

I. INTRODUCTION

Le 15 mars 2006, le Parlement et le Conseil de l'Union européenne ont adopté la **directive 2006/24/CE** relative à « *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*^{1, 2} ».

Cette directive a été adoptée dans le but d'obliger les opérateurs de télécommunications et les fournisseurs d'accès à Internet à conserver certaines données qu'ils sont amenés à traiter. De cette façon, la Commission et le Conseil de l'Union européenne veulent garantir que ce genre de données soient disponibles pour examiner, rechercher et poursuivre la criminalité grave.

La Ligue des droits de l'Homme et la Liga voor Mensenrechten tiennent à souligner que cette obligation de conserver les données restreint considérablement le droit au respect de la vie privée. En outre, des experts mettent en question la valeur ajoutée de cette mesure puisque, dans la pratique, **le stockage du trafic de télécommunication paraît être une mesure inadaptée** et qui implique, pour toutes les parties concernées, une charge financière et pratique déraisonnable.

II CONTENU DE LA DIRECTIVE

Cette directive concerne les données de trafic et d'emplacement des individus ainsi que les données liées qui sont nécessaires pour identifier l'abonné ou l'utilisateur enregistré. **Toutes les données relatives aux personnes concernées, le moment, le lieu, la durée, l'ampleur et la modalité d'une conversation téléphonique, d'un SMS ou d'un e-mail sont conservées**³. Seule restriction importante : les données révélant le contenu de la communication ne peuvent pas être conservées.

Cette directive laisse la liberté aux États membres de déterminer le délai de conservation des données de trafic et d'emplacement, dans un laps de temps compris entre 6 mois et deux ans⁴. En effet, la durée minimale de conservation des données est de six mois à partir de la date de la communication et la durée maximale de conservation des données est de deux ans à partir de la date de la communication, sauf si les États membres peuvent justifier d'une prolongation (limitée dans le temps) et s'ils en informent immédiatement la Commission et les autres États membres⁵. Les données conservées sont détruites à l'expiration du délai, à l'exception des données consultées qui ont été préservées⁶.

¹ Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

² Journal officiel n° L 105 du 13/04/2006 p. 0054 – 0063. Cette directive est en vigueur depuis le 3 mai 2006.

Voir : <http://www.europarl.europa.eu/oeil/file.jsp?id=5275032>.

³ Art. 5 de la directive 2006/24/CE.

⁴ Art. 6 de la directive 2006/24/CE.

⁵ Art. 12 de la directive 2006/24/CE.

⁶ Art. 7, d) de la directive 2006/24/CE.

Les États membres ne sont pas dans l'obligation de rembourser les frais de stockage et d'acheminement des données aux opérateurs de télécommunications et aux fournisseurs d'accès à Internet⁷. Les États membres doivent également faire en sorte que les opérateurs de télécommunications et les fournisseurs d'accès respectent certains principes en matière de sécurité des données⁸. Les États membres doivent incorporer **des garanties qui assurent que les données gardées sont uniquement fournies aux autorités nationales compétentes, cela en accord avec la législation nationale.**

En outre, **chaque État membre doit désigner un ou plusieurs organismes publics chargés de garantir la sécurité des données conservées**⁹. Ces instances doivent présenter des garanties d'**indépendance**. **L'accès ou le transfert non autorisé de données doivent être passibles de sanctions administratives ou pénales qui soient efficaces, proportionnées et dissuasives**¹⁰.

