# Cour constitutionnelle (Cour d'Arbitrage): Arrêt du 11 juin 2015 (Belgique). RG 84/2015

* Datum : 11-06-2015
* Taal : Frans
* Sectie : Rechtspraak
* Bron : Justel F-20150611-2
* Rolnummer : 84/2015

La Cour constitutionnelle,

composée des présidents J. Spreutels et A. Alen, et des juges E. De Groot, L. Lavrysen, J.-P. Snappe, J.-P. Moerman, E. Derycke, T. Merckx-Van Goey, P. Nihoul, F. Daoût, T. Giet et R. Leysen, assistée du greffier F. Meersschaut, présidée par le président J. Spreutels,

après en avoir délibéré, rend l'arrêt suivant :

I. Objet des recours et procédure

a. Par requête adressée à la Cour par lettre recommandée à la poste le 21 février 2014 et parvenue au greffe le 24 février 2014, l'Ordre des barreaux francophones et germanophone, assisté et représenté par Me E. Lemmens et Me J.-F. Henrotte, avocats au barreau de Liège, a introduit un recours en annulation de l'article 5 de la 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 90decies du Code d'instruction criminelle » (publiée au Moniteur belge du 23 août 2013).

b. Par requête adressée à la Cour par lettre recommandée à la poste le 24 février 2014 et parvenue au greffe le 25 février 2014, un recours en annulation de la loi du 30 juillet 2013 précitée a été introduit par l'ASBL « Liga voor Mensenrechten » et l'ASBL « Ligue des Droits de l'Homme », assistées et représentées par Me R. Jespers, avocat au barreau d'Anvers.

Ces affaires, inscrites sous les numéros 5856 et 5859 du rôle de la Cour, ont été jointes.

(...)

II. En droit

(...)

B.1.1. L'Ordre des barreaux francophones et germanophone, partie requérante dans l'affaire n° 5856, demande l'annulation de l'article 5 de la 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 90decies du Code d'instruction criminelle ».

L'ASBL « Liga voor Mensenrechten » et l'ASBL « Ligue des Droits de l'Homme », parties requérantes dans l'affaire n° 5859, demandent l'annulation des articles 1er à 7 de la même loi.

B.1.2. La loi du 30 juillet 2013 attaquée dispose :

« Article 1er. La présente loi règle une matière visée à l'article 78 de la Constitution.

Art. 2. La présente loi transpose partiellement en droit belge la Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la Directive 2002/58/CE (directive ' conservation de données ') (Journal officiel, 13 avril 2006, L 105/54) et l'article 15.1 de la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive ' vie privée et communications électroniques ') (Journal officiel, 31 juillet 2002, L 201/37).

CHAPITRE 2. - Modifications de la loi du 13 juin 2005 relative aux communications électroniques

Art. 3. L'article 1er de la loi du 13 juin 2005 relative aux communications électroniques, modifié par la loi du 10 juillet 2012, est complété par un alinéa rédigé comme suit :

' La présente loi transpose partiellement la Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la Directive 2002/58/CE (directive "conservation de données") (Journal officiel, 13 avril 2006, L 105/54) et l'article 15.1 de la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive "vie privée et communications électroniques") (Journal officiel, 31 juillet 2002, L 201/37). ' ».

Art. 4. A l'article 2 de la même loi, modifié par les lois des 18 mai 2009 et 10 juillet 2012, les modifications suivantes sont apportées :

a) le 11° est remplacé par ce qui suit :

' 11° "opérateur" : toute personne soumise à l'obligation d'introduire une notification conformément à l'article 9; ';

b) l'article est complété par un 74° rédigé comme suit :

' 74° "Appels infructueux" : toute communication au cours de laquelle un appel a été transmis mais est resté sans réponse ou a fait l'objet d'une intervention de la part du gestionnaire du réseau. '.

Art. 5. L'article 126 de la même loi est remplacé par ce qui suit :

' Art. 126. § 1er. Sans préjudice de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, les fournisseurs au public de services de téléphonie fixe, de téléphonie mobile, d'accès à l'internet, de courrier électronique par internet et de téléphonie par internet, ainsi que les fournisseurs des réseaux publics de communications électroniques sous-jacents, conservent les données de trafic, les données de localisation, les données d'identification d'utilisateurs finals, les données d'identification du service de communications électroniques utilisé et les données d'identification de l'équipement terminal qui est présumé avoir été utilisé, qui sont générées ou traitées par eux dans le cadre de la fourniture des services de communications concernés.

Par fournisseurs au sens du présent article, on entend également les revendeurs en nom propre et pour leur propre compte.

Par service de téléphonie au sens du présent article, on entend les appels téléphoniques - notamment les appels vocaux, la messagerie vocale, la téléconférence et la communication de données -, les services supplémentaires - notamment le renvoi ou le transfert d'appels - et les services de messagerie et multimédias, notamment les services de messages brefs (SMS), les services de médias améliorés (EMS) et les services multimédias (MMS).

