifs peuvent, grâce à l'extraction des données de trafic, identifier l'abonné qui se cache derrière cette adresse avant de déterminer si une enquête judiciaire peut être ouverte. Cela peut également permettre à la police de prévenir des victimes potentielles de cyberattaques: lorsque la police parvient à saisir un serveur de commande et contrôle utilisé par les opérateurs d'un botnet, elle ne peut voir que les adresses IP liées à ce serveur, mais en accédant aux données conservées, elle peut identifier et avertir les victimes potentielles qui possèdent ces adresses IP.

*Les données conservées font partie intégrante de l'enquête judiciaire*

Troisièmement, si les services répressifs et les juridictions de la plupart des États membres ne tiennent pas de statistiques sur le type de preuves qui se sont révélées capitales pour obtenir des condamnations ou des acquittements, les données conservées, elles, font partie intégrante

---

[109] Le projet intitulé "Measurement and analysis of p2p activity against paedophile content", financé par le programme Safer Internet, a produit des informations précises sur l'activité des pédophiles dans le système peer-to-peer eDonkey, permettant ainsi l'identification de 178 000 utilisateurs (sur 89 millions d'utilisateurs vérifiés) qui ont demandé un contenu pédophile.

de l'enquête judiciaire et des poursuites pénales dans l'UE. Certains États membres ont indiqué qu'il ne leur était pas toujours possible d'isoler l'impact des données conservées sur l'aboutissement positif des enquêtes judiciaires et des poursuites pénales, parce que le juge prend en considération l'ensemble des preuves qui lui sont présentées et conclut rarement qu'un élément de preuve particulier a été déterminant[110]. Les Pays-Bas ont rapporté qu'entre janvier et juillet 2010, les données historiques relatives au trafic ont été un facteur décisif dans 24 décisions judiciaires. La Finlande a signalé que dans 56 % des 3405 demandes, les données conservées se sont révélées «importantes» ou «essentielles» pour la détection et/ou la poursuite d'infractions pénales. Le Royaume-Uni a fourni des données visant à quantifier l'impact de la conservation des données sur les poursuites pénales. Selon les autorités britanniques, pour trois de ses services répressifs, des données conservées ont été nécessaires dans la plupart, voire toutes les enquêtes ayant abouti à des poursuites pénales ou à une condamnation.

### 5.5. Les évolutions technologiques et l'utilisation des cartes SIM prépayées

La répression doit suivre le rythme des évolutions technologiques permettant de commettre ou d'encourager une infraction. La conservation des données fait partie de l'arsenal d'enquête judiciaire nécessaire aux services répressifs pour faire face, de façon gérable et rentable, aux défis que pose la criminalité contemporaine en termes de diversité, de volume et de rapidité. Plusieurs modes de communication de plus en plus courants ne sont pas couverts par le champ d'application de la directive. Les réseaux privés virtuels des universités ou des grandes entreprises, par exemple, permettent à plusieurs utilisateurs de se connecter à l'internet par un point d'accès unique utilisant la même adresse IP. Or, on assiste actuellement à l'émergence d'une nouvelle technologie qui permet d'attribuer des adresses à des utilisateurs individuels de réseaux privés virtuels.

La proportion d'utilisateurs de téléphonie mobile qui utilisent des services prépayés fluctue à l'intérieur de l'Union européenne. Quelques États membres ont déclaré que les cartes SIM prépayées anonymes, surtout lorsqu'elles sont achetées dans un autre État membre, pourraient également être utilisées par des criminels pour éviter d'être identifiés dans le cadre d'une enquête judiciaire[111]. Six États membres (Danemark, Espagne, Italie, Grèce, Slovaquie et Bulgarie) ont adopté des mesures imposant l'enregistrement des cartes SIM prépayées. Ces États membres et quelques autres (Pologne, Chypre, Lituanie) se sont prononcés en faveur de l'adoption d'une mesure à l'échelle européenne rendant obligatoire l'identification des utilisateurs de services prépayés. Aucune preuve de l'efficacité de ces mesures nationales n'a cependant été apportée. Leurs limites potentielles ont été mises en évidence, comme dans les cas d'usurpation d'identité ou lorsqu'une carte SIM est achetée par un tiers ou qu'un utilisateur pratique l'itinérance avec une carte achetée dans un pays tiers. Globalement, la Commission n'est pas convaincue de la nécessité d'agir dans ce domaine au niveau européen pour l'instant.

---

110 Belgique, République tchèque et Lituanie.

111 Conclusions du Conseil sur la lutte contre l'utilisation, à des fins criminelles, des communications électroniques et de leur anonymat.

## 6. L'IMPACT DE LA CONSERVATION DES DONNEES SUR LES OPERATEURS ET LES CONSOMMATEURS

### 6.1. Les opérateurs et les consommateurs

Dans une déclaration conjointe adressée à la Commission, cinq grandes associations du secteur ont affirmé que l'impact économique de la directive était «considérable» ou «énorme» pour les «fournisseurs de services de taille plus réduite», parce que la directive laisse une «grande marge de manœuvre»[112]. Huit opérateurs ont présenté des estimations très divergentes du coût, en termes de capital et de dépenses opérationnelles, qu'implique le respect de la directive. Ces affirmations pourraient être confirmées par les niveaux de remboursement des coûts supportés par les opérateurs qui ont été communiqués par quatre des États membres (voir le tableau 6).

Une étude réalisée avant la transposition de la directive dans la plupart des États membres estimait le coût de mise en place d'un système de conservation de données pour un fournisseur de services internet comptant un demi-million de clients à environ 375 240 EUR la première année, et 9 870 EUR de coûts d'exploitation par mois ensuite[113], et les coûts de mise en place d'un système d'extraction de données à 131 190 EUR, les coûts d'exploitation s'élevant à 28 960 EUR par mois. La cour constitutionnelle allemande a toutefois conclu dans son arrêt du 2 mars 2010 que l'imposition d'une obligation de stockage n'était «pas particulièrement ou excessivement lourde pour les fournisseurs de services concernés [ni] disproportionnée au regard des charges financières assumées par les entreprises du fait de l'obligation de stockage»[114]. Les coûts de conservation des données par unité sont inversement proportionnels à la taille de l'opérateur et au niveau de normalisation des rapports d'un État membre avec les opérateurs[115].