III. GARANTIES

*L'efficacité de la mesure*¹¹

Nul ne contestera que le stockage des données relatives au trafic des télécommunications fait partie intégrante de la lutte contre la criminalité grave. Toutefois, certains **experts**¹² **estiment que cette directive n'est pas un instrument effectif pour ce faire.**

Tout d'abord, il existe un **problème lié à l'utilité des données à conserver**. En effet, il sera fréquent que l'utilisateur des services de télécommunication ne puisse pas être identifié à l'aide des données conservées. Par le biais des données de trafic, on peut déterminer quel serveur web un appareil affiche à l'écran, mais on ne sait pas si l'utilisateur final l'a lui-même consulté ni quel site Internet est concerné. En effet, il arrive que plusieurs utilisateurs se cachent derrière une seule adresse IP. En outre, dans le futur (avec Ipv6), le fait d'avoir une adresse IP unique se généralisera, de sorte que chaque e-mail et chaque visite d'un site Internet aura automatiquement sa propre adresse IP. Comme il est prévu de conserver une quantité énorme de données, il sera souvent difficile de retrouver l'information recherchée dans les immenses banques de données conservées, cela d'autant plus si le temps de conservation est élevé¹³.

Ensuite, certains experts soulignent que les données de trafic Internet qu'on pourrait enregistrer seront inutilisables en tant que pièces à conviction en raison du fait qu'elles **peuvent très facilement être falsifiées et manipulées**. D'après différentes associations de

⁷ Bien que ces frais peuvent, dans certains cas, être très élevés.

⁸ Art. 7 de la directive 2006/24/CE.

⁹ Art. 9 de la directive 2006/24/CE.

¹⁰ Art. 13 de la directive 2006/24/CE.

¹¹ DEENE, J, 'Bewaren van telecommunicatieverkeer verplicht vanaf juni 2007', *De Juristenkrant*, nr 126, 22 mars 2006 et VAN DOOREN, (06-09-2005), 'Verslag van een mondeling overleg' in Eerste Kamer der Staten-Generaal [WWW]:

<http://europapoort.eerstekamer.nl/9345000/1/j9vvy6i0ydh7th/vgbwr4k8ocw2/f=/vh24j3sk6zu8.pdf>.

¹² tel que le Professeur Hans Franken.

¹³ Internet Services Providers Association (ISPA), "Position of Principle on the matter of data retention", Bruxelles, Novembre 2006. Voir http://www.ispa.be/files/data_retention_positionpaper.pdf.

fournisseurs d'accès à Internet¹⁴, la directive sera assez facilement contournée par des individus ayant une connaissance de l'informatique ou des relations avec des informaticiens.

La portée de ces mesures¹⁵

La directive européenne reste relativement floue concernant les données concrètes à conserver. Bien qu'il y ait une prohibition explicite de la conservation des données desquelles on peut déduire le contenu de la communication, **il convient de souligner qu'il est possible de se faire une idée plus ou moins précise de certains aspects de la vie privée de quelqu'un en prenant systématiquement connaissance de ses données de trafic et d'emplacement.** En outre, les fournisseurs de réseaux règlent le trafic de leurs clients via de multiples serveurs sur lesquels **les données de trafic complètes de leurs clients se trouvent, y compris le contenu des communications.** C'est par la suite et à partir de cette information que les fournisseurs doivent extraire les données de trafic. Non seulement c'est contraire à la prohibition explicite contenue dans la directive européenne, mais dans la pratique c'est une source de problème. **Les fournisseurs d'accès à Internet craignent d'être incapables de garantir l'intégrité et la sécurité de toutes ces données¹⁶.**

Proportionnalité¹⁷

Nous sommes confrontés à **une violation du droit au respect de la vie privée.** Une ingérence dans ce droit au respect de la vie privée n'est justifiée, au titre de l'article 8 de la Convention européenne des Droits de l'Homme, que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire. Ce critère s'est concrétisé, dans la jurisprudence de la Cour européenne des Droits de l'Homme, autour des notions de proportionnalité, de finalité et de subsidiarité.

Le principe de proportionnalité n'est pas respecté, car il n'y a pas de **rapport raisonnable entre le but recherché (la répression des infractions) et les moyens mis en œuvre pour y arriver (le stockage de la totalité des données).** En effet, dans la pratique, le stockage du trafic des télécommunications paraît être non seulement une mesure inadaptée, mais il entraîne également, pour toutes les parties concernées, une charge financière et pratique déraisonnable. Quand on additionnera les données stockées par les différents fournisseurs, le nombre de données à conserver sera immense, tout comme les frais qui y sont liés, ce qui implique que le critère de proportionnalité n'est pas respecté.

