L'obligation de conservation des "métadonnnées"

Forget, Catherine

Published in:
Journal des Tribunaux

Publication date:
2017

Document Version
le PDF de l'éditeur

Bureau de dépôt : Louvain 1
Hebdomadaire, sauf juillet et août
ISSN 0021-812X
P301031

larcier

Journal des tribunaux

http://jt.larcier.be
1er avril 2017 - 136e année
13 - N° 6683
Georges-Albert Dal, rédacteur en chef

Sommaire

Doctrine

Jurisprudence

Chronique

Doctrine

L'obligation de conservation des « métadonnées » : la fin d'une longue saga juridique ?

L'arrêt Tele2 rendu le 21 décembre 2016 par la Cour de justice de l'Union européenne[1] apporte un nouvel éclairage sur l'obligation de conservation des « métadonnées » imposée aux opérateurs de communications électroniques à des fins de lutte contre la criminalité. Cet arrêt, sans mettre en cause l'efficacité d'un tel dispositif, vient mettre un sérieux frein à l'ardeur du législateur dans le domaine de la collecte « généralisée et indifférenciée » de données poursuivant une finalité répressive.

Introduction

L'obligation de conservation généralisée des « métadonnées »[2] imposée aux opérateurs et fournisseurs de réseaux et services de communications électroniques est une technique d'enquête controversée. La mesure consiste, en effet, en la collecte et le stockage systématique et *a priori* de l'ensemble des données traitées et générées lors d'une communication électronique à l'exception de leur contenu. Elle implique donc une ingérence « particulièrement grave » dans le droit au respect de la vie privée et à la protection des données à caractère personnel.

Entre, d'une part, la conservation des métadonnées par des acteurs privés et, d'autre part, l'accès à celles-ci par les autorités répressives, le législateur peine à établir un cadre adéquat. Au niveau européen, la directive 2006/24/CE a été déclarée « invalide » par la Cour de justice de l'Union européenne (ci-après C.J.U.E.) en raison de l'absence de garanties suffisantes permettant de limiter l'ingérence « au strict nécessaire ». Pour le même motif, la loi du 30 juillet 2013 transposant la directive précitée et modifiant l'article 126 de la loi du 13 juin 2005[3], a été annulée par la Cour constitutionnelle. Soucieux de tenir compte des enseignements de cette jurisprudence, le législateur a à nouveau modifié la loi du 13 juin 2005 par le biais de la loi du 29 mai 2016 sur la collecte et la conservation des données dans le secteur des communications électroniques[4]. Toutefois, l'arrêt de la C.J.U.E., prononcé le 21 décembre 2016, dit l'arrêt *Tele2*, remet indubitablement en cause la réglementation nationale actuelle.

(1) C.J.U.E., 21 décembre 2016, *Tele2 Sverige AB c. Post-och telestyrelsen et Secretary of State for the Home Department c. Tom Watson* e.a., aff. jointes C-203/15 et C-698/15 (ci-après l'arrêt *Tele2*).
(2) Les « métadonnées » sont les données traitées et générées lors d'une communication électronique à l'exception du contenu de celle-ci. Comme le soulignait déjà à l'époque Yves Poullet, « De telles données sont infinies : elles comprennent outre les données de simple connexion, leur durée, les destinataires de nos messages, les sites visités, la longueur des messages échangés, les caractéristiques du message et du système d'information de l'utilisateur ; les données de localisation révèlent à quelques mètres près l'endroit où se trouvent un mobilophone ou un G.P.S. même non en cours d'utilisation. C'est que l'utilisation de plus en plus intensive des technologies de l'information et la multiplication de services à valeur ajoutée qui leur sont attachées, trahissent les relations que nous nouons avec autrui, nos déplacements, nos goûts, nos convictions voire nos maladies, elles laissent en effet chez des intervenants de plus en plus nombreux et divers, des traces de plus en plus nombreuses en des lieux certes disparates mais certes susceptibles d'être reliés grâce aux vertus des réseaux et de systèmes de plus en plus performants de traitement de l'information. » Y. POULLET, « Lutte contre le crime et/ou vie privée : un débat difficile ! - À propos de l'alinéa 1er du paragraphe 2 de l'article 109*ter* de la loi belge du 25 mars 1991 introduit par la loi belge du 28 novembre 2000 sur la criminalité informatique », *Terminal*, 2003, p. 42.
(3) Loi du 30 juillet 2013 portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90*decies* du Code d'instruction criminelle, *M.B.*, 23 août 2013.
(4) Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques, *M.B.*, 18 juillet 2016.

1 Le champ d'application de la loi du 29 mai 2016

Avant de nous plonger dans le cœur des controverses juridiques, précisons la portée de la loi du 29 mai 2016 sur la collecte et la conservation des données dans le secteur des communications électroniques.

A. La collecte et le stockage des « métadonnées »

1. L'obligation de conservation *a priori* des « métadonnées » concerne les données traitées et générées lors d'une communication électronique, à l'exception du contenu de celle-ci. Une loi au sens formel du terme — l'article 126, § 3, de la loi du 13 juin 2005[5] — clarifie la portée de cette obligation en distinguant les données d'identification[6], les données d'accès et de connexion[7] et, enfin, les données de communication[8]. Toutefois, c'est au Roi qu'il revient d'établir la liste exacte des données devant être collectées par types de services[9]. À cet égard, aucun arrêté royal n'ayant été adopté depuis l'annulation par la Cour constitutionnelle de la loi du 30 juillet 2013, l'arrêté royal du 19 septembre 2013 reste d'application, à moins d'avoir fait l'objet d'un recours en temps utile devant le Conseil d'État[10].

2. Comme le précise le Groupe Article 29[11], même si le contenu des communications n'est pas concerné par une telle réglementation, l'étendue des « métadonnées » visées peut permettre de donner des informations très précises sur les abonnés et utilisateurs en raison de leur nature structurée[12]. Elles peuvent ainsi être regroupées, analysées et traitées afin d'établir certaines caractéristiques comportementales ou personnelles[13]. Vu le caractère exceptionnel d'une telle ingérence dans le droit à la vie privée, précisons déjà que la méthode de la « préservation de données » ou « gel rapide de données » — préconisée par la Convention de Budapest[14] — est souvent présentée comme une mesure alternative à celle de la loi du 29 mai 2016. Cette autre méthode consiste à conserver seulement *a posteriori* et à la suite d'une demande expresse des autorités certaines données traitées par une personne physique ou morale[15]. Les informations doivent alors être stockées dans les plus brefs délais et ce, pendant une période maximale de nonante jours, ce temps devant permettre aux enquêteurs d'accomplir des formalités supplémentaires[16].