Dans leur réponse au questionnaire de la Commission, la plupart des opérateurs étaient incapables de quantifier les répercussions de la directive sur la concurrence, les prix au détail pour les consommateurs ou les investissements dans de nouvelles infrastructures et services.

Il n'existe aucune preuve d'un quelconque effet quantifiable ou considérable de la directive sur les prix à la consommation des services de communications électroniques; aucune contribution à la consultation publique de 2009 n'a été envoyée par des représentants de consommateurs. Un sondage réalisé en Allemagne pour le compte d'une organisation appartenant à la société civile indiquait que les consommateurs avaient l'intention de changer leurs habitudes de communication et d'éviter d'utiliser les services de communications électroniques dans certaines circonstances, mais aucun élément n'indique qu'il y a eu un quelconque changement de comportement dans les États membres concernés ou dans l'Union européenne en général[116].

---

112 http://www.gsmeurope.org/documents/Joint_Industry_Statement_on_DRD.PDF

113 Wilfried Gansterer & Michael Ilger, Data retention – The EU Directive 2006/24/EC from a Technological Perspective, Wien: Verlag Medien und Recht, 2008.

114 Bundesverfassungsgericht, 1 BvR 256/08 du 2 mars 2010, point 299.

115 http://www.etsi.org/website/technologies/lawfulinterception.aspx (en anglais)

116 Le sondage a été réalisé par Forsa et commandité par AK Vorratsdatenspeicherung. http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf

La Commission entend évaluer les effets des futures modifications de la directive sur le secteur et sur les consommateurs, éventuellement par un sondage Eurobaromètre spécial pour mesurer la perception du public.

### 6.2. Le remboursement des coûts

La directive ne régit pas le remboursement des coûts supportés par les opérateurs du fait de l'obligation de conservation des données. Ces coûts peuvent être définis comme étant:

(a) les *dépenses d'exploitation*, c'est-à-dire les coûts d'exploitation ou les dépenses récurrentes qui sont liés à l'exploitation de l'entreprise, d'un dispositif, d'un composant, d'un équipement ou d'une installation, et

(b) les *dépenses en capital*, c'est-à-dire les dépenses qui génèrent des bénéfices futurs ou le coût du développement ou de la fourniture d'éléments non consommables pour le produit ou le système, pouvant inclure le coût du personnel et les dépenses liées à l'installation, comme le loyer ou les services d'utilité publique.

Tous les États membres prévoient une forme de remboursement lorsque les données sont demandées dans le cadre d'une procédure pénale devant un tribunal. Deux États membres ont déclaré rembourser à la fois les dépenses d'exploitation et les dépenses en capital. Six autres ne remboursent que les dépenses d'exploitation. Aucun autre régime de remboursement n'a été notifié à la Commission. Le tableau 6 présente la situation en détail.

**Tableau 6: États membres qui remboursent les coûts**

| État membre | Dépenses d'exploitation | Dépenses en capital | Coûts de remboursement annuels (en millions d'EUR) |
|---|---|---|---|
| Belgique | Oui | Non | 22 (2008) |
| Bulgarie | Non | Non | - |
| République tchèque | Directive non transposée[117]. | | |
| Danemark | Oui | Non | - |
| Allemagne | Directive non transposée. | | |
| Estonie | Oui | Non | - |
| Irlande | Non | Non | - |
| Grèce | Non | Non | - |
| Espagne | Non | Non | - |
| France | Oui | Non | - |
| Italie | - | - | - |
| Chypre | Non | Non | - |
| Lettonie | Non | Non | - |
| Lituanie | Oui, si demandées et justifiées. | Non | - |
| Luxembourg | Non | Non | - |
| Hongrie | Non | Non | - |

[117] Avant l'annulation de sa loi de transposition, la République tchèque remboursait les dépenses d'exploitation et les dépenses de capital et avait déclaré 6,8 millions EUR de coûts de remboursement pour 2009.

| | | | |
|---|---|---|---|
| Malte | Non | Non | - |
| Pays-Bas | Oui | Non | - |
| Autriche | Directive non transposée. | | |
| Pologne | Non | Non | - |
| Portugal | Non | Non | - |
| Roumanie | Directive non transposée. | | |
| Slovénie | Non | Non | - |
| Slovaquie | Non | Non | - |
| Finlande | Oui | Oui | 1 |
| Suède | Directive non transposée. | | |
| Royaume-Uni | Oui | Oui | 55 (remboursés au total pour les coûts supportés en trois ans). |

On peut conclure de ce qui précède que la directive n'a pas pleinement atteint son objectif d'instaurer des conditions de concurrence égales pour les opérateurs de l'UE. La Commission étudiera les solutions permettant de réduire au minimum les obstacles au fonctionnement du marché intérieur en assurant aux opérateurs un remboursement homogène des coûts qu'ils supportent pour se conformer à l'obligation de conservation des données, en accordant une attention particulière aux petits et moyens opérateurs.

## 7. LES EFFETS DE LA CONSERVATION DES DONNEES SUR LES DROITS FONDAMENTAUX

### 7.1. Le droit fondamental au respect de la vie privée et à la protection des données à caractère personnel

La conservation des données constitue une limitation du droit à la vie privée et du droit à la protection des données à caractère personnel, qui sont des droits fondamentaux dans l'Union européenne[118]. Conformément à l'article 52, paragraphe 1, de la Charte des droits fondamentaux, cette limitation doit être prévue par la loi et respecter le contenu essentiel des droits, dans le respect du principe de proportionnalité, et elle doit être nécessaire et répondre à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui. Concrètement, cette limitation doit donc[119]:

(a) être formulée de manière précise et prévisible;

(b) être nécessaire pour réaliser un objectif d'intérêt général ou pour protéger les droits et libertés d'autrui ;

(c) être proportionnée à l'objectif poursuivi; et

(d) respecter le contenu essentiel des droits fondamentaux concernés.