En outre, les frais directs pour l'usage d'Internet, qui naturellement seront facturés aux consommateurs, augmenteront de manière substantielle, ce qui va élargir le fossé numérique actuel dans notre société¹⁸. Même si le gouvernement décidait de prendre en charge une partie de ces frais, cela signifie tout de même que **le citoyen lui-même devra payer pour se faire contrôler.**

¹⁴ *Ibid.* Voir aussi European Internet Services Providers Association et US Internet Service Provider Association, "Position on the impact of data retention laws on the fight against cybercrime", Bruxelles, 30 septembre 2002. Voir: http://www.euroispa.org/docs/020930eurousispa_dretent.pdf.

¹⁵ VAN DOOREN, *op. cit.*

¹⁶ Voir European Internet Services Providers Association et US Internet Service Provider Association, *op. cit.*

¹⁷ VAN DOOREN, *op. cit.*

¹⁸ Voir European Internet Services Providers Association et US Internet Service Provider Association, *op. cit.*

Surtout, les fournisseurs d'accès à Internet démontrent que **le gouvernement n'a pas prouvé à suffisance qu'une conservation de ces données est nécessaire pour la sécurité de la société et que des mesures existantes et moins radicales ne suffisent pas**¹⁹.

La Belgique en veut plus

Dans notre pays, la directive européenne n'a pas encore d'impact pour le moment, parce qu'elle n'a pas encore été transposée dans une loi belge²⁰. L'Institut belge des services postaux et des télécommunications (IBPT) élabore actuellement un projet de loi visant à implémenter la directive européenne dans la législation belge. Le texte est attendu dans le courant de 2008, les négociations restant secrètes jusque là. **Toutefois, il semblerait que certains voudraient aller au-delà, sur certains points, de ce qu'exige la directive européenne. En effet, outre les données de trafic téléphonique ou d'e-mail, il est également envisagé d'enregistrer le comportement de navigation des individus.** De la sorte, la transposition de la directive européenne risque d'être utilisée pour introduire des mesures sollicitées depuis longtemps, mais étant disproportionnées et inacceptables.

L'enregistrement du comportement de navigation des individus peut avoir des conséquences négatives et peut entraîner une utilisation qui outrepassé l'intention initiale. Il existe dès lors un **danger qu'un projet de loi qui ne soit pas conforme au droit au respect de la vie privée soit utilisé pour contrôler une certaine parole critique au sein de la société et – potentiellement – de la faire taire.** Dans ce cas de figure, il s'agirait d'une évolution progressive vers un état sécurisé dans lequel certains acquis fondamentaux de la démocratie parlementaire sont sacrifiés sur l'autel de la lutte contre la criminalité grave et le terrorisme (ces derniers, soit dit en passant, poursuivant les mêmes buts...).

Evolutions récentes

Depuis les attentats du 11 septembre 2001 ayant frappé les Etats-Unis, les conceptions relatives au respect du droit à la vie privée ont été bouleversées. **Un climat particulier s'est instauré, dans lequel le droit à la protection de la vie privée est minimisé par rapport à l'aspiration à la sécurité.** Cela est permis en raison de la persistance de la croyance selon laquelle si l'on n'a rien à cacher, on n'a rien à craindre. Or, nombreux sont ceux qui **n'y voient aucun inconvénient car, la plupart du temps, ils ignorent ce qui peut arriver, et dans certains cas arrive déjà, avec leurs données personnelles.**

Ces dernières années, **d'innombrables mesures visant à lutter contre la criminalité grave, le terrorisme et la migration illégale** ont été introduites. Il y a eu, entre autres exemples, l'introduction de puces RFID (lisibles à distance) dans les billets de banque, l'introduction d'un passeport biométrique européen et de sa base de données nationale (et à terme une base de données centrale européenne), les différents systèmes de sécurité et d'information (comme les SIS I et II, le VIS, l'Eurodac ou encore des systèmes plus récents comme le PNR et le