Le Roi fixe, par arrêté délibéré en Conseil des Ministres, sur proposition du Ministre de la Justice et du ministre, et après avis de la Commission de la protection de la vie privée et de l'Institut, les données à conserver par type de service en application de l'alinéa 1er ainsi que les exigences auxquelles ces données doivent répondre.

Sauf disposition légale contraire, aucune donnée révélant le contenu des communications ne peut être conservée.

L'obligation de conserver les données visées à l'alinéa 1er s'applique également aux appels infructueux, pour autant que ces données soient, dans le cadre de la fourniture des services de communications concernés :

1° en ce qui concerne les données de la téléphonie, générées, traitées et stockées par les fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications électroniques, ou

2° en ce qui concerne les données de l'internet, journalisées par ces fournisseurs.

§ 2. Les données visées au paragraphe 1er, alinéa 1er, sont conservées en vue :

a) de la recherche, de l'instruction et de la poursuite d'infractions pénales visées aux articles 46bis et 88bis du Code d'instruction criminelle;

b) de la répression d'appels malveillants vers les services d'urgence, visée à l'article 107;

c) de la recherche par le Service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques, visée à l'article 43bis, § 3, 7°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques;

d) de l'accomplissement des missions de renseignement en ayant recours aux méthodes de collectes de données visées aux articles 18/7 et 18/8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Les fournisseurs de services et de réseaux visés au paragraphe 1er, alinéa 1er, font en sorte que les données reprises au paragraphe 1er, alinéa 1er, soient accessibles de manière illimitée à partir de la Belgique et à ce que ces données et toute autre information nécessaire concernant ces données puissent être transmises sans délai et sur simple demande aux autorités chargées des missions visées aux points a) à d) et uniquement à ces dernières.

§ 3. Les données visant à identifier les utilisateurs finals, le service de communications électroniques utilisé et l'équipement terminal qui est présumé avoir été utilisé sont conservées à partir de la souscription au service, aussi longtemps qu'une communication entrante ou sortante est possible à l'aide du service souscrit et pendant douze mois à compter de la date de la dernière communication entrante ou sortante enregistrée.

Les données de trafic et de localisation sont conservées douze mois à partir de la date de la communication.

Le Roi fixe, par arrêté délibéré en Conseil des Ministres, sur proposition du Ministre de la Justice et du ministre, et après avis de la Commission de la protection de la vie privée et de l'Institut, les données qui sont soumises à l'alinéa 1er et celles qui le sont à l'alinéa 2.

§ 4. A la suite du rapport d'évaluation visé au paragraphe 7, le Roi peut, par arrêté délibéré en Conseil des Ministres et après avis de l'Institut et de la Commission de la protection de la vie privée, adapter le délai de conservation des données pour certaines catégories de données, sans ce que ce délai ne puisse dépasser 18 mois.

Le Roi peut, dans les circonstances visées à l'article 4, § 1er, par arrêté délibéré en Conseil des Ministres, et après avis de l'Institut et de la Commission de la protection de la vie privée, et ce pour une période limitée, fixer un délai de conservation des données supérieur à douze mois.

Lorsque, dans les circonstances visées à l'alinéa 2, le Roi fixe un délai de conservation supérieur à vingt-quatre mois, le ministre notifie immédiatement à la Commission européenne et aux autres Etats membres de l'Union européenne toute mesure prise, accompagnée de sa motivation.

§ 5. Pour la conservation des données visées au paragraphe 1er, alinéa 1er, les fournisseurs de réseaux ou de services de communications électroniques visés au paragraphe 1er, alinéa 1er :

1° garantissent que les données conservées sont de la même qualité et sont soumises aux mêmes exigences de sécurité et de protection que les données sur le réseau;

2° veillent à ce que les données conservées fassent l'objet de mesures techniques et organisationnelles appropriées afin de les protéger contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle, ou le stockage, le traitement, l'accès ou la divulgation non autorisés ou illicites;

3° garantissent que l'accès aux données conservées n'est effectué que par un ou plusieurs membres de la Cellule de coordination de la Justice visée à l'article 2 de l'arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques et par les agents et préposés de ces fournisseurs spécifiquement autorisés par ladite Cellule;

4° veille à ce que les données conservées soient détruites lorsqu'est expiré le délai de conservation applicable à ces données.

Le Roi fixe, par arrêté délibéré en Conseil des Ministres, sur proposition du Ministre de la Justice et du ministre, et après avis de la Commission de la protection de la vie privée et de l'Institut, les mesures techniques et administratives que les fournisseurs de services et de réseaux visés au paragraphe 1er, alinéa 1er, doivent prendre en vue garantir la protection des données à caractère personnel conservées.