---

118 Les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne (JO C 83 du 30.3.2010, p. 389) garantissent le droit de toute personne à la «protection des données à caractère personnel la concernant». L'article 16 du traité sur le fonctionnement de l'Union européenne (JO C 83 du 30.3.2010, p. 1) consacre également le droit de toute personne «à la protection des données à caractère personnel la concernant».

119 Voir la check-list des droits fondamentaux établie par la Commission pour toutes les propositions législatives dans sa communication COM (2010) 573/4, intitulée «Stratégie de l'Union pour la mise en œuvre effective de la Charte des droits fondamentaux par l'Union européenne».

L'article 8, paragraphe 2, de la convention européenne des droits de l'homme reconnaît également que l'ingérence d'une autorité publique dans l'exercice du droit d'une personne à la vie privée peut se justifier si elle est nécessaire à la sécurité nationale, à la sûreté nationale ou à la prévention des infractions pénales[120]. L'article 15, paragraphe 1, de la directive sur la vie privée et les communications électroniques, et les considérants de la direction sur la conservation des données réitèrent ces principes qui sous-tendent l'approche adoptée par l'UE en matière de conservation des données.

La jurisprudence ultérieure de la Cour de justice et de la Cour européenne des droits de l'homme a défini les conditions que doit satisfaire toute restriction du droit au respect de la vie privée. Ces arrêts sont à prendre en compte pour déterminer si la directive doit être modifiée, en particulier en ce qui concerne les conditions d'accès et d'utilisation des données conservées.

*Toute restriction du droit à la vie privée doit être précise et permettre une prévisibilité*

Dans l'affaire *Österreichischer Rundfunk,* la Cour de justice a jugé qu'une ingérence dans la vie privée prévue par la loi doit «[être] libellé[e] avec suffisamment de précision pour permettre aux destinataires de la loi de régler leur conduite, et répond[re] ainsi à l'exigence de prévisibilité […]».

*Toute restriction du droit à la vie privée doit être nécessaire et assortie de garanties minimales*

Dans l'affaire Copland c. Royaume-Uni, qui concernait la surveillance par l'État des appels téléphoniques, du courrier électronique et de l'utilisation de l'internet d'une personne, la Cour européenne des droits de l'homme a déclaré que cette restriction du droit au respect de la vie privée ne pouvait être considérée comme nécessaire que si elle était prévue par la loi nationale[121]. Dans l'affaire S. et Marper c. Royaume-Uni, qui concernait la conservation des profils ADN ou des empreintes digitales d'une personne après la conclusion, par un acquittement ou par une décision de classement sans suite, des poursuites pénales, la Cour a jugé que cette restriction au droit au respect de la vie privée ne pouvait se justifier que si elle répondait à un besoin social impérieux, si elle était proportionnée au but poursuivi et si les motifs invoqués par les autorités publiques pour la justifier apparaissaient pertinents et suffisants[122]. Les principes clés de la protection des données imposaient que la conservation des données soit « proportionnée au but pour lequel elles ont été recueillies et limitée dans le temps»[123]. Dans le contexte des écoutes téléphoniques, de la surveillance secrète et de la collecte secrète de renseignements, «il [était] essentiel de fixer des règles claires et détaillées régissant la portée et l'application des mesures et imposant un minimum d'exigences concernant, notamment, la durée, le stockage, l'utilisation, l'accès des tiers, les procédures destinées à préserver l'intégrité et la confidentialité des données et les procédures de destruction de celles-ci, de manière à ce que les justiciables disposent de garanties suffisantes contre les risques d'abus et d'arbitraire».

---

120 Article 8 de la convention de sauvegarde des droits de l'homme et des libertés fondamentales (ETS n° 5), Conseil de l'Europe, 4.11.1950.

121 Copland c. Royaume-Uni, arrêt de la Cour européenne des droits de l'homme, Strasbourg, 3.4.2007, p. 9.

122 Marper c. Royaume-Uni, arrêt de la Cour européenne des droits de l'homme, Strasbourg, 4.12.2008, p. 31.

123 Marper, p. 30.

*Toute restriction au droit à la vie privée doit être proportionnée à l'intérêt général*

La Cour de justice, dans son arrêt Schecke & Eifert concernant la publication sur l'internet de tous les bénéficiaires de subventions agricoles[124], a conclu que le législateur européen semblait ne pas avoir pris les mesures appropriées pour trouver un équilibre entre le respect du contenu essentiel du droit au respect de la vie privée et l'intérêt général (transparence) tel que reconnu par l'UE. La Cour a notamment jugé que le législateur n'avait pas pris en considération d'autres méthodes qui auraient été compatibles avec l'objectif tout en causant moins d'ingérence dans le droit des bénéficiaires des subventions au respect de leur vie privée et à la protection de leurs données à caractère personnel. Elle a par conséquent conclu que le législateur avait outrepassé les limites de la proportionnalité car «les limitations à la protection des données à caractère personnel doivent s'opérer dans les limites du strict nécessaire».

### 7.2. Les critiques à l'égard du principe de conservation des données

De nombreuses organisations de la société civile ont écrit à la Commission pour affirmer que la conservation de données est, en principe, une restriction injustifiée et inutile du droit à la vie privée des personnes. Elles considèrent la conservation non consensuelle «générale et aveugle» de données relatives au trafic des télécommunications, à la localisation et à l'abonné comme une restriction illicite des droits fondamentaux À la suite d'une affaire portée devant les tribunaux d'un État membre (Irlande) par un groupe de défense des droits civils, la question de la légalité de la directive doit être soumise à la Cour de justice[125]. Le contrôleur européen à la protection des données a, lui aussi, exprimé des doutes quant à la nécessité de la mesure.