B. Les acteurs concernés

3. L'obligation de conservation de données au sens de l'article 126 de la loi du 13 juin 2005 s'applique aux opérateurs et fournisseurs de communications électroniques (ci-après de manière générique « les opérateurs »)[17]. Afin de clarifier l'étendue des personnes tenues par l'obligation de conservation, l'Institut belge des services postaux et des télécommunications (ci-après « IBPT ») considère que par « opérateur », il y a lieu d'entendre non seulement toute personne soumise à l'obligation d'introduire une notification auprès de lui[18] mais également celle fournissant un « réseau de communications électroniques »[19] ou un « service de communications électroniques »[20] au public.

4. À l'inverse, ne sont pas visés par la disposition les fournisseurs de réseaux qui ne traversent pas le domaine public ainsi que les fournisseurs de services exclusivement destinés à une personne morale comme, par exemple, le réseau interne d'une entreprise[21]. Sont ainsi exclus les hôtels, les cafés, les restaurants, les maisons de repos offrant le Wi-Fi gratuit pour autant qu'« il soit fait en sorte que » le service Wi-Fi ne puisse pas être utilisé librement dans le domaine public, en appliquant un mot de passe par exemple[22]. En outre, les services « over the top » (ci-après OTT)[23] tels WhatsApp, Viber ou Facebook ne seraient pas concernés. À leur égard la question reste néanmoins controversée, d'autant plus que l'Union européenne projette de réglementer leurs activités afin de les soumettre aux obligations des opérateurs télécoms historiques[24]. Enfin, notons qu'une entreprise peut être qualifiée d'opérateur en fonction du service qu'elle propose, les catégories ne sont donc pas étanches[25].

(5) Loi du 13 juin 2005 relatives aux communications électroniques, *M.B.*, 20 juin 2005. Dans le cadre de cette contribution, nous mentionnons la loi du 13 juin 2005 telle que modifiée par la loi du 29 mai 2016.
(6) Selon l'article 126, § 3, alinéa 1, de la loi du 13 juin 2005, les données d'identification sont les données permettant d'identifier l'utilisateur ou l'abonné et les moyens de communications. Pour le téléphone fixe ou mobile, il s'agit par exemple, des numéros, noms et adresse de l'abonné. Pour Internet il peut s'agir des noms et adresses de l'utilisateur d'une adresse IP.
(7) Selon l'article 126, § 3, alinéa 2, de la loi du 13 juin 2005, les données d'accès et de connexion sont les données permettant de déterminer le type de communication, le matériel utilisé et les données permettant de le localiser s'il est mobile.
(8) Selon l'article 126, § 3, alinéa 3, de la loi du 13 juin 2005, les données de communication comprennent également l'origine et la destination de la communication. Il peut s'agir de, par exemple, la date, l'heure et la durée d'une communication, de l'ouverture et de la fermeture d'une session du service d'accès à l'internet et de l'adresse IP mais aussi de la session d'un service de courrier électronique.
(9) Article 126, § 3, alinéa 4, de la loi du 13 juin 2005.
(10) En effet, comme le souligne Marc Verdussen, après l'annulation d'une loi par la Cour constitutionnelle, les actes réglementaires pris sur la base de la norme annulée « demeurent dans l'ordre juridique, mais ils sont en sursis. En clair, l'annulation n'affecte pas comme telle l'existence de ces actes et décisions, leur validité pouvant toutefois être remise en cause par l'autorité administrative ou juridictionnelle qui les a adoptés. (...) On précisera qu'en aucun cas, l'autorité administrative ou juridictionnelle ne peut agir d'office. Son intervention est liée à un recours déclenché par un citoyen directement concerné par l'acte ou la décision qu'il entend voir invalider ». Voy. M. Verdussen, « Chapitre I - Dans l'ordre interne », *in Justice constitutionnelle*, Bruxelles, Larcier, 2012, pp. 358-359.
(11) Le Groupe de travail de l'Article 29 est institué par la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont précisées à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE. Les avis du Groupe Article 29 sont disponibles à l'adresse suivante : http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.
(12) Néanmoins, sur la base de cette distinction entre données de contenu et métadonnées, la C.J.U.E. en a déduit que l'obligation de conservation de métadonnées ne portait pas atteinte à l'essence du droit au respect de la vie privée. C.J.U.E., 8 avril 2014, *Digital Rights Ireland Ltd & Michael Seitlinger* e.a., aff. jointes C-293/12 et C-594/12, § 39 (ci-après arrêt *Digital Rights*).
(13) Groupe Article 29, avis 04/2014 sur la surveillance des communications électroniques à des fins de renseignement et de sécurité nationale, 10 avril 2014.
(14) La Convention de Budapest offre aux États membres de nouvelles dispositions en matière de criminalité informatique et de procédure pénale. Convention sur la cybercriminalité, Budapest, 23 novembre 2001, *S.T.C.E.*, n° 185.
(15) Sur ces notions, voy. Comité de la Convention sur la cybercriminalité du Conseil de l'Europe, « Rapport d'évaluation », 5-6 décembre 2012.
(16) Article 16 de la Convention sur la cybercriminalité, Budapest, 23 novembre 2001, *S.T.C.E.*, n° 185.
(17) Plus précisément, il s'agit des « opérateurs fournissant des réseaux publics de communications électroniques ainsi [qu'aux] opérateurs fournissant un de ces services » mais aussi aux « fournisseurs au public de services de téléphonie, en ce compris par Internet, d'accès à l'Internet, de courrier électronique par Internet ».
(18) Article 2, 11°, de la loi du 13 juin 2005. Pour une liste exemplative mais non exhaustive de 288 opérateurs concernées, voy. I.B.P.T., « List of Telecom Operators », 10 octobre 2016, disponible sur www.bipt.be.
(19) Article 2, 3°, de la loi du 13 juin 2005.
(20) Article 2, 5°, de la loi du 13 juin 2005.
(21) Ces deux exceptions sont prévues à l'article 9, §§ 5 et 6, de la loi du 13 juin 2005.
(22) I.B.P.T., Communication du Conseil de l'IBPT du 27 février 2015 concernant l'obligation de notification à l'IBPT en tant qu'opérateur, 21 octobre 215, p. 11.
(23) Il n'existe pas de définition pour les services « over the top » ; il est par contre communément admis que ces services utilisent les réseaux de communications existants pour fournir des services de communications.
(24) Les opérateurs de « réseaux de communications électroniques » classiques tels Orange ou Proximus, et les fournisseurs d'accès à Internet dénoncent la concurrence déloyale des services OTT, ceux-ci n'étant pas soumis aux « Paquet télécoms » découlant de différentes directives européennes. Il s'agit notamment de la connexion aux services d'urgence, l'obligation de collaboration en matière d'interception des communications ou encore l'enregistrement des données de communications. La Commission européenne, consciente de l'enjeu, s'est saisie de la question et a récemment publié une proposition de règlement. Voy. proposition de règlement du Parlement européen et du conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques »), Bruxelles, 10 janvier 2017, [COM(2017) 10 final], *J.O.*, 2017/0003(COD).
(25) Ainsi, lorsque Skype fournit un service type « SkypeOut » c'est-à-dire un service permettant d'effectuer des appels téléphoniques contre rémunération, il agit en tant qu'opérateur. Par contre, lorsque le service est fourni gratuitement, la société agissant en tant qu'OTT est actuellement exclue du champ d'application de la réglementation et n'est dès lors pas soumise à l'obligation de conservation de données. Sont également exclus du champ d'application de

C. La durée de conservation

5. En vertu de l'article 126, § 3, de la loi du 13 juin 2005, les « métadonnées » doivent être conservées pendant une période uniforme de douze mois. Par contre, le point de départ du délai diffère selon la catégorie de données concernée. Ainsi, les données d'identification doivent être conservées à partir « de la date à laquelle une communication est possible pour la dernière fois à l'aide du service utilisé », les données relatives à l'accès et à la connexion, « à partir de la date de la communication » et les données de communication, en ce compris l'origine et la destination, « à partir de la date de la communication ».