Les fournisseurs de services et réseaux visés au paragraphe 1er, alinéa 1er, sont considérés comme responsables du traitement de ces données au sens de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

§ 6. Le ministre et le Ministre de la Justice font en sorte que des statistiques sur la conservation des données qui sont générées ou traitées dans le cadre de la fourniture de services ou réseaux de communications accessibles au public soient transmises annuellement à la Commission européenne et à la Chambre des représentants. Ces statistiques comprennent notamment :

1° les cas dans lesquels des informations ont été transmises aux autorités compétentes conformément aux dispositions légales applicables;

2° le laps de temps écoulé entre la date à partir de laquelle les données ont été conservées et la date à laquelle les autorités compétentes ont demandé leur transmission;

3° les cas dans lesquels des demandes de données n'ont pu être satisfaites.

Ces statistiques ne peuvent comprendre des données à caractère personnel.

Les données qui concernent l'application du paragraphe 2, a), seront également jointes au rapport que le Ministre de la Justice doit faire au Parlement conformément à l'article 90decies du Code d'instruction criminelle.

Le Roi détermine, sur proposition du Ministre de la Justice et ministre et sur avis de l'Institut, les statistiques que les fournisseurs de services ou de réseaux transmettent annuellement à l'Institut et celles que l'Institut transmet au ministre et au Ministre de la Justice.

§ 7. Sans préjudice du rapport visé au paragraphe 6, alinéa 3, le ministre et le Ministre de la Justice font un rapport d'évaluation à la Chambre des représentants, deux ans après l'entrée en vigueur de l'arrêté royal visé au paragraphe 1er, alinéa 3, sur la mise en oeuvre de cet article, afin de vérifier si des dispositions doivent être adaptées, en particulier en ce qui concerne les données à conserver et la durée de la conservation. '.

Art. 6. Dans l'article 145 de la même loi, modifié par la loi du 25 avril 2007, il est inséré un paragraphe 3ter rédigé comme suit :

' § 3ter. Est puni d'une amende de 50 euros à 50 000 euros et d'une peine d'emprisonnement de six mois à trois ans ou d'une de ces peines seulement :

1° toute personne qui, à l'occasion de l'exercice de ses fonctions, hors les cas prévus par la loi ou sans respecter les formalités qu'elle prescrit, avec une intention frauduleuse ou à dessein de nuire, reprend de quelque manière que ce soit, détient, ou fait un usage quelconque des données visées à l'article 126;

2° celui qui, sachant que les données ont été obtenues par la commission de l'infraction visée au 1° les détient, les révèle à une autre personne, ou les divulgue ou fait un usage quelconque des données ainsi obtenues. '

CHAPITRE 3. - Modification de l'article 90decies du Code d'instruction criminelle

Art. 7. L'article 90decies du Code d'instruction criminelle, inséré par la loi du 30 juin 1994 et modifié par les lois du 8 avril 2002, 7 juillet 2002 et du 6 janvier 2003, est complété par un alinéa, rédigé comme suit :

' A ce rapport est joint le rapport dressé en application de l'article 126, § 6, alinéa 3, de la loi du 13 juin 2005 relative aux communications électroniques. ' ».

B.2.1. La partie requérante dans l'affaire n° 5856 prend un moyen unique de la violation, par l'article 5 de la loi attaquée, des articles 10 et 11 de la Constitution, lus seuls ou en combinaison avec les articles 6 et 8 de la Convention européenne des droits de l'homme ainsi qu'avec les articles 7, 8 et 47 de la Charte des droits fondamentaux de l'Union européenne.

B.2.2. Elle reproche à l'article 5 précité de traiter de manière identique les utilisateurs de services de télécommunications ou de communications électroniques soumis au secret professionnel, dont notamment les avocats, et les autres utilisateurs de ces services sans tenir compte du statut particulier de l'avocat, du caractère fondamental du secret professionnel auquel il est soumis et de la nécessaire relation de confiance qui doit l'unir à ses clients.

La disposition attaquée traiterait également à tort de manière identique les justiciables qui font l'objet de mesures d'enquête ou de poursuite pour des faits susceptibles de s'inscrire dans ces finalités et ceux qui ne font pas l'objet de telles mesures.

B.3.1. Le premier moyen dans l'affaire n° 5859 est pris de la violation, par l'article 5 de la loi attaquée, des articles 10, 11, 12, 15, 22 et 29 de la Constitution, lus isolément ou en combinaison avec les articles 5, 8, 9, 10, 11, 14, 15, 17 et 18 de la Convention européenne des droits de l'homme, avec les articles 7, 8, 11 et 52 de la Charte des droits fondamentaux de l'Union européenne et avec l'article 17 du Pacte international relatif aux droits civils et politiques, avec les principes généraux du droit de la sécurité juridique, de la proportionnalité et de « l'autodétermination informationnelle » ainsi qu'avec l'article 5.4 du Traité sur l'Union européenne (ci-après : TUE).