¹⁹ *Ibid.*

²⁰ Cette directive a du être transposée en législation nationale pour le 15/09/2007, mais uniquement en ce qui concerne le stockage des données de communication concernant les réseaux téléphoniques fixes et mobiles. Chaque Etat membre peut cependant retarder l'implémentation de la directive jusqu'au 15/03/2009 en ce qui concerne le stockage des données de communication concernant l'accès à Internet, la téléphonie par Internet et l'e-mail, pour peu que cela soit préalablement communiqué au Conseil et à la Commission européenne. Plusieurs Etats membres l'ont déjà fait (pour différents délais) : les Pays Bas, l'Autriche, le Royaume-Uni, l'Estonie, la Chypre, la Grèce, le Luxembourg, la Slovénie, la Suède, la Lituanie, la Lettonie, la Tchèque, la Belgique, la Pologne, la Finlande et l'Allemagne.

système *entry/exit*), de même qu'une explosion du nombre des caméras de surveillance installées. Si l'on couple ces évolutions au fait que les données des usagers **vont de plus en plus être jointes et pourront donc être recoupées, la protection du droit au respect de la vie privée sera de plus en plus menacée**. Le Contrôleur européen de la protection des données (CEPD) est d'avis qu'il conviendrait plutôt de procéder à l'évaluation des initiatives déjà prises avant de poursuivre l'adoption de nouvelles mesures²¹. A défaut, il pourrait s'avérer ardu de garder une vision de l'évolution de ces mesures et d'avoir un aperçu plus ou moins précis des violations potentielles des droits fondamentaux des individus²².

Présomption d'innocence

Les mesures susmentionnées **renversent le principe démocratique selon lequel chacun est présumé innocent jusqu'à la preuve du contraire**. En effet, les données des individus sont largement conservées et les services de sécurité et de maintien de l'ordre ont un accès très étendu à ces bases de données. Or, le Comité permanent de contrôle des services de police (Comité P) a déjà pu mettre en évidence le fait que **la confiance dans le professionnalisme de ces services n'est pas toujours permise**. Le Comité P a ainsi pu constater qu'il était fréquent que des agents des forces de l'ordre consultent indûment les bases de données externes ou de la police²³. En effet, le Comité P a mis en évidence le fait qu'une partie substantielle des membres des forces de l'ordre ne peut pas donner de justification lorsqu'elle cherche des informations privées dans les bases de données à sa disposition et qu'il s'agit, dans la plupart des cas, d'une utilisation impropre des bases de données²⁴. Dans l'hypothèse où il est donné à tous les agents de police un accès aux données de trafic ou d'emplacement des opérateurs de télécommunications et des fournisseurs d'Internet, ainsi qu'aux données relatives au comportement de navigation de chacun, il est raisonnable de penser que de telles pratiques auraient également cours. Dans ce cas, les conséquences de telles pratiques pourraient prendre des proportions énormes. Par exemple, il serait possible pour toute personne ayant accès à ce type de données de savoir quels sites Internet un voisin - avec lequel il est en conflit depuis des années - a fréquenté les derniers mois ; si un membre de sa famille a une relation extraconjugale sur base de son utilisation du téléphone ; si un ex-partenaire participe à des programmes de dating sur base de son comportement de navigation ; etc.

Protection des données

Ceci mène dès lors à **une question cruciale : quelles autorités nationales sont jugées compétentes pour consulter les données conservées et à quelles conditions ?** L'information conservée est en effet d'un niveau très sensible et **son accès doit être strictement réglementé** (limité, par exemple, au cadre strict d'une instruction judiciaire, sous le contrôle d'un juge d'instruction). Toutefois, le ministre de l'Intérieur a indiqué au Parlement, lors des discussions relatives au Plan national de sécurité 2008-2011, que les services policiers souhaitent pouvoir

²¹ HUSTINX, P., "Preliminary comments on three Communications from the Commission on border management (COM (2008) 69, COM (2008)68 and COM (2008)67)", European Data Protection Supervisor, Bruxelles, le 3 mars 2008. Voir : http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf.