D. Les conditions d'accès

6. Une fois collectées et stockées *a priori* par les opérateurs, les métadonnées doivent être transmises « sans délai » sur simple demande des autorités énumérées par l'article 126, § 2, de la loi du 13 juin 2005[26].

7. En ce qui concerne les autorités judiciaires[27], la loi du 29 mai 2016 modifie le Code d'instruction criminelle (ci-après C.i.cr.) et distingue les données d'identification accessibles en application de l'article 46*bis* C.i.cr. et les données de trafic et de localisation accessibles en application de l'article 88*bis* C.i.cr. Ainsi, le procureur du Roi — ou en cas d'extrême urgence, un officier de police judiciaire — peut accéder aux données d'identification pour une durée limitée aux six derniers mois si l'infraction n'est pas de nature à emporter une peine d'emprisonnement correctionnel principal d'un an ou à une peine plus lourde[28]. Les données de trafic et de localisation peuvent, quant à elles, être sollicitées sur ordonnance du juge d'instruction « s'il existe des indices sérieux que les infractions peuvent donner lieu à une peine d'emprisonnement correctionnel principal d'un an ou à une peine plus lourde »[29]. L'accès est toutefois limité aux données stockées depuis six mois pour les infractions punies de un à cinq ans d'emprisonnement, neuf mois lorsque l'infraction est de nature à emporter une peine de cinq ans ou plus, douze mois lorsqu'il est question de terrorisme[30].

2 Les conditions d'ingérence aux droits au respect de la vie privée et à la protection des données

8. Une méthode d'enquête telle que l'obligation de conservation des « métadonnées » à des fins de lutte contre la criminalité emporte une atteinte aux droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel. Ces droits sans être absolus, sont garantis par différents instruments internationaux qui encadrent, par la voie d'exceptions, les conditions de l'ingérence constituée par la collecte et le stockage *a priori* de ces données.

A. La Charte des droits fondamentaux

9. Au sein de l'Union européenne, la Charte des droits fondamentaux (ci-après la Charte) garantit le droit à la vie privée et le droit à la protection des données à caractère personnel[31]. À la différence de l'article 8, § 1er, de la Convention européenne des droits de l'homme (ci-après la Convention)[32], celle-ci distingue expressément les deux droits et encadre dès lors tout traitement de données à caractère personnel indépendamment d'une atteinte éventuelle à la vie privée[33]. L'article 52, § 1er, de la Charte autorise les États membres à limiter la portée des droits et libertés par la voie législative pour autant la mesure respecte le contenu essentiel desdits droits et que, dans le respect du principe de proportionnalité, elle soit nécessaire et réponde effectivement à un objectif d'intérêt général reconnu par l'Union[34].

B. Les directives 95/46/CE et 2002/58/CE

10. L'Union européenne s'est également dotée de deux directives. La directive 95/46/CE[35] harmonise d'une manière générale les dispositions relatives à la protection des données et le droit au respect de la vie privée[36]. La directive 2002/58/CE[37] complète la directive 95/46/CE en s'appliquant spécifiquement au secteur des communications électroniques[38]. Celle-ci consacre expressément le principe de la confidentialité des communications[39]. Elle interdit le stockage des données de trafic[40] et de localisation[41] sauf lorsque la loi l'autorise

l'article 126 de la loi du 13 juin 2005, les intermédiaires au sens du Code de droit économique, les services disposant d'une responsabilité éditoriale et les services de radiodiffusion et télévision. I.B.P.T., Version non confidentielle de la décision du Conseil de l'IBPT du 30 mai 2016 relative à l'imposition d'une amende administrative à Skype Communications s. à r.l. pour le non-respect de l'article 9, § 1er, de la loi du 13 juin 2005, 15 juillet 2016, pp. 6-7.

(26) Article 126, § 2, de la loi du 13 juin 2005. Il s'agit des autorités judiciaires conformément aux articles 46*bis* et 88*bis* du Code d'instruction criminelle, des services de renseignements et de sécurité, de tout officier de police judiciaire de l'IBPT dans le cadre d'une infraction prévue aux articles 114 (sécurité des données), 124 (atteinte à la confidentialité des communications) et 126 de la loi du 30 juin 2005, des services d'urgence offrant de l'aide sur place lorsqu'ils ne disposent pas des données d'identification de l'appelant, de l'officier de police judiciaire de la Cellule des personnes disparues de la police fédérale, du Service de médiation pour les télécommunications dans le cas d'utilisation malveillante des services de communications électroniques ou d'un réseau et des autorités prévues par la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques.

(27) En ce qui concerne les autres autorités, la loi du 29 mai 2016 distingue également des périodes d'accès aux données par les services de renseignements et de sécurité selon la gravité de la menace, variant par exemple de six mois pour les menaces liées aux organisations sectaires nuisibles à douze mois pour les activités qui peuvent être liées à l'extrémisme. Par ailleurs, l'accès est limité aux données conservées depuis quarante-huit heures à dater de la demande en ce qui concerne la Cellule des personnes disparues et vingt-quatre heures pour les services d'urgence. En outre, les médecins ou les avocats bénéficient de garanties supplémentaires, l'accès à leurs « métadonnées » étant autorisé à la condition qu'ils soient eux-mêmes suspects dans le cadre d'une enquête et pour autant que le bâtonnier ou le représentant de l'ordre provincial des médecins en soit averti.

(28) Article 46*bis*, § 2, C.i.cr.

(29) Article 88*bis*, § 2, C.i.cr.

(30) Article 88*bis*, § 2, C.i.cr.

(31) Articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne.

(32) Convention européenne des droits de l'homme, *S.T.C.E.*, no 005, 1950. Au niveau du Conseil de l'Europe, l'article 8, § 1er, garantit le droit à la vie privée. Cet article inclut au terme d'une jurisprudence abondante, le droit à la protection des données à caractère personnel (voy. C.E.D.H., 4 mai 2000, *Amann c. Suisse*, no 27798/5, § 65). La Cour de Strasbourg examine les litiges qui lui sont soumis à la lumière de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel seul instrument contraignant en matière de protection de données au niveau international. Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, *S.T.C.E.*, no 108, 1981. (ci-après Convention 108) Ainsi, la Cour a eu l'occasion de préciser que la mémorisation des données relatives à la vie privée d'un individu, constitue en elle-même une atteinte au droit à la vie privée, peu importe que les informations mémorisées soient ou non utilisées par la suite. C.E.D.H., 4 décembre 2008, *S. Marper c. Royaume-Uni*, nos 30562/04 et 30566/04, § 67.