B.3.2. Dans une première branche du moyen, les parties requérantes renvoient aux conclusions de l'avocat général à la Cour de justice de l'Union européenne rendues le 12 avril 2013 dans les affaires jointes C-293/12 et C-594/12. Dans ces conclusions, l'avocat général a estimé que la directive « conservation des données » était incompatible, dans son ensemble, avec l'article 52.1 de la Charte des droits fondamentaux de l'Union européenne en ce que les limitations à l'exercice des droits fondamentaux qu'elle comporte, du fait de l'obligation de conservation des données qu'elle impose, ne s'accompagnent pas des principes indispensables appelés à régir les garanties nécessaires à l'encadrement de l'accès auxdites données et leur exploitation. L'avocat général était également d'avis que l'article 6 de la directive était incompatible avec les articles 7 et 52.1 de la Charte en ce qu'il imposait aux Etats membres de garantir que les données visées à son article 5 soient conservées pendant une durée pouvant atteindre deux ans. Les parties requérantes constatent encore que, selon ces conclusions, la directive est disproportionnée par rapport à la nécessité alléguée de réguler le marché interne et est par conséquent contraire à l'article 5.4 du TUE.

Les parties requérantes dans l'affaire n° 5859 en déduisent que dans la mesure où l'article 5 de la loi attaquée transpose la directive « conservation des données », elle viole aussi l'article 5.4 du TUE ainsi que les articles 7 et 52.1 de la Charte des droits fondamentaux de l'Union européenne.

B.3.3. Dans une deuxième branche du moyen, les parties requérantes dans l'affaire n° 5859 énoncent encore huit griefs à l'encontre de l'article 5 de la loi attaquée qui remplace l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques. Ainsi, la nature et l'ampleur des données conservées violeraient le droit au respect de la vie privée. Les parties requérantes reprochent également au législateur de ne pas avoir créé de règles distinctes pour la directive 2002/58/CE et pour la directive 2006/24/CE. Elles soutiennent encore que l'article 126, § 2, d), de la loi du 13 juin 2005 aboutirait à des situations où la sécurité juridique et l'interdiction d'arbitraire seraient compromises et où l'ingérence des autorités dans la vie privée ainsi que dans la liberté d'expression, la liberté de presse et le droit de se réunir et de s'associer serait disproportionnée. Le manque de précision de l'article 126, § 2, a), quant à la désignation d'une autorité compétente et de la même disposition en son point d) quant au pouvoir d'appréciation des services de renseignement est également dénoncé. Il est soutenu dans un point e) de la deuxième branche du moyen que la loi ne prévoit pas un contrôle juridictionnel suffisant contre les atteintes arbitraires des autorités. Dans un point f), les parties requérantes soutiennent que la notion d'infraction pénale utilisée par la loi attaquée ne répondrait pas au principe de légalité et serait en tout état de cause disproportionnée. Le point g) de la deuxième branche du même moyen dénonce l'absence de définition des données à conserver par type de service ainsi que l'absence d'exigences auxquelles ces données doivent répondre. Enfin, le délai de conservation des données prévu par la loi attaquée est critiqué dans un point h).

B.4. En ce qu'ils visent tous deux l'article 5 de la loi attaquée, le moyen unique dans l'affaire n° 5856 et le premier moyen dans l'affaire n° 5859 doivent être examinés conjointement.

B.5.1. Avant d'être remplacé par l'article 5 de la loi attaquée, l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques (ci-après : la loi du 13 juin 2005) disposait :

« § 1er. Par arrêté délibéré en Conseil des Ministres, le Roi fixe, sur proposition du Ministre de la Justice et du ministre et après avis de la Commission pour la protection de la vie privée et de l'Institut, les conditions dans lesquelles les opérateurs enregistrent et conservent les données de trafic et les données d'identification d'utilisateurs finals en vue de la poursuite et la répression d'infractions pénales, en vue de la répression d'appels malveillants vers les services d'urgence et en vue de la recherche par le service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques, ainsi qu'en vue de l'accomplissement des missions de renseignement prévues par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

§ 2. Les données à conserver ainsi que la durée de la conservation, qui en matière de service téléphonique accessible au public ne peut ni être inférieure à douze mois ni dépasser trente-six mois, sont déterminées par le Roi dans un arrêté délibéré en Conseil des ministres, après avis de la Commission pour la protection de la vie privée et de l'Institut.

Les opérateurs font en sorte que les données reprises au § 1er soient accessibles de manière illimitée de Belgique ».

B.5.2. Comme l'indique l'article 2 de la loi attaquée, celle-ci constitue la transposition partielle en droit belge de la directive « conservation des données » et de l'article 15.1 de la directive « vie privée et communications électroniques ».

L'exposé des motifs de la loi précise à cet égard :

« Cette directive 2006/24/CE a pour objectif d'harmoniser les dispositions des Etats membres relatives aux obligations des fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications électroniques en matière de conservation de certaines données qui sont générées ou traitées par ces fournisseurs, en vue de garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque Etat membre dans son droit interne.

