Numéros du rôle : 5856 et 5859
Arrêt n° 84/2015 du 11 juin 2015

A R R E T

En cause : les recours en annulation partielle (article 5) ou totale 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 90*decies* du Code d'instruction criminelle », introduits respectivement par l'Ordre des barreaux francophones et germanophone et par l'ASBL « Liga voor Mensenrechten » et l'ASBL « Ligue des Droits de l'Homme ».

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 90*decies* 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.

Le Conseil des ministres, assisté et représenté par Me E. Jacubowitz, Me P. Schaffner et Me A. Poppe, avocats au barreau de Bruxelles, a introduit des mémoires, les parties requérantes ont introduit des mémoires en réponse et le Conseil des ministres a également introduit des mémoires en réplique.

Par ordonnance du 3 février 2015, la Cour, après avoir entendu les juges-rapporteurs F. Daoût et T. Merckx-Van Goey, a décidé que les affaires étaient en état, qu'aucune audience ne serait tenue, à moins qu'une partie n'ait demandé, dans le délai de sept jours suivant la réception de la notification de cette ordonnance, à être entendue, et qu'en l'absence d'une telle demande, les débats seraient clos le 4 mars 2015 et les affaires mises en délibéré.

A la suite des demandes des parties requérantes à être entendues, introduites dans le délai précité, la Cour, par ordonnance du 3 mars 2015, a fixé l'audience au 18 mars 2015.

A l'audience publique du 18 mars 2015 :

- ont comparu :

. Me E. Lemmens, Me J.-F. Henrotte et Me A. Cassart, avocat au barreau de Liège, pour la partie requérante dans l'affaire n° 5856;

. Me R. Jespers, pour les parties requérantes dans l'affaire n° 5859;

. Me P. Schaffner et Me A. Poppe, pour le Conseil des ministres;

- les juges-rapporteurs F. Daoût et T. Merckx-Van Goey ont fait rapport;

- les avocats précités ont été entendus;

- les affaires ont été mises en délibéré.

Les dispositions de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle relatives à la procédure et à l'emploi des langues ont été appliquées.

II. *En droit*

- A -

Quant à l'intérêt des parties requérantes

A.1.1. L'Ordre des barreaux francophones et germanophone, partie requérante dans l'affaire n° 5856, se fonde sur l'article 495 du Code judiciaire et sur l'arrêt de la Cour n° 126/2005 du 13 juillet 2005 pour justifier son intérêt à demander l'annulation de la disposition attaquée au motif qu'elle est susceptible d'affecter directement et défavorablement la situation des avocats ainsi que celle des justiciables qu'ils défendent. La disposition attaquée porterait atteinte au secret professionnel de l'avocat dans la mesure où la consultation des métadonnées conservées permet de déterminer si un avocat a été consulté, d'identifier cet avocat, d'identifier ses clients ainsi que les dates et heures de leurs communications. La partie requérante se fonde sur l'arrêt n° 10/2008 du 23 janvier 2008 pour affirmer que le secret professionnel de l'avocat constitue un principe général qui participe du respect des droits fondamentaux.

A.1.2. L'ASBL « Liga voor Mensenrechten », première partie requérante dans l'affaire n° 5859, se fonde sur les articles 3 et 4 de ses statuts pour justifier son intérêt à demander l'annulation de la loi attaquée dans la mesure où celle-ci porterait atteinte aux droits fondamentaux, en particulier le droit au respect de la vie privée et des données à caractère personnel, le droit à la confidentialité des communications, le droit à la liberté personnelle et à la liberté d'expression, de réunion et d'association, la liberté de la presse, le droit de propriété, le principe du droit à un procès équitable et à ne pas être puni sans une disposition législative, le droit à un recours effectif, le principe de la légalité en matière pénale, le principe de sécurité juridique et le principe de proportionnalité ainsi que le principe de présomption d'innocence. L'objet social de l'ASBL requérante est de protéger les principes précités. Une abondante jurisprudence de la Cour irait dans ce sens.

A.1.3. L'ASBL « Ligue des Droits de l'Homme », deuxième partie requérante dans l'affaire n° 5859, aurait un intérêt à agir dans la mesure où son objet social est d'assurer la protection du droit à un procès équitable, du droit de la défense, de la liberté individuelle, du principe d'égalité et du principe de la légalité en matière pénale.

Quant au fond

Dans l'affaire n° 5856

A.2.1. La partie requérante dans l'affaire n° 5856 prend un moyen unique de la violation 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.