(33) C. Docksey, « Articles 7 and 8 of the EU Charter : two distinct fundamental rights », *in Quelle protection des données personnelles en Europe ?*, Bruxelles, Larcier, 2015, pp. 71-97.

(34) Article 52, § 1er, de la Charte des droits fondamentaux de l'Union européenne.

(35) 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, *J.O.* L 281 du 23 novembre 1995, p. 31. (ci-après la directive 95/46/CE).

(36) De manière similaire à la Convention 108, celle-ci encadre tout traitement de données dans le respect des principes de finalité, de loyauté et de proportionnalité. Voy. articles 6 et 8 de la directive 95/46/CE.

(37) 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, *J.O.C.E.* L 201/37 du 31 juillet 2002, pp. 0037-0047 (ci-après directive 2002/58/CE).

(38) Article 3 de la directive 2002/58/CE.

(39) Article 5 de la directive 2002/58/CE.

(40) Par données relatives au trafic, il y a lieu d'entendre données « traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation ». Voy. article 2, b), de la directive 2002/58/CE. Dans le cadre de l'acheminement d'une communication, les données de trafic doivent en principe être effacées ou anonymisées dès le moment où la communication a pris fin. Article 6, § 1er, de la directive 2002/58/CE.

(41) Article 9 de la directive 2002/58/CE. Par données de localisation, il y a lieu d'entendre « toutes les don-

expressément[42]. Ainsi ces données peuvent être stockées à des fins de facturation et uniquement pendant la période au cours de laquelle la facture peut encore être contestée ou lorsque des poursuites sont encore susceptibles d'être engagées afin d'en obtenir le paiement[43]. Par exception, l'article 15, § 1er, de la directive 2002/58/CE autorise les États membres à limiter la portée de certains droits et libertés par voie législative. Le texte précise toutefois que la mesure doit s'avérer « nécessaire, appropriée et proportionnée » au sein d'une société démocratique, afin de « 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 ».

C. Le règlement général sur la protection des données

11. Applicable à partir du 25 mai 2018, le règlement européen sur la protection des données à caractère personnel renforce les règles actuelles et les rassemble en un texte unique[44]. Il fixe les principes généraux relatifs au traitement de données à caractère personnel[45] et prévoit en son article 23, § 1er, une possibilité de limiter sous certaines conditions la portée des droits garantis. La mesure considérée ne peut avoir pour effet de porter atteinte à l'essence des droits et libertés fondamentaux, elle doit être nécessaire et proportionnée dans une société démocratique pour garantir par exemple, la sécurité nationale, la sécurité publique, la prévention et la détection d'infractions pénales ou encore pour permettre l'exécution des demandes de droit civil. Si l'article 23, § 1er, fait écho à l'article 52, § 1er, de la Charte des droits fondamentaux, il complète néanmoins celui-ci par une série de critères devant spécifiquement figurer dans la disposition nationale. Celle-ci doit notamment prévoir des dispositions relatives « aux finalités du traitement ou des catégories de traitement », « aux catégories de données à caractère personnel » mais aussi « aux durées de conservation et aux garanties applicables, en tenant compte de la nature, de la portée et des finalités du traitement ou des catégories de traitement »[46].

3 Les critères de l'obligation de conservation des « métadonnées »

A. Bref historique national

12. La Belgique s'est dotée une première fois d'une disposition imposant la conservation *a priori* de métadonnées par la loi du 28 novembre 2000 modifiant la loi du 21 mars 1991[47], celle-ci adaptant la procédure pénale belge afin de faciliter l'identification des auteurs d'infractions sur les réseaux numériques[48]. La mesure obligeait les fournisseurs et opérateurs de réseaux de télécommunications à conserver les données d'appel de moyens de télécommunications et les données d'identification des utilisateurs de ces services pendant une période minimum de douze mois[49].

À l'époque, la Commission européenne critiquait déjà l'absence de garanties suffisantes contre le risque d'accès illicite ou arbitraire aux données[50]. La loi du 13 juin 2005 relative aux communications électroniques[51] clarifia la disposition concernée. Celle-ci resta néanmoins critiquée par la Commission de la protection de la vie privée en raison de sa mise en œuvre indépendante de l'ouverture d'une enquête[52]. Toutefois, ces dispositions ne furent jamais effectives à défaut d'arrêtés royaux d'exécution[53].

B. La directive 2006/24/CE

13. Dans un contexte marqué par les attentats de Madrid et de Londres en 2004 et 2005, l'Union européenne se dota de la directive 2006/24/CE[54]. En vertu de l'article 1er, § 1er, de celle-ci, les métadonnées devaient être conservées pendant six à vingt-quatre mois et mises à la disposition des autorités à des « fins de recherche, de détection et de poursuite d'infractions graves »[55]. À la différence du projet de décision-cadre initialement proposé[56], la directive 2006/24/CE encadrait uniquement la *conservation* des données et non *l'accès* à celles-ci par les autorités nationales compétentes. En effet, avant l'adoption du Traité de Lisbonne, l'Union européenne était organisée en trois piliers[57]. Or la mesure pouvait concerner tant le premier pilier, vu l'objectif d'harmonisation des dispositions nationales[58], que le troisième pilier, les données étant collectées à des fins de lutte contre la grande criminalité et le terrorisme[59]. Saisie d'un recours en annulation, la Cour de justice de l'Union européenne avalisa la forme juridique choisie en reconnaissant un objectif « prépondérant » relevant du droit communautaire[60]. Par conséquent, il revenait aux États membres de