### 7.3. Les appels à des règles plus sévères en matière de sécurité et de protection des données

Dans son rapport sur la deuxième action de contrôle de l'application de la législation de l'UE, le groupe de travail «Article 29» soutenait que les risques de violation de la confidentialité des communications et de la liberté d'expression étaient inhérents au stockage des données relatives au trafic. Il critiquait certains aspects de l'application nationale de la directive, notamment la journalisation des données, les durées de conservation, le type de données conservées et les mesures relatives à la sécurité des données. Il faisait état de cas où des détails du *contenu* des communications par l'internet, qui ne relève pas du champ d'application de la directive, étaient conservés, y compris les adresses IP de destination et les URL de sites internet, l'objet des messages envoyés par courrier électronique et la liste des destinataires mis en copie. Il appelait donc à introduire une mention précisant que les catégories sont exhaustives et à n'imposer aucune obligation supplémentaire de conservation des données aux opérateurs.

Le contrôleur européen de la protection des données a affirmé, quant à lui, que la directive «n'est pas parvenue à harmoniser les législations nationales» et que l'utilisation des données

---

124 Affaires C-92/09, Volker et Markus Schecke GbR/Land Hessen, et C-93/09, Eifert/Land Hessen et Bundesanstalt für Landwirtschaft und Ernahrung, arrêt du 9 novembre 2010.

125 Le 5 mai 2010, la High Court irlandaise a autorisé Digital Rights Ireland Limited à saisir la Cour de justice au titre de l'article 267 du traité sur le fonctionnement de l'Union européenne.

conservées n'est pas strictement limitée à la lutte contre les infractions graves[126]. Il a déclaré qu'un instrument de l'UE énonçant des règles relatives à l'obligation de conserver des données devrait, si la nécessité était démontrée, également prévoir des dispositions régissant l'accès des services répressifs à ces données et leur utilisation par ces services. Il a appelé l'UE à adopter un cadre législatif exhaustif qui impose non seulement aux opérateurs de conserver les données, mais réglemente également la manière dont les États membres utilisent les données à des fins répressives afin de garantir une «sécurité juridique aux citoyens».

De manière générale, les autorités chargées de la protection des données ont indiqué que la conservation des données emporte un risque intrinsèque de violations de la vie privée, que la directive ne résout pas au niveau de l'Union, au lieu de quoi elle oblige les États membres à veiller au respect des règles nationales de protection des données. Bien qu'aucun exemple concret d'atteintes graves à la vie privée n'ait été rapporté, le risque de violation de la sécurité des données demeure et pourrait augmenter avec l'évolution technologique et les nouvelles formes de communications, que les données soient stockées à des fins commerciales ou de sécurité, à l'intérieur ou à l'extérieur de l'UE, à moins que d'autres garanties ne soient mises en place.

## 8. CONCLUSIONS ET RECOMMANDATIONS

Le présent rapport a mis en évidence un certain nombre de points positifs et d'aspects à améliorer dans le régime actuel de la conservation des données dans l'UE. La directive avait été adoptée à un moment où les risques d'attentats terroristes imminents étaient majeurs. L'étude d'impact que la Commission entend réaliser offre l'occasion d'évaluer 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 exposées ci-après.

### 8.1. L'UE devrait 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 preuves soumises par les États membres, sous la forme de statistiques et d'exemples, n'attestent pas moins le rôle capital que les données conservées jouent dans les enquêtes judiciaires. Ces données fournissent des preuves et des indices précieux pour prévenir et poursuivre les infractions et garantir une justice pénale. Leur utilisation a abouti à des condamnations pour des infractions pénales qui, si les données n'avaient pas été conservées, seraient restées impunies. Elle a également permis l'acquittement de personnes innocentes. 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

[126] Discours prononcé par Peter Hustinx lors de la conférence «Taking on the Data Retention Directive», 3 décembre 2010.

toute l'Union d'un niveau élevé de respect de la vie privée et de protection des données à caractère personnel.

### 8.2. La transposition de la directive a été inégale

Une législation de transposition est en vigueur dans vingt-deux États membres. La latitude considérable laissée aux États membres par l'article 15, paragraphe 1, de la directive sur la vie privée pour adopter des mesures relatives à la conservation des données rend cependant 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. Trois États membres sont en situation de manquement depuis que leur loi de transposition a été annulée par leur cour constitutionnelle. Deux autres États membres doivent encore transposer la directive. La Commission poursuivra sa collaboration avec les États membres pour garantir la bonne mise en œuvre de la directive. Elle continuera également d'assurer son rôle de gardienne du droit de l'Union et recourra, s'il le faut, à la procédure d'infraction.

### 8.3. La directive n'a pas pleinement harmonisé l'approche de la conservation des données ni créé des conditions de concurrence égales pour les opérateurs

Grâce à la directive, la conservation des données est une réalité dans la plupart des États membres. Mais 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; il n'est dès lors pas surprenant qu'il n'existe pas d'approche commune, que ce soit sur des dispositions spécifiques de la directive, comme la limitation des finalités ou les durées de conservation, ou sur des aspects ne relevant pas de son champ d'application, tels que le remboursement des coûts. Néanmoins, au-delà du degré de variance expressément prévu par la directive, les divergences dans l'application nationale de la conservation des données ont créé des difficultés considérables pour les opérateurs.

### 8.4. Les opérateurs devraient bénéficier d'un remboursement homogène des coûts qu'ils supportent

L'insécurité juridique demeure pour le secteur. 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. Rien n'indique toutefois que, globalement, le secteur des télécommunications ait souffert du fait de la directive. La Commission envisagera des moyens de proposer un remboursement homogène aux opérateurs.

### 8.5. 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 et l'approche de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice[127], 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[128].

### 8.6. Prochaines étapes

À 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

---

127 Voir plus haut la référence à la communication relative à la mise en œuvre de la charte des droits fondamentaux; «Présentation générale de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice», COM(2010)385 du 20.7.2010

128 COM (2010) 609 du 4.11.2010.

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.

## Annexe: Statistiques complémentaires sur la conservation des données relatives au trafic

Notes pour l'annexe:

1. L'ancienneté des données désigne le délai écoulé entre la date à partir de laquelle les données ont été conservées et la date à laquelle l'autorité compétente a demandé leur transmission.

2. Les données relatives à l'internet désignent les données concernant l'accès à l'internet, le courrier électronique sur l'internet et la téléphonie par l'internet.

3. Les statistiques pour la République tchèque, la Lettonie et la Pologne font l'objet de réserves (voir la section 5.1).

