LA LIGUE DES DROITS DE L'HOMME

ANALYSE
TRANSPOSITION EN DROIT BELGE DE LA DIRECTIVE 2006/24/CE DE L'UNION EUROPENNE RELATIVE AU STOCKAGE DES DONNEES

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.

Le Comité de vigilance démocratique tient à souligner que cette obligation de conserver les données restreint considérablement le droit au respect de la vie privée.

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 ans[4]. 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 membres[5]. Les données conservées sont détruites à l'expiration du délai, à l'exception des données consultées qui ont été préservées[6].

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 doivent également faire en sorte que les opérateurs de télécommunications et les fournisseurs d'accès respectent certains principes en matière de sécurité des données[7]. 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**[8]. 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**[9].

III. CRITIQUES

1. Critiques générales

L'efficacité de la mesure[10]

Nul ne contestera que le stockage des données relatives au trafic des télécommunications fait partie intégrante de la lutte contre la criminalité grave. Toutefois, on peut craindre **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**. 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 élevé[11].

La portée de ces mesures[12]

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.**

2. Critiques liées au respect de la CEDH

Légalité

Nous sommes confrontés à **une ingérence dans le 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.

7 Art. 7 de la directive 2006/24/CE.
8 Art. 9 de la directive 2006/24/CE.
9 Art. 13 de la directive 2006/24/CE.
10 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/j9vvgy6i0ydh7th/vgbwr4k8ocw2/f=/vh24j3sk6zu8.pdf.
11 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.
12 VAN DOOREN, op. cit.

Or, si la CEDH admet de telles ingérences dans certaines circonstances et à certaines conditions, elle établit clairement que ces ingérences doivent être prévues par la loi. Il ne serait donc pas admissible que des données aussi fondamentales que le type de données récoltées et les conditions de leur conservation ou encore le contrôle sur la gestion de ces données soient fixées par arrêté royal et non par la loi.

Objectif légitime

Les ingérences dans les droits fondamentaux prévues par la loi doivent poursuivre un objectif légitime. En l'espèce, on ne peut contester que la nécessaire répression des infractions graves constitue un objectif légitime.

Proportionnalité

Mais, ces ingérences doivent également être proportionnées à l'objectif légitime. Or, à cet égard, nous pensons que la conservation généralisée des informations personnelles concernant tous les citoyens du Royaume et au-delà pour une période si longue est clairement disproportionnée.

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).** 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.

Surtout, **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**[13].

3. Critiques particulières

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 police[14]. 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 données[15]. 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.

13 Ibid.
14 Comité permanent de contrôle des services de police, Rapport d'activités 2005, pp. 53 et suiv. : http://www.comitep.be/Fr/fr.html.
15 Ibid., pp. 55-56.

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 faire un usage proactif de telles mesures[16]. A été mentionnée, notamment, la volonté d'avoir la possibilité de pirater un ordinateur. Or, les données stockées sur un ordinateur sont particulièrement sensibles.

Protection des mineurs

A cet égard, il convient de rappeler l'arrêt S. et Marper c. RU du 4 décembre 2008. Dans cet arrêt, concernant des bases de données ADN, la Cour a affirmé qu'elle « *est frappée par le caractère général et indifférencié du pouvoir de conservation en vigueur en Angleterre et au Pays de Galle. En effet, les données en cause peuvent être conservée quelles que soient la nature et la gravité des infractions dont la personne était à l'origine soupçonnée et indépendamment de son âge*. »

Force est de constater que nous sommes ici dans la même situation : conservation générale et indifférenciées de données à caractère personnel, quelles que soient la nature et la gravité des infractions et **indépendamment de l'âge, la situation des mineurs, grands consommateurs de nouvelles technologies, n'étant absolument pas prise en compte.**

Protection du secret professionnel et des sources journalistiques

Enfin, il est évident qu'il existe d'indéniables risques pour des principes aussi cardinaux dans notre Etat de droit que ceux de **la protection des sources journalistiques et de la protection du secret professionnel** (des médecins, avocats et autres profession soumises à l'art. 458 CP). En effet, comment encore garantir ces principes si toutes les données de ces individus sont conservées ?