Il est reproché à la disposition attaquée 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 les finalités de la conservation des données électroniques litigieuses et ceux qui ne font pas l'objet de telles mesures.

A.2.2. La partie requérante cite des extraits des travaux préparatoires de la loi attaquée qui indiquent que le projet de loi avait pour objet de transposer 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 la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications et modifiant la directive 2002/58/CE - dite directive conservation des données – (ci-après : directive 2006/24/CE) 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) » (ci-après : directive 2002/58/CE).

Or, les obligations de conservation imposées aux fournisseurs de services de communications électroniques accessibles au public et de réseaux publics de communication seraient excessives par rapport aux objectifs de la loi. Aucune garantie ne serait prévue en ce qui concerne la collecte, la conservation ou l'accès aux données qui concernent des avocats alors que ces données sont confidentielles et couvertes par le secret professionnel.

La partie requérante relève que même si la disposition querellée précise que sauf disposition légale contraire, aucune donnée révélant le contenu des communications ne peut être conservée, la simple prise de connaissance de métadonnées qui pourraient concerner les avocats permettrait d'identifier la consultation d'un avocat mais également de tirer certaines conclusions en fonction des circonstances. Cette situation serait discriminatoire non seulement à l'égard des avocats mais également à l'égard des justiciables.

Il est souligné que la raison d'être du secret professionnel de l'avocat est d'intérêt général. Il s'agit de donner à ceux qui exercent cette profession les garanties nécessaires de crédibilité pour que tous ceux qui s'adressent à un avocat en confiance puissent avoir la certitude que les secrets confiés à leur conseil ne seront pas dévoilés à des tiers. Or, la loi attaquée porterait atteinte à cette garantie fondamentale alors qu'elle touche directement au droit à un procès équitable et au droit au respect de la vie privée. Rien ne permettrait de justifier que la disposition litigieuse traite de manière identique les utilisateurs des services de communications électroniques accessibles au public et de réseaux publics de communications titulaires du secret professionnel et les autres personnes qui utilisent les mêmes services.

A.2.3. La Cour européenne des droits de l'homme aurait elle-même confirmé que la mémorisation par une autorité publique de données relatives à la vie privée d'un individu constituait une ingérence dans le droit au respect de la vie privée garanti par l'article 8 de la Convention européenne des droits de l'homme. Or, pour que cette ingérence soit admissible, elle doit être nécessaire, ce qui implique l'existence d'un besoin social impérieux et, en particulier, la proportionnalité de l'ingérence au but légitime poursuivi. La partie requérante cite également l'arrêt de la Cour n° 127/2013 du 26 septembre 2013 dans lequel celle-ci a rappelé l'importance du secret professionnel de l'avocat.

A.2.4. En l'espèce, il est reproché à la disposition attaquée de permettre la conservation de données couvertes par le secret professionnel de l'avocat ainsi qu'un libre accès aux métadonnées ainsi conservées durant une période extrêmement longue sans qu'un mécanisme de contrôle ou de recours ne soit par ailleurs prévu. Des poursuites pénales pourraient parfaitement être diligentées par les autorités compétentes sur la base de données confidentielles ainsi consultées. L'absence de contrôle juridictionnel aux divers stades de la procédure ne serait pas conforme à l'article 6 de la Convention européenne des droits de l'homme et à l'article 47 de la Charte des droits fondamentaux de l'Union européenne.

A.2.5. En ce qui concerne la discrimination dénoncée à l'égard de certains justiciables, la partie requérante soutient qu'il existerait un risque non négligeable que les bases de données litigieuses soient gérées avec légèreté par les opérateurs réticents face au coût représenté par la nouvelle obligation légale. La disposition attaquée ne prévoit aucune garantie en la matière en ce qui concerne les données confidentielles couvertes par le secret

professionnel de l'avocat et se contente de charger le Roi de fixer les mesures techniques et administratives que les opérateurs devront prendre en vue de garantir la protection des données à caractère personnel qui ont été conservées.

A.2.6. La partie requérante précise encore que d'un point de vue technique, il serait simple de faire le tri entre les métadonnées ordinaires et celles qui sont liées à un titulaire du secret professionnel via un mécanisme de filtre à l'entrée. Le législateur pourrait donc contraindre facilement « les opérateurs de communications à prendre note de la qualité de titulaire du secret professionnel de leurs clients et à partager cette information entre eux ». Les opérateurs pourraient ainsi ne pas verser les métadonnées générées par les communications entrantes et sortantes des avocats et des autres titulaires du secret professionnel dans les bases de données constituées en exécution de la disposition attaquée.