### Statistiques transmises par les États membres pour 2008

| Tableau 7: Demandes de données de trafic conservées par ancienneté (2008) | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Ancienneté des données demandées (mois)/État membre** | **0-3** | **3-6** | **6-9** | **9-12** | **12-15** | **15-18** | **18-21** | **21-24** | **Total** |
| Belgique | Non communiquées | | | | | | | | |
| Bulgarie | Non communiquées | | | | | | | | |
| République tchèque | 102691 | 18440 | 10110 | 319 | 0 | 0 | 0 | 0 | 131560 |
| Danemark | 2669 | 672 | 185 | 37 | 23 | 2 | 7 | 4 | 3599 |
| Allemagne | 9363 | 2336 | 985 | 0 | 0 | 0 | 0 | 0 | 12684 |
| Estonie | 2773 | 733 | 157 | 827 | 0 | 0 | 0 | 0 | 4490 |
| Irlande | 8981 | 2016 | 936 | 1855 | 90 | 85 | 78 | 54 | 14095 |
| Grèce | Pas de ventilation par ancienneté | | | | | | | | 584 |
| Espagne | 22629 | 15868 | 10298 | 4783 | 0 | 0 | 0 | 0 | 53578 |
| France | Pas de ventilation par ancienneté | | | | | | | | 503437 |
| Italie | Non communiquées | | | | | | | | |
| Chypre | 30 | 4 | 0 | 0 | 0 | 0 | 0 | 0 | 34 |
| Lettonie | 10539 | 2739 | 1368 | 1211 | 597 | 438 | 0 | 0 | 16892 |
| Lituanie | 55735 | 23817 | 5251 | 512 | 0 | 0 | 0 | 0 | 85315 |
| Luxembourg | Non communiquées | | | | | | | | |
| Hongrie | Non communiquées | | | | | | | | |
| Malte | 810 | 59 | 0 | 0 | 0 | 0 | 0 | 0 | 869 |
| Pays-Bas | Pas de ventilation par ancienneté | | | | | | | | 85000 |
| Autriche | Pas de ventilation par ancienneté | | | | | | | | 3093 |
| Pologne | Non communiquées | | | | | | | | |
| Portugal | Non communiquées | | | | | | | | |
| Roumanie | Non communiquées | | | | | | | | |
| Slovénie | Pas de ventilation par ancienneté | | | | | | | | 2821 |
| Slovaquie | Non communiquées | | | | | | | | |
| Finlande | 9134 | 1144 | 448 | 214 | 268 | | | | 4008 |
| Suède | Non communiquées | | | | | | | | |
| Royaume-Uni | 315350 | 88339 | 34665 | 19398 | 6385 | 2973 | 1536 | 1576 | 470222 |
| **Total** | **533504** | **156167** | **64403** | **29156** | **7095*** | **3230*** | **1353*** | **1366*** | **1392281** |

* À l'exception de la Finlande

| Tableau 8: Demandes de données de trafic conservées par type de données (2008) (entre parenthèses, nombre de cas où les demandes de données n'ont pu être satisfaites – si fourni) | | | | |
|---|---|---|---|---|
| **Type de données/ État membre** | **Téléphonie fixe** | **Téléphonie mobile** | **Données internet** | **Total** |
| Belgique | Non communiquées | | | |
| Bulgarie | Non communiquées | | | |
| République tchèque | 4983 (131) | 125040 (2276) | 1537 (83) | 131560 (2490) |
| Danemark | 192 (0) | 3273 (5) | 134 (0) | 3599 (5) |
| Allemagne | Pas de ventilation par type de données | | | 12684 (931) |
| Estonie | 4114 (1519) | 376 (7) | Non communiquées | 4490 (1526) |
| Irlande | 5317 (16) | 5873 (48) | 2905 (33) | 14095 (97) |
| Grèce | Pas de ventilation par type de données | | | 584 |
| Espagne | 4448 (0) | 40013 (0) | 9117 (0) | 53578 (0) |
| France | Pas de ventilation par type de données | | | 503437 |
| Italie | Non communiquées | | | |
| Chypre | 3 (0) | 31 (5) | 0 (0) | 34 (5) |
| Lettonie | 1602 (90) | 14238 (530) | 1052 (76) | 16892 (696) |
| Lituanie | 765 (72) | 84550 (5657) | Non communiquées | 85315 (5729) |
| Luxembourg | Non communiquées | | | |
| Hongrie | Non communiquées | | | |
| Malte | 29 (0) | 748 (120) | 92 (13) | 869 (133) |
| Pays-Bas | Pas de ventilation par type de données | | | 85000 |
| Autriche | Pas de ventilation par type de données | | | 3093 |
| Pologne | Non communiquées | | | |
| Portugal | Non communiquées | | | |
| Roumanie | Non communiquées | | | |
| Slovénie | Pas de ventilation par type de données | | | 2821 |
| Slovaquie | Non communiquées | | | |
| Finlande | Pas de ventilation par type de données | | | 4008 |
| Suède | Non communiquées | | | |
| Royaume-Uni | 90747 (0) | 329421 (0) | 50054 (0) | 470222 (0) |
| **Total** | | | | 1392281 |