La directive 2006/24/CE aurait dû être transposée en principe pour le 15 septembre 2007, à l'exception de ce qui concerne la conservation des données de communication concernant l'accès à Internet, la téléphonie par Internet et le courrier électronique par Internet, pour lesquels la date butoir de transposition était fixée au 15 mars 2009, la Belgique ayant utilisé la faculté prévue par la directive de demander un report.

Fin septembre 2012, la Commission européenne a mis la Belgique en demeure de transposer la directive et a attiré l'attention de la Belgique sur les sanctions pécuniaires que la Cour de justice pourrait lui infliger pour transposition incomplète de la directive. Il est donc exclu d'attendre encore plus longtemps et, à plus forte raison, d'attendre un amendement éventuel de la directive.

En vue de la transposition en droit belge de la directive 2006/24/CE, il est indispensable de revoir le libellé de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques qui, sur un certain nombre de points, contient des dispositions ne correspondant pas au prescrit européen.

La transposition de la directive 2006/24/CE sera complétée en partie par une modification de l'article 126 de la loi du 13 juin 2005 précitée, et en partie par l'adoption d'un arrêté royal d'exécution de ce nouvel article 126, de telle sorte que la liste des données à conserver et les exigences auxquelles ces données doivent répondre seront fixées par le Roi » (Doc. parl., Chambre, 2012-2013, DOC 53-2921/001, pp. 3-4).

B.6. Par un arrêt du 8 avril 2014, rendu en grande chambre en réponse aux questions préjudicielles de la Haute Cour d'Irlande et de la Cour constitutionnelle d'Autriche (CJUE, C-293/12, Digital Rights Ireland Ltd et C-594/12, Kärntner Landesregierung e.a.), la Cour de justice de l'Union européenne a invalidé la directive « conservation des données ».

B.7. Dans son mémoire, le Conseil des ministres constate qu'en raison de l'autorité de chose jugée attachée aux arrêts rendus par la Cour de justice de l'Union européenne, tout juge est désormais tenu de considérer la directive 2006/24/CE comme invalide. Il soutient toutefois que l'arrêt précité de la Cour de justice n'a d'incidence que sur les articles 2 et 3 de la loi attaquée dans lesquels il est annoncé que la loi transpose partiellement en droit belge la directive. Pour ce qui concerne l'article 5 de la loi attaquée, il y aurait, en revanche, lieu de considérer que celui-ci n'est pas affecté par l'arrêt de la Cour de justice et que les Etats membres sont compétents pour régler la matière de la conservation des données, en l'absence de mesures d'harmonisation en la matière.

B.8. Les entreprises tenues de conserver les données ainsi que la liste des données à conserver sont énumérées à l'article 126, § 1er, de la loi du 13 juin 2005, modifié par l'article 5 de la loi attaquée.

Les entreprises visées par l'obligation de conserver les données sont les fournisseurs au public de services de téléphonie fixe, de téléphonie mobile, d'accès à l'internet, de courrier électronique par internet et de téléphonie par internet, ainsi que les fournisseurs des réseaux publics de communications électroniques sous-jacents.

Il ressort des travaux préparatoires de la loi attaquée que le législateur a entendu adapter la terminologie employée afin de la rendre compatible avec la directive 2006/24/CE, les catégories de fournisseurs visées par la loi correspondant à celles énumérées par ladite directive (Doc. parl., Chambre, 2012-2013, DOC 53-2921/001, p. 12).

Quant aux données à conserver, elles ont elles aussi été regroupées en plusieurs catégories, tout comme la liste de données à conserver établie par la directive (ibid., p. 13). D'après l'article 126, § 1er, de la loi du 13 juin 2005, modifié par l'article 5 attaqué, il s'agit des données de trafic, des données de localisation, des données d'identification d'utilisateurs finals, des données d'identification du service de communications électroniques utilisé et des données d'identification de l'équipement terminal qui est présumé avoir été utilisé, qui sont générées ou traitées dans le cadre de la fourniture des services de communications concernés.

Les buts dans lesquels ces données sont conservées sont décrits au paragraphe 2 de l'article 126 modifié. Il s'agit de la recherche, de l'instruction et de la poursuite d'infractions pénales visées aux articles 46bis à 88bis du Code d'instruction criminelle ou de la répression d'appels malveillants vers les services d'urgence. Il s'agit également de permettre la recherche par le Service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques, ou encore de l'accomplissement des missions de renseignement en application des articles 18/7 et 18/8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Un délai minimum de douze mois pour la conservation des données est fixé à l'article 126, § 3, de la loi du 13 juin 2005 modifié, ce délai pouvant être porté à dix-huit mois en vertu du paragraphe 4 de la même disposition, voire à plus de vingt-quatre mois dans les circonstances visées à l'article 4, § 1er, lu en combinaison avec l'article 4, § 4, alinéas 2 et 3, de la loi du 13 juin 2005.