A.2.7. La partie requérante précise qu'au moment où elle a introduit son recours, la Cour de justice de l'Union européenne était saisie d'une demande de décision préjudicielle formée par la Cour constitutionnelle d'Autriche relative à la compatibilité de la directive 2006/24/CE transposée par la loi attaquée avec les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne respectivement relatifs au respect de la vie privée et à la protection des données à caractère personnel. Elle reproduit ensuite de larges extraits des conclusions présentées le 12 décembre 2013 par l'avocat général Pedro Cruz Villalon. La partie requérante estime à plusieurs égards que les critiques formulées par l'avocat général pourraient être transposées en ce qui concerne la disposition attaquée.

A.2.8. A titre subsidiaire, si la Cour ne devait pas adhérer à l'argumentation que la partie requérante a développée, elle ajoute que la durée de conservation des données prévues par la loi attaquée serait excessive par rapport à l'objectif répressif poursuivi. Il en serait d'autant plus ainsi que la conservation de ces données pourrait théoriquement être infinie compte tenu du pouvoir excessif conféré au Roi en la matière.

A.2.9. La partie requérante se fonde encore sur un arrêt de la Cour constitutionnelle fédérale allemande du 2 mars 2010 qui, saisie d'un recours en annulation relatif à la loi par laquelle l'Allemagne a transposé la directive 2006/24/CE, a confirmé que la conservation des données créait un sentiment diffus et continu de surveillance qui peut entraver le libre exercice des droits fondamentaux.

A.2.10. La partie requérante souligne encore que la disposition attaquée, tout comme la directive, prévoit que les données ne sont pas conservées par les autorités publiques elles-mêmes mais par les fournisseurs de services de communications électroniques sur lesquels pèse l'essentiel des obligations garantissant leur protection et leur sécurité. Ce constat serait de nature à démontrer l'absence de proportionnalité de la double discrimination évoquée par la partie requérante par rapport au but poursuivi par le législateur.

A.2.11. A titre subsidiaire, la partie requérante demande qu'une question préjudicielle soit posée à la Cour de justice de l'Union européenne relative à la compatibilité de la directive 2006/24/CE avec les articles 6 et 8 de la Convention européenne des droits de l'homme ainsi qu'avec les articles 7, 8, 47 et 52 de la Charte des droits fondamentaux de l'Union européenne.

A.3.1. En ce qui concerne la première branche du moyen dans l'affaire n° 5856, le Conseil des ministres soutient dans son mémoire que la distinction opérée par la partie requérante n'est pas pertinente en l'espèce. Il note, en effet, que la conservation des données critiquée ne porte pas sur le contenu des communications mais uniquement sur les métadonnées, de sorte que le contenu des communications n'est pas concerné et reste couvert par le secret professionnel. Il ne pourrait être raisonnablement soutenu que le contenu d'une communication peut être déduit du seul fait de l'existence de celle-ci. D'autres moyens pourraient permettre de savoir qu'une personne a consulté un avocat, telle la demande d'assistance lors d'une audition, sans que cette information soit considérée comme portant atteinte de manière disproportionnée au droit au respect de la vie privée ou au droit à un procès équitable. Le Conseil des ministres ajoute que les données en question étaient déjà conservées par des fournisseurs de services de télécommunication pour la facturation ainsi que pour la consultation et la communication des données dans le cadre des instructions mentionnées dans l'article 126, § 2, de la loi du 13 juin 2005 relative aux communications électroniques.

A.3.2. Quant aux circonstances dans lesquelles le secret professionnel peut être levé, le Conseil des ministres souligne que ce ne peut être le cas que lorsqu'il existe des présomptions que le praticien concerné a lui-même commis une infraction. Le Conseil des ministres renvoie à l'article 90*octies* du Code d'instruction criminelle.

A.3.3. Quant à la distinction préconisée par la partie requérante, le Conseil des ministres soutient qu'elle est difficile voire impossible à réaliser dès lors que les fournisseurs chargés de conserver les métadonnées ne savent pas nécessairement si les personnes concernées par ces données sont ou non tenues par le secret professionnel. Le Conseil des ministres ajoute que la grande majorité des citoyens utilisent actuellement des adresses IP dynamiques, plusieurs adresses étant utilisées par différentes personnes pour éviter une surcharge du système. Toutes les communications devraient donc être filtrées et examinées pour éviter la conservation de données qui concernent des personnes soumises à un secret professionnel.