nées traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public ». Voy. article 2, c), de la directive 2002/58/CE.
(42) Articles 5 et 9 de la directive 2002/58/CE.
(43) Article 6, § 2, de la directive 2002/58/CE.
(44) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (texte présentant de l'intérêt pour l'E.E.E.), *J.O.* L 119 du 4 mai 2016, p. 1 (ci-après le règlement général sur la protection des données).
(45) Article 5 du règlement général sur la protection des données.
(46) Article 23, § 2, points a) à h), du règlement général sur la protection des données.
(47) Article 109*ter*, E, de la loi du 28 novembre 2000 relative à la criminalité informatique, *M.B.*, 3 février 2001, p. 02909.
(48) F. DE VILLENFAGNE et S. DUSSOLIER, « La Belgique sort enfin ses armes contre la cybercriminalité : à propos la loi du 28 novembre 2000 sur la criminalité informatique », *A&M*, 2001, nº 1, p. 71.
(49) Article 109*ter*, E, § 2, alinéa 1, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, *M.B.*, 27 mars 1991. Notons que selon la Commission de la protection de la vie privée, il eut été préférable de fixer le délai exact et la liste des données dans la loi plutôt que par arrêté royal et ceci afin de limiter la marge de manœuvre confiée au pouvoir exécutif conformément à l'article 22 de la Constitution. Avis publié in *Doc. parl.* Chambre, 0213/004, p. 30.
(50) *Doc. parl.*, Chambre, 1999-2000, 0213/011, p.18.
(51) Article 126 de la loi du 13 juin 2005, *M.B.*, 20 juin 2005, p. 28070.
(52) La Commission de la protection de la vie privée rappela que « ni les textes internationaux (...), ni la loi du 8 décembre 1992 (principes de proportionnalité, durée limitée...) n'autorisent les méthodes de surveillance globale indépendamment d'instructions relatives à des infractions particulières (si l'on excepte le cas très particulier de la recherche proactive, qui est strictement encadrée) », C.P.V.P., avis nº 08/2004 du 14 juin 2004 sur l'avant-projet de loi relatif aux communications électroniques.
(53) A. CASSART et J.-F. HENROTTE, « L'invalidation de la directive 2006/24 sur la conservation des données de communication électronique ou la chronique d'une mort annoncée », *J.L.M.B.*, 2014, p. 955.
(54) 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, *J.O.* L 105 du 13 avril 2006, pp. 54-63, (ci-après directive 2006/24/CE).
(55) Article 1, § 1er, de la directive 2006/24/CE.
(56) Conseil européen, projet de décision-cadre sur la conservation de données traitées et stockées en relation avec la mise à disposition de services de communications électroniques disponibles publiquement ou de données sur les réseaux de communications publiques aux fins de la prévention, l'étude, la détection et la poursuite des actes criminels, y compris le terrorisme, version partiellement publique du 8 novembre 2004.
(57) F. DUMORTIER et Y. POULLET, « La protection des données à caractère personnel dans le contexte de la construction en piliers de l'Union européenne », *Défis du droit à la protection à la vie privée*, vol. 31, 2008.
(58) Article 1, § 1er, de la directive 2006/24/CE. Dans le cadre du premier pilier, le législateur européen pouvait prendre des dispositions relatives au marché intérieur sous la forme de directives (article 95 ainsi que les articles 251 et s. du Traité UE).
(59) Considérant 21 de la directive 2006/24/CE. Dans le cadre du troisième pilier, réservé au domaine de la « coopération policière et judiciaire en matière pénale », il devait intervenir sous la forme de décisions-cadres. Voy. article 31, § 1er, point c), du Traité UE.
(60) Selon la Cour, la directive 2006/24/CE s'applique indépendamment « de la mise en œuvre de toute éventuelle action de coopération policière et judiciaire en matière pénale » et « n'harmonise 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 ». Le juge de Luxembourg en déduit que, même si le texte comprend des éléments de droit pé-

prévoir, dans leurs droits internes, des garanties suffisantes régissant l'accès des autorités aux données collectées.

C. La transposition de la directive 2006/24/CE en droit interne

14. Après deux projets de loi controversés[61], le législateur belge adopta dans l'urgence et sous la pression de la Commission[62], la loi du 30 juillet 2013[63] en vertu de laquelle les fournisseurs de communications électroniques devaient conserver les données durant douze mois, période susceptible d'être portée à vingt-quatre mois, voire à trente-six mois dans certains cas exceptionnels[64]. Cette loi fut complétée par l'arrêté royal du 19 septembre 2013[65] qui détermine, par type de services, les métadonnées devant être conservées[66].

D. L'arrêt *Digital Rights* de la C.J.U.E. du 8 avril 2014

15. Peu après la transposition de la directive 2006/24/CE dans l'ordre juridique belge, la C.J.U.E., saisie de deux questions préjudicielles, invalida *ab initio* la directive 2006/24/CE en s'appuyant sur trois points essentiels[67]. Premièrement, elle fit le constat du caractère généralisé du dispositif en cause, les données étant collectées de manière globale indépendamment d'un lien entre l'attitude des personnes et des éventuelles infractions graves[68]. Deuxièmement, elle pointa l'absence d'un cadre procédural ou matériel permettant de limiter l'accès aux données collectées ou l'utilisation de celles-ci par les autorités nationales[69]. Troisièmement, la Cour souligna au sujet de la durée de conservation de six à vingt-quatre mois l'absence de lien entre les différentes catégories de données collectées et l'objectif poursuivi[70]. Elle conclut que l'ingérence était donc « d'une vaste ampleur et d'une gravité particulière » sans être « précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire »[71].

16. À ce stade, relevons que la Cour passa sous silence la difficulté inhérente à la forme juridique choisie par le législateur de l'Union à savoir une directive et non une décision-cadre. En effet, finalement adoptée dans le cadre du premier pilier, la directive 2006/24/CE ne régulait pas les conditions d'accès aux données par les autorités nationales, dans le souci d'éviter le risque pour le législateur communautaire de violer les règles de répartition des compétences. Or la Cour ne précisa pas quelle eut-été sa position si l'accès aux données avait été encadrée par la réglementation soumise à son contrôle, laissant ainsi la porte ouverte à des possibles interprétations divergentes sur la teneur de sa décision.

E. L'arrêt « rétention de données » de la Cour constitutionnelle du 11 juin 2015

17. Dans le même sens, et à l'instar d'autres juridictions nationales européennes[72], la Cour constitutionnelle annula avec effet rétroactif la loi du 30 juillet 2013 transposant la directive 2006/24/CE dans l'ordre interne[73]. Alignant son argumentaire sur l'arrêt *Digital Rights*, la Cour conclut que « par identité des motifs avec ceux qui ont amené la Cour de justice de l'Union européenne à juger la directive conservation des données invalide »[74], le législateur national a dépassé les limites qu'impose le respect du principe de proportionnalité[75].

18. Ce raisonnement pour le moins rapide, appelle plusieurs observations. Premièrement, la Cour constitutionnelle a omis de tenir compte de différences essentielles entre la directive 2006/24/CE et la loi du 30 juillet 2013. À la différence de la directive, la loi attaquée encadrait l'accès aux données puisqu'elle se référait aux articles 46*bis* et 88*bis* du Code d'instruction criminelle et à la loi du 30 novembre 1998 relative aux services de renseignements et de sécurité[76]. Deuxièmement, la Cour constitutionnelle examina la légalité de la loi du 30 juillet 2013 sans prendre en considération la disparition de la directive 2006/24/CE de l'ordre juridique européen. Or, une fois cette norme européenne invalidée, la disposition nationale aurait dû être examinée au regard des critères établis par l'article 15, § 1er, de la directive 2002/58/CE en combinaison avec les articles 7, 8 et 52, § 1er, de la Charte. Quoiqu'il en soit, le législateur s'empressa d'adopter une nouvelle loi pour combler le vide juridique laissé.