| **Tableau 9: Demandes de données de trafic de la *téléphonie fixe* conservées ayant été transmises, par ancienneté, en 2008** | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Ancienneté des données demandées (mois)/État membre** | **0-3** | **3-6** | **6-9** | **9-12** | **12-15** | **15-18** | **18-21** | **21-24** | **Total** |
| Belgique | Non communiquées | | | | | | | | |
| Bulgarie | Non communiquées | | | | | | | | |
| République tchèque | 3669 | 916 | 143 | 124 | 0 | 0 | 0 | 0 | 4852 |
| Danemark | 133 | 28 | 31 | 0 | 0 | 0 | 0 | 0 | 192 |
| Allemagne | Non communiquées | | | | | | | | |
| Estonie | 1876 | 161 | 74 | 484 | 0 | 0 | 0 | 0 | 2595 |
| Irlande | 4118 | 712 | 197 | 182 | 32 | 21 | 23 | 16 | 5301 |
| Grèce | Non communiquées | | | | | | | | |
| Espagne | 1948 | 1431 | 741 | 328 | 0 | 0 | 0 | 0 | 4448 |
| France | Non communiquées | | | | | | | | |
| Italie | Non communiquées | | | | | | | | |
| Chypre | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 |
| Lettonie | 698 | 213 | 167 | 193 | 104 | 137 | 0 | 0 | 1512 |
| Lituanie | 251 | 442 | 0 | 0 | 0 | 0 | 0 | 0 | 693 |
| Luxembourg | Non communiquées | | | | | | | | |
| Hongrie | Non communiquées | | | | | | | | |
| Malte | 28 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 29 |
| Pays-Bas | Non communiquées | | | | | | | | |
| Autriche | Non communiquées | | | | | | | | |
| Pologne | Non communiquées | | | | | | | | |
| Portugal | Non communiquées | | | | | | | | |
| Roumanie | Non communiquées | | | | | | | | |
| Slovénie | Non communiquées | | | | | | | | |
| Slovaquie | Non communiquées | | | | | | | | |
| Finlande | Non communiquées | | | | | | | | |
| Suède | Non communiquées | | | | | | | | |
| Royaume-Uni | 54805 | 27052 | 5340 | 753 | 1135 | 437 | 1050 | 175 | 90747 |
| **Total** | **67529** | **30956** | **6693** | **2064** | **1271** | **595** | **1073** | **191** | **110372** |

| **Tableau 10: Demandes de données de trafic de la *téléphonie mobile* conservées ayant été transmises, par ancienneté, en 2008** | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Ancienneté des données demandées (mois)/État membre** | **0-3** | **3-6** | **6-9** | **9-12** | **12-15** | **15-18** | **18-21** | **21-24** | **Total** |
| Belgique | Non communiquées | | | | | | | | |
| Bulgarie | Non communiquées | | | | | | | | |
| République tchèque | 98232 | 17013 | 7518 | 1 | 0 | 0 | 0 | 0 | 122764 |
| Danemark | 2433 | 628 | 143 | 33 | 20 | 1 | 7 | 3 | 3268 |
| Allemagne | Non communiquées | | | | | | | | |
| Estonie | 248 | 58 | 35 | 28 | 0 | 0 | 0 | 0 | 369 |
| Irlande | 4326 | 820 | 230 | 240 | 57 | 63 | 52 | 37 | 5825 |
| Grèce | Non communiquées | | | | | | | | |
| Espagne | 17403 | 12114 | 7444 | 3052 | 0 | 0 | 0 | 0 | 40013 |
| France | Non communiquées | | | | | | | | |
| Italie | Non communiquées | | | | | | | | |
| Chypre | 23 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 26 |
| Lettonie | 8928 | 2298 | 1085 | 746 | 394 | 257 | 0 | 0 | 13708 |
| Lituanie | 55484 | 23375 | 14 | 20 | 0 | 0 | 0 | 0 | 78893 |
| Luxembourg | Non communiquées | | | | | | | | |
| Hongrie | Non communiquées | | | | | | | | |
| Malte | 575 | 53 | 0 | 0 | 0 | 0 | 0 | 0 | 628 |
| Pays-Bas | Non communiquées | | | | | | | | |
| Autriche | Non communiquées | | | | | | | | |
| Pologne | Non communiquées | | | | | | | | |
| Portugal | Non communiquées | | | | | | | | |
| Roumanie | Non communiquées | | | | | | | | |
| Slovénie | Non communiquées | | | | | | | | |
| Slovaquie | Non communiquées | | | | | | | | |
| Finlande | Non communiquées | | | | | | | | |
| Suède | Non communiquées | | | | | | | | |
| Royaume-Uni | 229375 | 52241 | 26228 | 16040 | 3333 | 521 | 339 | 1344 | 329421 |
| **Total** | **417027** | **108603** | **42697** | **20160** | **3804** | **842** | **398** | **1384** | **594915** |

| **Tableau 11: Demandes de données de trafic *internet* conservées ayant été transmises, par ancienneté, en 2008** | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Ancienneté des données demandées (mois)/État membre** | **0-3** | **3-6** | **6-9** | **9-12** | **12-15** | **15-18** | **18-21** | **21-24** | **Total** |
| Belgique | Non communiquées | | | | | | | | |
| Bulgarie | Non communiquées | | | | | | | | |
| République tchèque | 737 | 412 | 137 | 168 | 0 | 0 | 0 | 0 | 1454 |
| Danemark | 102 | 14 | 11 | 2 | 3 | 1 | 0 | 1 | 134 |
| Allemagne | Non communiquées | | | | | | | | |
| Estonie | Non communiquées | | | | | | | | |
| Irlande | 492 | 460 | 498 | 1422 | 0 | 0 | 0 | 0 | 2872 |
| Grèce | Non communiquées | | | | | | | | |
| Espagne | 3278 | 2323 | 2113 | 1403 | 0 | 0 | 0 | 0 | 9117 |
| France | Non communiquées | | | | | | | | |
| Italie | Non communiquées | | | | | | | | |
| Chypre | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Lettonie | 424 | 150 | 75 | 219 | 74 | 34 | 0 | 0 | 976 |
| Lituanie | Non communiquées | | | | | | | | |
| Luxembourg | Non communiquées | | | | | | | | |
| Hongrie | Non communiquées | | | | | | | | |
| Malte | 76 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 79 |
| Pays-Bas | Non communiquées | | | | | | | | |
| Autriche | Non communiquées | | | | | | | | |
| Pologne | Non communiquées | | | | | | | | |
| Portugal | Non communiquées | | | | | | | | |
| Roumanie | Non communiquées | | | | | | | | |
| Slovénie | Non communiquées | | | | | | | | |
| Slovaquie | Non communiquées | | | | | | | | |
| Finlande | Non communiquées | | | | | | | | |
| Suède | Non communiquées | | | | | | | | |
| Royaume-Uni | 31170 | 9046 | 3097 | 2605 | 1917 | 2015 | 147 | 57 | 50054 |
| **Total** | **36279** | **12408** | **5931** | **5819** | **1994** | **2050** | **147** | **58** | **64686** |