Durée de la conservation des données

Le délai maximum de deux ans prévu par la directive est manifestement trop long. Cet avis est également partagé par la Commission de protection de la vie privée[17].

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.

Concrètement, le Comité de vigilance démocratique souhaite 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, des

16 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.
17 Commission pour la Protection de la Vie privée, avis n° 24 du 2 juillet 2008.

sanctions efficaces, proportionnées et dissuasives doivent être prévues en cas d'infraction et des compétences étendues doivent être attribuées aux organismes publics de contrôle.

V. RECOMMANDATIONS

Nous estimons que la directive 2006/24/CE 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 est en tant que telle problématique et devrait faire l'objet de modifications permettant de trouver le juste équilibre entre la nécessaire répression des infractions et la protection des plus hautes valeurs protégées par notre Constitution.

C'est la raison pour laquelle nous estimons que le gouvernement devrait porter ce débat auprès de ses homologues européens afin d'obtenir une modification de la directive.

Il faut noter que la rétention de données personnelles a été déclarée inconstitutionnelle par les juridictions constitutionnelles d'Allemagne, Roumanie[18], Bulgarie[19], Chypre[20] et République tchèque[21]. La cour constitutionnelle fédérale allemande, dans un arrêt du 2 mars 2011, a estimé que la loi de transposition de la directive ne prévoyait pas suffisamment de précautions pour protéger le secret des correspondances électroniques. Selon cette dernière, « *un stockage des données relatives à la circulation des communications électroniques pendant six mois impose une grave restriction au secret de la correspondance en raison de son ampleur – presque toutes les communications sont concernées – qu'en raison du caractère sensible des données recueillies – elles peuvent permettre d'avoir un tableau complet des relations d'un individu et donc de ses préférences. De plus, les risques encourus par les citoyens sont importants – une seule communication peut donner une image erronée d'une personne et les risques d'abus de la part des opérateurs ne sont pas négligeables* »[22] .

Par ailleurs, la *High Court of Ireland* a posé une question préjudicielle à la Cour de justice de l'Union européenne concernant sa compatibilité avec le droit européen et la Convention européenne des droits de l'Homme[23]. L'arrêt de la Cour n'a pas encore été rendu mais il conviendrait, *a minima*, que **le législateur attende la réponse de la Cour avant de se lancer dans une transposition qui pourrait être contraire à la jurisprudence de celle-ci[24]**.

[18] Digital Civil Rights in Europe, « Romania : Data Retention Law Declared Unconstitutionnal », EDRI-gram, n° 7-20, 21 octobre 2009.
[19] Digital Civil Rights in Europe, « Bulgarian Court annuls a vague article of the data retention law », EDRI-gram, n° 6-24, 17 décembre 2008.
[20] Digital Civil Rights in Europe, « Data retention law provisions declared unlawful in Cyprus », EDRI-gram, n° 9-3, 9 février 2011.
[21] Digital Civil Rights in Europe, « Czech Constitutional Court rejects data retention legislation », EDRI-gram, n° 9-7, 6 avril 2011.
[22] Cité par M. FROMONT, « Le contrôle du respect du secret de la correspondance par une loi transposant une directive européenne », *Rev. trim. dr. h.*, 2010, n° 84, p. 946.
[23] C.J.U.E., Digital Rights Ireland Ltd c. Minister for Communication & Ors, 11 juin 2012, aff. C-293/12, JOUE, 25/08/2012, C 258/11; High Court of Ireland, 5 mai 2010, Digital Rights Ireland Ltd v. Minister for Communication & Ors, IEC 221, http://judgmental.org.uk/judgments/IEHC/2010/%5B2010%5D_IEHC_221.html.
[24] Par ailleurs, un document interne à la Commission, publié par le collectif de hackers autrichiens Quintessenz, révèle que la Commission a confirmé qu'il existe des doutes quant à la légalité de certains aspects de la directive en question. Pourtant, elle continue d'exiger que les Etats membres procèdent à sa transposition. Voir : http://quintessenz.org/doqs/000100011699/2011_12_15,Eu_Commission_data_retention_reform.pdf.