F. La loi du 29 mai 2016 : une loi s'annonçant réparatrice

19. Lors des travaux parlementaires de la loi du 29 mai 2016, le législateur indiqua intégrer, dans la mesure du possible, les critiques adressées par la C.J.U.E. et par la Cour constitutionnelle[77]. En effet, aucune de ces juridictions n'avait précisé si les critères de proportionnalité suggérés quant à la *conservation* et à *l'accès* devaient se cumuler — conduisant implicitement à l'interdiction de principe d'une obligation générale de conservation de données, ou pouvaient se compenser l'un l'autre[78]. Le législateur pencha plutôt pour la seconde option[79]. Ainsi, la loi du 29 mai 2016 catégorise sommairement[80] les métadonnées devant être conservées, renforce les conditions d'accès des autorités compétentes en limitant leur période d'accès en fonction de l'infraction considérée[81], et enfin, renforce la sécurisation des données conservées par les opérateurs[82]. Néanmoins, en dépit du caractère

nal, on ne saurait vider la compétence du législateur dans le cadre du premier pilier. C.J.U.E., 10 février 2009, *Irlande c. Parlement européen et Conseil*, aff. C-301/06, §83.

(61) Le premier projet de loi n'emporta pas la conviction de la Commission de la protection de la vie privée. Celle-ci considéra que le texte laissait une marge de manœuvre trop importante au pouvoir exécutif, prévoyait peu de garanties quant à la conservation des données et ne justifiait pas la nécessité de conserver celles-ci durant vingt-quatre mois. Voy C.P.V.P., avis n° 24/2008 du 2 juillet 2008, pp. 7 et 13. Le second projet de loi fut par contre approuvé mais assorti de certaines conditions, dont notamment celles de limiter la durée de conservation des données à une période maximale de douze mois et de fixer cette durée dans la loi plutôt que par arrêté royal. Voy. C.P.V.P., avis n° 20/2009 du 1er juillet 2009, pp. 7 et 13. La disposition resta toutefois « au frigo » en raison notamment de la chute du gouvernement le 26 avril 2010.

(62) Le 30 mai 2013, la Commission européenne demanda à la Belgique de mettre sa législation en conformité avec la directive. À défaut d'une transposition dans les deux mois, celle-ci menaçait de saisir la C.J.U.E. Mémo de la Commission européenne du 30 mai 2013 sur les procédures d'infraction du mois de mai, MEMO/13/470, 30 mai 2013.

(63) Loi du 30 juillet 2013 portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90*decies* du Code d'instruction criminelle, *M.B.*, 23 août 2013.

(64) Rapport fait au nom de la commission du Sénat, *Doc. parl.*, Sénat, 2012-2013, n° 5-2222/3.

(65) A.R. du 19 septembre 2013 portant exécution de l'article 126 de la loi du 13 juin 2005, *M.B.*, 8 octobre 2013.

(66) Rapport fait au nom de la commission du Sénat, *Doc. parl.*, Sénat, 2012-2013, n° 5-2222/3.

(67) C.J.U.E., 8 avril 2014, *Digital Rights Ireland Ltd & Michael Seitlinger* e.a., aff. jointes C-293/12 et C-594/12. Pour un commentaire voy. P. Dethy, « Quelques réflexions à la suite de l'arrêt de la Cour de justice n° C-293/12, C-594/12 du 8 avril 2014 », *RDIR* 2014, liv. 3, pp. 343-349.

(68) Point 58 de l'arrêt *Digital Rights*.

(69) Point 60 de l'arrêt *Digital Rights*.

(70) Point 63 de l'arrêt *Digital Rights*.

(71) Point 65 de l'arrêt *Digital Rights*.

(72) Les Cours constitutionnelles roumaine, allemandes, tchèque, bulgare et chypriote ont en effet annulé totalement ou partiellement les lois nationales transposant la directive 2006/24/CE. Pour une analyse des différentes décisions nationales voy. F. Boehm et M.D. Cole, « Data retention after the Judgement of the Court of Justice of the European Union, Münster/Luxembourg », 30 juin 2014, pp. 14-18.

(73) C. const., 11 juin 2015, n° 84/2015.

(74) C. const., 11 juin 2015, n° 84/2015, point B.11.

(75) C. const., 11 juin 2015, n° 84/2015, point B.10.1. La Cour constitutionnelle estima que la loi belge comportait une ingérence dans les droits fondamentaux de presque l'entièreté de la population et qu'elle était entachée de lacunes, à savoir l'absence de limite relative à une zone géographique déterminée ou à une période temporelle et l'absence de relation entre l'objectif poursuivi, la durée de la conservation et le type de données collectées. Pour un commentaire d'arrêt voy. C. Conings et F. Verbruggen, « Grondwettelijk Hof plaatst reparateurs dataretentiewet voor moeilijke opdracht », *Juristenkrant* 2015, afl. 312, pp. 1 et 3.

(76) Par ailleurs, contrairement à l'article 52, § 1er, de la Charte, l'article 22 de la Constitution exige de fixer les conditions d'ingérence dans le droit à la vie privée dans une loi au sens formel du terme et de limiter la délégation au pouvoir exécutif. La Cour constitutionnelle n'examina pourtant pas cet aspect.

(77) *Doc. parl.*, Chambre, 2015-2016, doc 54, 1567/001, p. 76.

(78) *Doc. parl.*, Chambre, 2015-2016, doc 54, 1567/001, p. 11.

(79) Reprenant les termes de la CPVP, le législateur indique : « aucun des deux arrêts ne conclut qu'un seul des quatre éléments suffit à constituer une violation du principe de proportionnalité. Si un élément déterminé des arrêts ne peut pas être retenu, il faut compenser cet élément par un régime plus strict sur les autres aspects » (*Doc. parl.*, Chambre, 2015-2016, doc 54, 1567/001, p. 13).

(80) Pour rappel, l'article 126, § 3, de la loi du 13 juin 2005 distingue les données d'identification, les données d'accès et de connexion et, enfin, les données de communication.

(81) Voy. *supra*.

(82) Ces derniers sont notamment tenus d'assurer les mêmes exigences de sécurité et de protection que les données sur le réseau, de veiller à l'adoption de mesures techniques et organisationnelles appropriées, de ré-

« réparateur » de la loi du 29 mai 2016, sa légalité est remise en cause compte tenu de l'arrêt *Tele2* de la C.J.U.E. du 21 décembre 2016.

4 Les conditions d'une conservation des données selon l'enseignement de l'arrêt *Tele2*

20. L'affaire *Tele2* récemment rendue par la C.J.U.E., fait suite à deux questions préjudicielles posées par les juridictions suédoise et britannique. Celles-ci s'interrogent sur la compatibilité au droit de l'Union d'une réglementation nationale imposant la conservation de données telle que le prévoyait la directive 2006/24/CE[83]. Ce faisant, la Cour est amenée à préciser la portée de l'arrêt *Digital Rights* et saisit l'occasion de préciser les conditions d'une conservation de données indépendamment des conditions d'accès à ces données par les autorités compétentes.