²² *Ibid.*

²³ Comité permanent de contrôle des services de police, Rapport d'activités 2005, pp. 53 et suiv. :

<http://www.comitep.be/Fr/fr.html>.

²⁴ *Ibid.*, pp. 55-56.

faire un usage proactif de telles mesures²⁵. A été mentionnée, notamment, la volonté d'avoir la possibilité de pirater un ordinateur. Or, les données stockées sur un ordinateur sont particulièrement sensibles. A cet égard, il convient de signaler le récent arrêt de la Cour constitutionnelle fédérale allemande (*Bundesverfassungsgericht*), qui a annulé une loi controversée autorisant un contrôle secret des ordinateurs dans le cadre de la lutte contre le terrorisme. Sa motivation se basait sur le fait que, dans ce cas de figure, les droits fondamentaux des citoyens doivent primer sur des intérêts de sécurité²⁶. **La conception selon laquelle la sécurité serait mieux protégée par l'abandon des protections du droit au respect de la vie privée est un dogme non fondé et dangereux.**

Cependant, cette conception est à la base de la philosophie actuelle des négociations entre l'IBPT, la Federal Computer Crime Unit (FCCU) et les administrations concernées : le dogme du sacrifice des libertés pour garantir un degré de sécurité plus élevé n'est pas remis en question mais, en revanche, la discussion porte sur la question de savoir si le refus de stocker les données de télécommunication peut être pénalisé ou sur celle de savoir si l'IBPT peut dresser une liste des sous-traitants agréés garantissant le stockage des données.

IV. CONCLUSION

La directive européenne concernée peut être la source d'atteintes au droit à la protection de la vie privée. La finalité, la proportionnalité et la subsidiarité de ces atteintes n'est pas démontrée. En outre, elle crée des possibilités d'utilisation qui excèdent le but original. Aucune garantie que le législateur belge implémentera cette directive d'une manière conforme au droit au respect de la vie privée n'existe à l'heure actuelle. **Il est donc grand temps de débattre du déséquilibre actuel existant entre les libertés civiles d'une part et la sécurité et le maintien de l'ordre d'autre part.**

Même si un certain nombre de mesures trouvent leur source dans le droit européen, il existe encore un espace pour les États membres de les implémenter en respectant les libertés fondamentales. **Concrètement, la Ligue des droits de l'Homme et la Liga voor Mensenrechten souhaitent que le Parlement précise de manière claire quelles sont les données qui peuvent être conservées, par quels acteurs et pour quelle durée, quelles personnes auront accès à ces données et à quelles conditions. D'autre part, la Ligue des droits de l'Homme et la Liga voor Mensenrechten requièrent que des sanctions efficaces, proportionnées et dissuasives soit prévues en cas d'infraction et que des compétences étendues soient attribuées aux organismes publics de contrôle.** En outre, il est important que la législateur belge n'excède pas les exigences de la directive européenne en obligeant les fournisseurs d'accès à Internet à enregistrer le comportement de navigation. Il est donc souhaitable que, devant les parlements nationaux, se joue un important 'deuxième tour' concernant cette directive européenne.

²⁵ Chambre des Représentants de Belgique, 'Échange de vues concernant le Plan national de sécurité 2008-2011', 5 mars 2008, p.25 : <http://www.lachambre.be/FLWB/PDF/52/0812/52K0812002.pdf>.

²⁶ Voir (en allemand): http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html.

Pour toute information, n'hésitez pas à contacter Maartje De Schutter, Collaboratrice de la Liga voor Mensenrechten : 09/223 07 38 – maartje@mensenrechten.be, ou Manuel Lambert, Conseiller juridique de la Ligue des droits de l'Homme : 02/209.62.80 - mlambert@liguedh.be.