L'article 126, § 5, de la loi du 13 juin 2005, modifié par l'article 5 de la loi attaquée, charge les fournisseurs de réseaux ou de services de communications électroniques de garantir la qualité des données conservées ainsi que leur sécurité et leur protection. Les fournisseurs doivent également veiller aux mesures qui doivent être prises pour éviter leur destruction accidentelle ou illicite, leur perte, leur altération accidentelle ou un stockage, un traitement, un accès ou une divulgation qui ne serait pas autorisé ou serait illicite.

Les fournisseurs doivent encore garantir que l'accès aux données conservées n'est effectué que par un ou plusieurs membres de la Cellule de coordination de la Justice visée à l'article 2 de l'arrêté royal du 9 janvier 2003 « déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques » ainsi que par les agents et préposés de ces fournisseurs autorisés par ladite Cellule.

Enfin, la destruction des données conservées est également mise à la charge des fournisseurs.

B.9. Comme la Cour de justice de l'Union européenne l'a jugé par son arrêt précité du 8 avril 2014 (point 34), l'obligation imposée par les articles 3 et 6 de la directive 2006/24/CE aux fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communication de conserver pendant une certaine durée des données relatives à la vie privée d'une personne et à ses communications, telles que celles visées à l'article 5 de cette directive, constitue en soi une ingérence dans les droits garantis par l'article 7 de la Charte.

La Cour de justice a également jugé au point 35 de l'arrêt que « l'accès des autorités nationales compétentes aux données constitue une ingérence supplémentaire dans ce droit fondamental (voir, en ce qui concerne l'article 8 de la CEDH, arrêts Cour EDH, Leander c. Suède, 26 mars 1987, série A n° 116, § 48; Rotaru c. Roumanie [GC], n° 28341/95, § 46, CEDH 2000-V, ainsi que Weber et Saravia c. Allemagne (déc.), n° 54934/00, § 79, CEDH 2006-XI). Ainsi, les articles 4 et 8 de la directive 2006/24 prévoyant des règles relatives à l'accès des autorités nationales compétentes aux données sont également constitutifs d'une ingérence dans les droits garantis par l'article 7 de la Charte ».

Cette ingérence de la directive a été qualifiée de particulièrement grave (point 37), bien que la directive ne permette pas de prendre connaissance du contenu en tant que tel des communications électroniques conservées (point 39). Contrôlant la proportionnalité de l'ingérence constatée, la Cour de justice a conclu ce qui suit :

« 48. En l'espèce, compte tenu, d'une part, du rôle important que joue la protection des données à caractère personnel au regard du droit fondamental au respect de la vie privée et, d'autre part, de l'ampleur et de la gravité de l'ingérence dans ce droit que comporte la directive 2006/24, le pouvoir d'appréciation du législateur de l'Union s'avère réduit de sorte qu'il convient de procéder à un contrôle strict.

49. En ce qui concerne la question de savoir si la conservation des données est apte à réaliser l'objectif poursuivi par la directive 2006/24, il convient de constater que, eu égard à l'importance croissante des moyens de communication électronique, les données qui doivent être conservées en application de cette directive permettent aux autorités nationales compétentes en matière de poursuites pénales de disposer de possibilités supplémentaires d'élucidation des infractions graves et, à cet égard, elles constituent donc un instrument utile pour les enquêtes pénales. Ainsi, la conservation de telles données peut être considérée comme apte à réaliser l'objectif poursuivi par ladite directive.

50. Cette appréciation ne saurait être remise en cause par la circonstance, invoquée notamment par MM. Tschohl et Seitlinger ainsi que par le gouvernement portugais dans leurs observations écrites soumises à la Cour, qu'il existe plusieurs modalités de communications électroniques qui ne relèvent pas du champ d'application de la directive 2006/24 ou qui permettent une communication anonyme. Si, certes, cette circonstance est de nature à limiter l'aptitude de la mesure de conservation des données à atteindre l'objectif poursuivi, elle n'est toutefois pas de nature à rendre cette mesure inapte, ainsi que l'a relevé M. l'avocat général au point 137 de ses conclusions.

51. En ce qui concerne le caractère nécessaire de la conservation des données imposée par la directive 2006/24, il convient de constater que, certes, la lutte contre la criminalité grave, notamment contre la criminalité organisée et le terrorisme, est d'une importance primordiale pour garantir la sécurité publique et son efficacité peut dépendre dans une large mesure de l'utilisation des techniques modernes d'enquête. Toutefois, un tel objectif d'intérêt général, pour fondamental qu'il soit, ne saurait à lui seul justifier qu'une mesure de conservation telle que celle instaurée par la directive 2006/24 soit considérée comme nécessaire aux fins de ladite lutte.

52. S'agissant du droit au respect de la vie privée, la protection de ce droit fondamental exige, selon la jurisprudence constante de la Cour, en tout état de cause, que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire (arrêt IPI, C-473/12, EU: C: 2013: 715, point 39, et jurisprudence citée).