A. L'interdiction d'une conservation « généralisée et indifférenciée » des métadonnées

21. S'alignant ici sur sa propre jurisprudence, la Cour caractérise l'ingérence d'une réglementation imposant la conservation généralisée des métadonnées de « particulièrement grave » et de « vaste ampleur » dans l'exercice du droit à la vie privée et à la protection des données à caractère personnel[84]. En conséquence, la Cour rappelle que l'examen de la proportionnalité doit s'opérer dans le respect des « limites du strict nécessaire »[85]. Ensuite, la Cour dénonce un changement de paradigme puisque, en imposant une collecte et le stockage généralisée de données, l'interdiction de conserver celles-ci devient la règle au contraire d'être l'exception comme le prévoit pourtant la *ratio legis* de l'article 15, § 1er, de la directive 2002/58/CE[86].

22. En outre, une telle disposition s'applique à « tous les abonnés et utilisateurs inscrits et vise tous les moyens de communication électroniques ainsi que l'ensemble des données relatives au trafic, ne prévoit aucune différenciation, limitation ou exception en fonction de l'objectif poursuivi. Elle concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques, sans que ces personnes se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales. Elle s'applique donc même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions pénales graves. En outre, elle ne prévoit aucune exception, de telle sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel »[87]. Et la Cour de conclure qu'une telle réglementation nationale « excède donc les limites du strict nécessaire et ne saurait être considérée comme étant justifiée, dans une société démocratique » au regard des dispositions dont elle assure le contrôle[88].

B. Les critères d'une conservation « ciblée » de données

23. En revanche, selon la Cour, l'article 15, § 1er, de la directive 2002/58/CE ne s'oppose pas à une « réglementation permettant, à titre préventif, la conservation ciblée des données relatives au trafic et des données de localisation, à des fins de lutte contre la criminalité grave » mais dans le respect de certaines conditions[89]. En premier lieu, le texte doit contenir des garanties suffisantes c'est-à-dire une réglementation claire, accessible et prévisible permettant d'éviter tout risque d'abus et de protéger efficacement les données à caractère personnel[90]. En second lieu, des conditions matérielles relatives à la conservation des données doivent établir « un rapport entre les données à conserver et l'objectif poursuivi. En particulier, de telles conditions doivent s'avérer, en pratique, de nature à délimiter effectivement l'ampleur de la mesure et, par suite, le public concerné »[91]. Et la Cour de préciser ce qu'elle entend par « public et situations potentiellement concernées », à savoir qu'il s'agit de fixer dans la réglementation « des éléments objectifs permettant de viser un public dont les données sont susceptibles de révéler un lien, au moins indirect, avec des actes de criminalité grave, de contribuer d'une manière ou d'une autre à la lutte contre la criminalité grave ou de prévenir un risque grave pour la sécurité publique »[92].

24. La Cour rappelle ainsi les critères mentionnés dans l'arrêt *Digital Rights*, en précisant cette fois sans ambiguïté leur caractère cumulatif et ceci, indépendamment des modalités d'accès aux données. De manière prospective, la Cour semble appliquer les critères retenus par l'article 23, § 2, du règlement général sur la protection des données. Celui-ci impose de fixer dans la réglementation des dispositions spécifiques relatives « aux durées de conservation et aux garanties applicables, en tenant compte de la nature, de la portée et des finalités du traitement ou des catégories de traitement »[93].

5 Les conséquences de l'arrêt *Tele2* en droit interne : vers la conservation *a posteriori* des données ?

25. Depuis l'arrêt *Tele2*, il paraît difficile d'affirmer que la loi du 29 mai 2016 rencontre les exigences formulées par la C.J.U.E. alors que celle-ci condamne clairement la conservation « générale et indifférenciée » de données indépendamment des conditions d'accès. En effet, les améliorations apportées par le législateur national[94] ne sauraient suffire à respecter les exigences d'une collecte « ciblée » des données, exigences qui imposent de fixer dans la réglementation l'ampleur de la mesure et le public concerné en fonction de l'objectif poursuivi.

26. En filigrane, les critères suggérés par la C.J.U.E. par le biais de l'arrêt en cause rappellent la mesure de préservation de données ou de « gel rapide de données » encore appelée « quick freeze » dont nous avons déjà fait mention *supra*[95]. Dans ce cadre, les données ne sont pas conservées *a priori* mais *a posteriori*, les enquêteurs ordonnant de

pondre aux demandes des autorités par le biais de la Cellule de coordination, de conserver les données sur le territoire de l'Union européenne et d'assurer une journalisation des données. En outre, les critères paraissant peu applicables à savoir, différencier les personnes ont les données sont collectées ou prévoir des zones géographiques particulières sont omis par le législateur (*Doc. parl.*, Chambre, 2015-2016, doc 54, 1567/001, p. 11).

(83) En particulier, la Cour effectue son examen au regard de l'article 15, § 1er, de la directive 2002/58/CE pris à la lumière des articles 7, 8, 11 et 52, § 1er, de la Charte des droits fondamentaux de l'Union européenne.

(84) Point 100 de l'arrêt *Tele2*. Au point 96 de l'arrêt *Tele2*, la Cour rappelle que ces données « prises dans leur ensemble » peuvent donner des informations très précises relevant de la vie privée des personnes voire d'établir « le profil des personnes concernées, information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications ».

(85) Point 96 de l'arrêt *Tele2*.

(86) Point 104 de l'arrêt *Tele2*.

(87) Point 105 de l'arrêt *Tele2*.

(88) Point 107 de l'arrêt *Tele2*.

(89) Point 108 de l'arrêt *Tele2*.

(90) Point 109 de l'arrêt *Tele2*. La Cour ajoute que texte doit donc « indiquer en quelles circonstances et sous quelles conditions une mesure de conservation des données peut, à titre préventif, être prise » Ce critère est également rappelé à de nombreuses reprises par la Cour européenne des droits de l'homme. Voy. C.E.D.H., 2 août 1984, *Malone c. Royaume-Uni*, série A, n° 82, § 67, ainsi que *Gillan et Quinton c. Royaume-Uni*, 12 janvier 2010, n° 4158/05, § 77, *CEDH* 2010) ».

(91) Point 110 de l'arrêt *Tele2*.

(92) Point 111 de l'arrêt *Tele2*.

(93) Article 23, § 2, b) à h), du règlement général sur la protection des données.

(94) En vertu de l'article 126, § 3, de la loi du 13 juin 2005 tel que modifié par la loi du 29 mai 2016, les données sont catégorisées mais conservées durant une période unique de douze mois et ce, indépendamment de leur intérêt potentiel dans le cadre d'enquêtes pénales. De plus, la mesure présente toujours le risque d'atteinte au secret professionnel, les données des avocats et des médecins étant stockées indépendamment de leur caractère confidentiel. Notons que la proposition initiale suggérait de conserver les données d'identification durant douze mois. Les données de connexion et de localisation devaient être conservées entre neuf et douze mois. Seules les données de communication devaient être conservées deux mois. En définitive, plus les données sont potentiellement utiles pour les enquêteurs, plus la durée de conservation aurait été longue (*Doc. parl.*, Chambre, 2015-2016, doc. 54, 1567/001, p. 11).