## Statistiques transmises par les États membres pour 2009

| Tableau 12: Demandes de données conservées par ancienneté (2009) | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Ancienneté des données demandées (mois)/État membre** | **0-3** | **3-6** | **6-9** | **9-12** | **12-15** | **15-18** | **18-21** | **21-24** | **Total** |
| Belgique | Non communiquées | | | | | | | | |
| Bulgarie | Non communiquées | | | | | | | | |
| République tchèque | 210975 | 56623 | 11620 | 1053 | 0 | 0 | 0 | 0 | 280271 |
| Danemark | 2980 | 685 | 179 | 104 | 54 | 38 | 12 | 14 | 4066 |
| Allemagne | non fourni | | | | | | | | |
| Estonie | 4299 | 1836 | 1210 | 1065 | 0 | 0 | 0 | 0 | 8410 |
| Irlande | 8117 | 1652 | 805 | 297 | 168 | 134 | 69 | 41 | 11283 |
| Grèce | Non communiquées | | | | | | | | |
| Espagne | 29775 | 19346 | 13999 | 6970 | 0 | 0 | 0 | 0 | 70090 |
| France | Pas de ventilation par ancienneté | | | | | | | | 514813 |
| Italie | Non communiquées | | | | | | | | |
| Chypre | 31 | 8 | 1 | 0 | 0 | 0 | 0 | 0 | 40 |
| Lettonie | 20758 | 2414 | 1088 | 796 | 565 | 475 | 0 | 0 | 26096 |
| Lituanie | 30247 | 35456 | 5886 | 884 | 0 | 0 | 0 | 0 | 72473 |
| Luxembourg | Non communiquées | | | | | | | | |
| Hongrie | Non communiquées | | | | | | | | |
| Malte | 3336 | 362 | 151 | 174 | 0 | 0 | 0 | 0 | 4023 |
| Pays-Bas | Non communiquées | | | | | | | | |
| Autriche | Non communiquées | | | | | | | | |
| Portugal | Non communiquées | | | | | | | | |
| Roumanie | Non communiquées | | | | | | | | |
| Pologne | 642327 | 178306 | 75525 | 52526 | 27098 | 23924 | 13984 | 34628 | 1048318 |
| Slovénie | Pas de ventilation par ancienneté | | | | | | | | 1918 |
| Slovaquie | Pas de ventilation par ancienneté | | | | | | | | 5214 |
| Finlande | 2000 | 1310 | 532 | 152 | 76 | 0 | 0 | 0 | 4070 |
| Suède | Non communiquées | | | | | | | | |
| Royaume-Uni | Non communiquées | | | | | | | | |
| **Total** | **954845** | **297998** | **110996** | **64021** | **27961** | **24571** | **14065** | **34683** | **2051085** |

| Tableau 13: Demandes de données conservées par type de données (2009) (entre parenthèses, nombre de cas où les demandes de données n'ont pu être satisfaites – si fourni) | | | | |
|---|---|---|---|---|
| **Type de données/ État membre** | **Téléphonie fixe** | **Téléphonie mobile** | **Données internet** | **Total** |
| Belgique | Non communiquées | | | |
| Bulgarie | Non communiquées | | | |
| République tchèque | 13843 (934) | 256074 (9141) | 10354 (371) | 280271 (10446) |
| Danemark | 133 (0) | 3771 (10) | 162 (1) | 4066 (11) |
| Allemagne | Non communiquées | | | |
| Estonie | 6422 (2279) | 902 (21) | 1086 (468) | 8410 (2768) |
| Irlande | 4542 (16) | 5239 (20) | 1502 (56) | 11283 (92) |
| Grèce | Non communiquées | | | |
| Espagne | 5055 (0) | 56133 (0) | 8902 (0) | 70090 (0) |
| France | Pas de ventilation par type de données | | | 514813 |
| Italie | Non communiquées | | | |
| Chypre | 0 (0) | 23 (3) | 14 (0) | 40 (3) |
| Lettonie | 1672 (218) | 22796 (102) | 1628 (240) | 26096 (560) |
| Lituanie | 1321 (0) | 51573 (6237) | 19579 (343) | 72473 (6580) |
| Luxembourg | Non communiquées | | | |
| Hongrie | Non communiquées | | | |
| Malte | 156 (10) | 3693 (882) | 174 (10) | 4023 (902) |
| Pays-Bas | Non communiquées | | | |
| Autriche | Non communiquées | | | |
| Pologne | Pas de ventilation par type de données | | | 1048318 |
| Portugal | Non communiquées | | | |
| Roumanie | Non communiquées | | | |
| Slovénie | Pas de ventilation par type de données | | | 1918 (48) |
| Slovaquie | Pas de ventilation par type de données | | | 5214 (157) |
| Finlande | Pas de ventilation par type de données | | | 4070 |
| Suède | Non communiquées | | | |
| Royaume-Uni | Non communiquées | | | |
| **Total** | | | | 2051082 (1069885) |