53. A cet égard, il convient de rappeler que la protection des données à caractère personnel, résultant de l'obligation explicite prévue à l'article 8, paragraphe 1, de la Charte, revêt une importance particulière pour le droit au respect de la vie privée consacré à l'article 7 de celle-ci.

54. Ainsi, la réglementation de l'Union en cause doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant un minimum d'exigences de sorte que les personnes dont les données ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données (voir, par analogie, en ce qui concerne l'article 8 de la CEDH, arrêts Cour EDH, Liberty et autres c. Royaume-Uni, n° 58243/00, § 62 et 63, du 1er juillet 2008; Rotaru c. Roumanie, précité, § 57 à 59, ainsi que S et Marper c. Royaume-Uni, précité, § 99).

55. La nécessité de disposer de telles garanties est d'autant plus importante lorsque, comme le prévoit la directive 2006/24, les données à caractère personnel sont soumises à un traitement automatique et qu'il existe un risque important d'accès illicite à ces données (voir, par analogie, en ce qui concerne l'article 8 de la CEDH, arrêts Cour EDH, S et Marper c. Royaume-Uni, précité, § 103, ainsi que M. K. c. France, n° 19522/09, § 35, du 18 avril 2013).

56. Quant à la question de savoir si l'ingérence que comporte la directive 2006/24 est limitée au strict nécessaire, il convient de relever que cette directive impose, conformément à son article 3 lu en combinaison avec son article 5, paragraphe 1, la conservation de toutes les données relatives au trafic concernant la téléphonie fixe, la téléphonie mobile, l'accès à l'internet, le courrier électronique par Internet ainsi que la téléphonie par l'internet. Ainsi, elle vise tous les moyens de communication électronique dont l'utilisation est très répandue et d'une importance croissante dans la vie quotidienne de chacun. En outre, conformément à son article 3, ladite directive couvre tous les abonnés et utilisateurs inscrits. Elle comporte donc une ingérence dans les droits fondamentaux de la quasi-totalité de la population européenne.

57. A cet égard, il importe de constater, en premier lieu, que la directive 2006/24 couvre de manière généralisée toute personne et tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif de lutte contre les infractions graves.

58. En effet, d'une part, la directive 2006/24 concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques, sans toutefois que les personnes dont les données sont conservées 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 graves. En outre, elle ne prévoit aucune exception, de sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel.

59. D'autre part, tout en visant à contribuer à la lutte contre la criminalité grave, ladite directive ne requiert aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique et, notamment, elle n'est pas limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique déterminée et/ou sur un cercle de personnes données susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la prévention, à la détection ou à la poursuite d'infractions graves.

60. En deuxième lieu, à cette absence générale de limites s'ajoute le fait que la directive 2006/24 ne prévoit aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure à des fins de prévention, de détection ou de poursuites pénales concernant des infractions pouvant, au regard de l'ampleur et de la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, être considérées comme suffisamment graves pour justifier une telle ingérence. Au contraire, la directive 2006/24 se borne à renvoyer, à son article 1er, paragraphe 1, de manière générale aux infractions graves telles qu'elles sont définies par chaque Etat membre dans son droit interne.

61. En outre, quant à l'accès des autorités nationales compétentes aux données et à leur utilisation ultérieure, la directive 2006/24 ne contient pas les conditions matérielles et procédurales y afférentes. L'article 4 de cette directive, qui régit l'accès de ces autorités aux données conservées, ne dispose pas expressément que cet accès et l'utilisation ultérieure des données en cause doivent être strictement restreints à des fins de prévention et de détection d'infractions graves précisément délimitées ou de poursuites pénales afférentes à celles-ci, mais il se borne à prévoir que chaque Etat membre arrête la procédure à suivre et les conditions à remplir pour avoir accès aux données conservées dans le respect des exigences de nécessité et de proportionnalité.

62. En particulier, la directive 2006/24 ne prévoit aucun critère objectif permettant de limiter le nombre de personnes disposant de l'autorisation d'accès et d'utilisation ultérieure des données conservées au strict nécessaire au regard de l'objectif poursuivi. Surtout, l'accès aux données conservées par les autorités nationales compétentes n'est pas subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante dont la décision vise à limiter l'accès aux données et leur utilisation à ce qui est strictement nécessaire aux fins d'atteindre l'objectif poursuivi et intervient à la suite d'une demande motivée de ces autorités présentée dans le cadre de procédures de prévention, de détection ou de poursuites pénales. Il n'a pas non plus été prévu une obligation précise des Etats membres visant à établir de telles limitations.

63. En troisième lieu, s'agissant de la durée de conservation des données, la directive 2006/24 impose, à son article 6, la conservation de celles-ci pendant une période d'au moins six mois sans que soit opérée une quelconque distinction entre les catégories de données prévues à l'article 5 de cette directive en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées.