(95) Article 16 de la Convention sur la cybercriminalité, Budapest, 23 novembre 2001, *S.T.C.E.*, n° 185. Voy. § 2 de la présente contribution.

manière provisoire et ciblée la préservation immédiate des données de manière à éviter de perdre des éléments pouvant s'avérer utiles dans le cadre d'enquêtes pénales. Une telle méthode, évoquée par le Groupe Article 29 et le Contrôleur européen de la protection des données[96], limiterait la gravité de l'ingérence dans la vie privée des personnes bien qu'elle s'appliquerait aussi aux données de contenu[97].

27. Au niveau national, le législateur a récemment adopté l'article 39*ter* du Code d'instruction criminelle, disposition qui transpose la mesure de préservation des données telle que préconisée par la Convention de Budapest[98]. Ainsi, dans le cadre de la poursuite de crimes ou de délits, cette disposition permet à tout officier de police judiciaire d'imposer la préservation immédiate des données traitées par une personne physique ou morale s'il existe des raisons de croire que ces données sont susceptibles de perte ou de modification. La décision doit être écrite et motivée et ne peut avoir une portée excédant nonante jours. Notons deux distinctions notables avec l'obligation de conservation de données au sens de l'article 126 de la loi du 13 juin 2005. Premièrement, le champ d'application est plus large puisque les enquêteurs peuvent saisir les données de contenu. Deuxièmement, la mesure s'impose à toute personne physique et morale, et non pas uniquement aux « opérateurs » ou « fournisseurs de services de communications électroniques ». En tout état de cause, la préservation de données fait donc à présent partie de notre arsenal législatif.

Conclusions

Dans son arrêt *Tele2*, la C.J.U.E. censure une obligation de conservation de données imposée aux opérateurs en raison de son caractère « généralisé et indifférencié » et préconise une conservation « ciblée » des données. Si cette décision clarifie la position de la Cour, elle passe sous silence des questions essentielles relatives à la nécessité d'adopter un tel dispositif à des fins de lutte contre la criminalité.

Tout d'abord, indépendamment d'une obligation légale de conservation telle que la prévoit l'article 126 de la loi du 13 juin 2005, les opérateurs peuvent stocker des métadonnées à des fins de marketing et de facturation en vertu des articles 122 et 123 de la même loi[99]. Ces données sont également accessibles sur demande des autorités judiciaires dans les conditions prévues par les articles 46*bis* et 88*bis* du Code d'instruction criminelle. Toutefois, celles-ci n'étant pas répertoriées ou listées par les opérateurs, il n'est pas possible de déterminer si les données conservées en vertu des articles 122 et 123 de la loi du 13 juin 2005 diffèrent de celles traitées et conservées en vertu de son article 126. Dans l'hypothèse où ces données ne se recouperaient pas, il eût été intéressant de déterminer l'intérêt des données collectées à des fins de facturation dans le cadre d'enquêtes pénales et en conséquence, la réelle nécessité d'imposer la conservation de données supplémentaires aux opérateurs.

Une seconde remarque concerne la durée de conservation de douze mois prévue par la loi du 29 mai 2016. Les statistiques de l'IBPT relèvent que la majorité des métadonnées exigées par les autorités datent de moins de trois mois[100]. On peut dès lors s'interroger sur la nécessité de prévoir une durée de conservation quatre fois plus longue et, à tout le moins, plus longue que celle nécessaire à des fins de facturation, comme le fit observer à de nombreuses reprises le Groupe Article 29[101].

Enfin, les obstacles rencontrés par le législateur mettent en lumière l'exercice difficile d'encadrer par le biais d'une seule et même mesure à la fois le traitement de données par les opérateurs et l'accès à ces données par les autorités nationales compétentes. Cette approche traduit l'idée récurrente du législateur de confier une mission d'intérêt public à des acteurs privés. Or, comme le soulignait déjà Yves Poullet il y a presque quinze ans : « Cette constatation a des conséquences sur le fondement de la légitimité des traitements et bien évidemment sur le statut des personnes tenues à cette conservation »[102]. Quoi qu'il en soit, la balle est à présent dans le camp de la Cour constitutionnelle puisque l'Ordre des barreaux francophones et germanophone et les a.s.b.l. Liga voor Mensenrechten et Ligue des droits de l'homme ont introduit des recours en annulation à l'encontre de la loi du 29 mai 2016.

Catherine FORGET[103]
Avocate au barreau de Bruxelles
Chercheuse au CRIDS (UNamur)

(96) C.E.P.D., avis du 26-9-2005 sur la proposition de directive du Parlement européen et du Conseil sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, et modifiant la directive 2002/58/CE [COM(2005) 438 final], *J.O.* C 298 du 29 novembre 2005. Notons que le C.E.P.D. se définit comme « une autorité de contrôle indépendante, qui veille à ce que les institutions et organes communautaires respectent leurs obligations en matière de protection des données. Ces règles sont énoncées dans le règlement (CE) n° 45/2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données ». Voy. le site internet du C.E.P.D. : https://secure.edps.europa.eu/EDPSWEB/edps/lang/fr/EDPS/Dataprotection/QA/QA1.
(97) Groupe Article 29, avis 9/2004 sur le projet de décision-cadre sur la conservation de données traitées et stockées en relation avec la mise à disposition de services de communications électroniques disponibles publiquement ou de données sur les réseaux de communications publiques aux fins de la prévention, l'étude, la détection et la poursuite des actes criminels, y compris le terrorisme. Proposition présentée par la France, l'Irlande, la Suède et la Grande-Bretagne (Document du Conseil 8958/04 du 28 avril 2004), adoptée le 9 novembre 2004.
(98) Loi du 22 décembre 2016 portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocales, *M.B.*, 19 janvier 2017.
(99) Ces articles transposent les articles 5 et 6 de la directive 2002/58/CE dont nous avons fait mention *supra*.
(100) I.B.P.T., Informations statistiques : conservation des données pour 2014 et 2015, version à destination du public, 27 septembre 2016, p. 6.
(101) Groupe Article 29, recommandation 3/99 relative à la préservation des données de trafic par les fournisseurs de services Internet pour le respect du droit, 7 septembre 1999, p. 7. Les avis du Groupe Article 29 sont disponibles à l'adresse suivante : http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.
(102) Y. POULLET, « Lutte contre le crime et/ou vie privée : un débat difficile ! - À propos de l'alinéa 1er du paragraphe 2 de l'article 109*ter* de la loi belge du 25 mars 1991 introduit par la loi belge du 28 novembre 2000 sur la criminalité informatique », *Terminal*, 2003, p. 32.
(103) L'auteure remercie vivement Franck Dumortier pour son apport scientifique et ses précieuses relectures.