| Tableau 14: Demandes de données relatives à la *téléphonie fixe* conservées ayant été transmises, par ancienneté, en 2009 | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Ancienneté des données demandées (mois)/État membre** | **0-3** | **3-6** | **6-9** | **9-12** | **12-15** | **15-18** | **18-21** | **21-24** | **Total** |
| Belgique | Non communiquées | | | | | | | | |
| Bulgarie | Non communiquées | | | | | | | | |
| République tchèque | 9919 | 2907 | 47 | 36 | 0 | 0 | 0 | 0 | 12909 |
| Danemark | 105 | 19 | 7 | 2 | 0 | 0 | 0 | 0 | 133 |
| Allemagne | Non communiquées | | | | | | | | |
| Estonie | 2254 | 866 | 599 | 424 | 0 | 0 | 0 | 0 | 4143 |
| Irlande | 3934 | 337 | 69 | 70 | 50 | 39 | 16 | 11 | 4526 |
| Grèce | Non communiquées | | | | | | | | |
| Espagne | 2371 | 1492 | 844 | 348 | 0 | 0 | 0 | 0 | 5055 |
| France | Non communiquées | | | | | | | | |
| Italie | Non communiquées | | | | | | | | |
| Chypre | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Lettonie | 744 | 253 | 157 | 143 | 68 | 89 | 0 | 0 | 1454 |
| Lituanie | 469 | 773 | 73 | 6 | 0 | 0 | 0 | 0 | 1321 |
| Luxembourg | Non communiquées | | | | | | | | |
| Hongrie | Non communiquées | | | | | | | | |
| Malte | 83 | 25 | 18 | 20 | 0 | 0 | 0 | 0 | 146 |
| Pays-Bas | Non communiquées | | | | | | | | |
| Autriche | Non communiquées | | | | | | | | |
| Pologne | Non communiquées | | | | | | | | |
| Portugal | Non communiquées | | | | | | | | |
| Roumanie | Non communiquées | | | | | | | | |
| Slovénie | Non communiquées | | | | | | | | |
| Slovaquie | Non communiquées | | | | | | | | |
| Finlande | Non communiquées | | | | | | | | |
| Suède | Non communiquées | | | | | | | | |
| Royaume-Uni | Non communiquées | | | | | | | | |
| **Total** | **19879** | **6672** | **1814** | **1049** | **118** | **128** | **16** | **11** | **29687** |

| **Tableau 15: Demandes de données relatives à la *téléphonie mobile* conservées ayant été transmises, par ancienneté, en 2009** | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Ancienneté des données demandées (mois)/État membre** | **0-3** | **3-6** | **6-9** | **9-12** | **12-15** | **15-18** | **18-21** | **21-24** | **Total** |
| Belgique | Non communiquées | | | | | | | | |
| Bulgarie | Non communiquées | | | | | | | | |
| République tchèque | 197620 | 48841 | 472 | 0 | 0 | 0 | 0 | 0 | 246933 |
| Danemark | 2777 | 639 | 162 | 98 | 47 | 19 | 12 | 7 | 3761 |
| Allemagne | Non communiquées | | | | | | | | |
| Estonie | 318 | 397 | 96 | 70 | 0 | 0 | 0 | 0 | 881 |
| Irlande | 3669 | 835 | 220 | 210 | 115 | 92 | 50 | 28 | 5219 |
| Grèce | Non communiquées | | | | | | | | |
| Espagne | 24065 | 15648 | 11147 | 5273 | 0 | 0 | 0 | 0 | 56133 |
| France | Non communiquées | | | | | | | | |
| Italie | Non communiquées | | | | | | | | |
| Chypre | 17 | 16 | 0 | 0 | 0 | 0 | 0 | 0 | 23 |
| Lettonie | 18832 | 1912 | 778 | 515 | 394 | 263 | 0 | 0 | 22694 |
| Lituanie | 25713 | 19595 | 28 | 0 | 0 | 0 | 0 | 0 | 45336 |
| Luxembourg | Non communiquées | | | | | | | | |
| Hongrie | Non communiquées | | | | | | | | |
| Malte | 2332 | 246 | 111 | 122 | 0 | 0 | 0 | 0 | 2811 |
| Pays-Bas | Non communiquées | | | | | | | | |
| Autriche | Non communiquées | | | | | | | | |
| Pologne | Non communiquées | | | | | | | | |
| Portugal | Non communiquées | | | | | | | | |
| Roumanie | Non communiquées | | | | | | | | |
| Slovénie | Non communiquées | | | | | | | | |
| Slovaquie | Non communiquées | | | | | | | | |
| Finlande | Non communiquées | | | | | | | | |
| Suède | Non communiquées | | | | | | | | |
| Royaume-Uni | Non communiquées | | | | | | | | |
| **Total** | **275343** | **88119** | **13014** | **6288** | **556** | **374** | **62** | **35** | **383791** |

| **Tableau 16: Demandes de données *relatives à l'internet* conservées ayant été transmises, par ancienneté, en 2009** | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Ancienneté des données demandées (mois)/État membre** | **0-3** | **3-6** | **6-9** | **9-12** | **12-15** | **15-18** | **18-21** | **21-24** | **Total** |
| Belgique | Non communiquées | | | | | | | | |
| Bulgarie | Non communiquées | | | | | | | | |
| République tchèque | 3369 | 4811 | 861 | 942 | 0 | 0 | 0 | 0 | 9983 |
| Danemark | 98 | 27 | 10 | 4 | 4 | 7 | 0 | 1 | 151 |
| Allemagne | Non communiquées | | | | | | | | |
| Estonie | 315 | 145 | 56 | 102 | 0 | 0 | 0 | 0 | 618 |
| Irlande | 489 | 455 | 502 | 0 | 0 | 0 | 0 | 0 | 1446 |
| Grèce | Non communiquées | | | | | | | | |
| Espagne | 3339 | 2206 | 2008 | 1349 | 0 | 0 | 0 | 0 | 8902 |
| France | Non communiquées | | | | | | | | |
| Italie | Non communiquées | | | | | | | | |
| Chypre | 12 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 14 |
| Lettonie | 852 | 198 | 74 | 90 | 88 | 86 | 0 | 0 | 1388 |
| Lituanie | 4060 | 15087 | 1 | 88 | 0 | 0 | 0 | 0 | 19236 |
| Luxembourg | Non communiquées | | | | | | | | |
| Hongrie | Non communiquées | | | | | | | | |
| Malte | 150 | 14 | 0 | 0 | 0 | 0 | 0 | 0 | 164 |
| Pays-Bas | Non communiquées | | | | | | | | |
| Autriche | Non communiquées | | | | | | | | |
| Pologne | Non communiquées | | | | | | | | |
| Portugal | Non communiquées | | | | | | | | |
| Roumanie | Non communiquées | | | | | | | | |
| Slovénie | Non communiquées | | | | | | | | |
| Slovaquie | Non communiquées | | | | | | | | |
| Finlande | Non communiquées | | | | | | | | |
| Suède | Non communiquées | | | | | | | | |
| Royaume-Uni | Non communiquées | | | | | | | | |
| **Total** | **12684** | **22945** | **3512** | **2575** | **92** | **93** | **0** | **1** | **41902** |