64. Cette durée se situe, en outre, entre six mois au minimum et vingt-quatre mois au maximum, sans qu'il soit précisé que la détermination de la durée de conservation doit être fondée sur des critères objectifs afin de garantir que celle-ci est limitée au strict nécessaire.

65. Il résulte de ce qui précède que la directive 2006/24 ne prévoit pas de règles claires et précises régissant la portée de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte. Force est donc de constater que cette directive comporte une ingérence dans ces droits fondamentaux d'une vaste ampleur et d'une gravité particulière dans l'ordre juridique de l'Union sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire.

66. De surcroît, en ce qui concerne les règles visant la sécurité et la protection des données conservées par les fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications, il convient de constater que la directive 2006/24 ne prévoit pas des garanties suffisantes, telles que requises par l'article 8 de la Charte, permettant d'assurer une protection efficace des données conservées contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données. En effet, en premier lieu, l'article 7 de la directive 2006/24 ne prévoit pas de règles spécifiques et adaptées à la vaste quantité des données dont la conservation est imposée par cette directive, au caractère sensible de ces données ainsi qu'au risque d'accès illicite à celles-ci, règles qui seraient destinées notamment à régir de manière claire et stricte la protection et la sécurité des données en cause, afin de garantir leur pleine intégrité et confidentialité. En outre, il n'a pas non plus été prévu une obligation précise des Etats membres visant à établir de telles règles ».

B.10.1. Comme la Cour de justice l'a relevé aux points 56 et 57 de son arrêt, la directive impose la conservation de toutes les données relatives au trafic concernant la téléphonie fixe, la téléphonie mobile, l'accès à l'internet, le courrier électronique par internet ainsi que la téléphonie par l'internet, couvrant de manière généralisée toute personne et tous les moyens de communication électronique sans distinction en fonction de l'objectif de lutte contre les infractions graves que le législateur de l'Union entendait poursuivre.

La loi attaquée ne se distingue nullement de la directive sur ce point. En effet, ainsi qu'il est dit en B.8, les catégories de données qui doivent être conservées sont identiques à celles énumérées par la directive tandis qu'aucune distinction n'est opérée quant aux personnes concernées ou aux règles particulières à prévoir en fonction de l'objectif de lutte contre les infractions décrites à l'article 126, § 2, de la loi du 13 juin 2005 remplacé par la loi attaquée. Tout comme la Cour de justice l'a constaté à propos de la directive (point 58), la loi s'applique donc également 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 les infractions énumérées par la loi attaquée. De même, la loi s'applique sans aucune exception, également à des personnes dont les communications sont soumises au secret professionnel.

B.10.2. Pas plus que ce n'est le cas pour la directive, l'article 5 attaqué ne requiert-il une relation entre les données dont la conservation est prévue et une menace pour la sécurité publique. Il ne limite pas non plus la conservation des données afférentes à une période temporelle ou à une zone géographique déterminée ou encore à un cercle de personnes susceptibles d'être mêlées à une infraction visée par la loi, ou qui pourraient contribuer par la conservation des données, à prévenir, détecter ou poursuivre ces infractions.

B.10.3. Si les autorités compétentes pour avoir accès aux données conservées sont énumérées à l'article 126, § 5, 3°, de la loi du 13 juin 2005, remplacé par l'article 5 de la loi attaquée, aucune condition matérielle ou procédurale n'est définie par la loi quant à cet accès.

B.10.4. Enfin, en ce qui concerne la durée de conservation des données, la loi n'opère aucune distinction entre les catégories de données en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées.

B.11. Par identité de motifs avec ceux qui ont amené la Cour de justice de l'Union européenne à juger la directive « conservation des données » invalide, il y a lieu de constater que par l'adoption de l'article 5 de la loi attaquée, le législateur a excédé les limites qu'impose le respect du principe de proportionnalité au regard des articles 7, 8 et 52.1 de la Charte des droits fondamentaux de l'Union européenne.

Partant, l'article 5 précité viole les articles 10 et 11 de la Constitution lus en combinaison avec ces dispositions. Le moyen unique dans l'affaire n° 5856 et le premier moyen dans l'affaire n° 5859 sont fondés.

B.12. En raison de leur caractère indissociable avec l'article 5, il y a lieu d'annuler également les articles 1er à 4, 6 et 7 de la loi du 30 juillet 2013 attaquée et donc l'intégralité de ladite loi.

B.13. Compte tenu de ce qu'ils ne peuvent conduire à une annulation plus étendue, il n'y a pas lieu d'examiner les autres moyens dans l'affaire n° 5859.

Par ces motifs,

la Cour

annule la 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 90decies du Code d'instruction criminelle ».

Ainsi rendu en langue française, en langue néerlandaise et en langue allemande, conformément à l'article 65 de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, le 11 juin 2015.

Le greffier,

F. Meersschaut

Le président,

J. Spreutels