Le Conseil des ministres souligne encore que toutes les communications réalisées par le titulaire d'un secret professionnel ne sont pas couvertes par ce secret. Il n'y aurait donc pas lieu d'exclure cette catégorie de personnes du champ d'application de la loi.

A.3.4. En ce qui concerne la deuxième branche du moyen unique, le Conseil des ministres soutient qu'ici encore, la différence de traitement proposée par la partie requérante n'est pas pertinente et est impossible à mettre en œuvre dès lors que les fournisseurs de services concernés n'ont aucun moyen de savoir si les personnes dont les métadonnées sont conservées font ou non l'objet de mesures d'enquête ou de poursuite.

A.4.1. Dans son mémoire en réponse, la partie requérante dans l'affaire n° 5856 s'étonne de constater que l'Etat belge ne tient pas compte de l'arrêt C-293/12 prononcé le 8 avril 2014 par la Cour de justice de l'Union européenne, lequel a invalidé la directive 2006/24/CE dont la disposition querellée assure la transposition. Après avoir reproduit de larges extraits dudit arrêt, la partie requérante soutient que, par identité de motifs, la disposition attaquée qui assure la transposition de la directive violerait elle aussi les dispositions reprises au moyen. Il en irait d'autant plus ainsi que le fait que la conservation des données critiquée ne concerne pas le contenu des communications ne permet pas de garantir la confidentialité des données couvertes par le secret professionnel, contrairement à ce que soutient l'Etat belge.

A.4.2. La partie requérante aurait démontré dans son recours que les données conservées étaient elles-mêmes confidentielles et couvertes par le secret professionnel. La Cour de justice l'aurait confirmé de manière implicite mais certaine au point 58 de son arrêt.

A.4.3. Quant à l'affirmation du Conseil des ministres selon laquelle un avocat, fût-il pénaliste, peut être consulté sur des questions tellement variées qu'on ne saurait valablement en tirer des conclusions quant au contenu d'une communication par le seul fait de son existence, la partie requérante dans l'affaire n° 5856 soutient que cette affirmation est visiblement avancée pour les besoins de la cause. En effet, les données conservées permettent de dresser une véritable carte digitale précise de chaque personne, ce qui serait confirmé par l'arrêt de la Cour de justice de l'Union européenne.

L'Etat belge ne pourrait par ailleurs être suivi quand il compare la situation d'une personne qui choisit d'avoir recours à un avocat dans le cadre d'une audition et celle qui consulte un avocat pour obtenir un avis et voit les données confidentielles liées à cette consultation faire l'objet d'une conservation en raison des dispositions litigieuses. Dans le premier cas, en effet, la personne concernée consulte un avocat pour obtenir son assistance de manière publique lors d'une future audition, cette mention apparaissant le cas échéant dans le procès-verbal dressé à son terme, tandis que dans le second cas, la personne concernée reste libre de ne pas souhaiter que le fait qu'elle ait consulté un avocat soit divulgué.

A.4.4. Quant à l'article 90*octies* du Code d'instruction criminelle auquel se réfère le Conseil des ministres, il ne concerne que l'hypothèse de la mise en œuvre d'une des méthodes particulières de recherche prévues par le Code au sein d'un cabinet d'avocats ou chez un médecin. La référence à cet article ne répondrait dès lors pas aux critiques formulées par la partie requérante.

A.4.5. Quant à l'impossibilité invoquée de mettre en œuvre une distinction selon que les données émanent de titulaires du secret professionnel ou d'autres personnes, ces difficultés ne justifieraient pas qu'une annulation pure et simple de la disposition critiquée ne puisse être prononcée afin de mettre fin à une situation discriminatoire.

Le même constat pourrait être posé en ce qui concerne la seconde branche du moyen unique. Les prétendues difficultés techniques mises en avant par le Conseil des ministres ne pourraient en effet justifier le maintien d'une discrimination en violation des dispositions visées au moyen. La Cour de justice de l'Union européenne partagerait cette analyse dans l'arrêt qu'elle a récemment rendu.

A.4.6. La partie requérante dans l'affaire n° 5856 rappelle enfin qu'elle a sollicité à titre subsidiaire qu'une question préjudicielle soit adressée à la Cour de justice de l'Union européenne à propos de la compatibilité de la directive 2006/24/CE avec les articles 6 et 8 de la Convention européenne des droits de l'homme et avec les articles 7, 8, 47 et 52 de la Charte des droits fondamentaux de l'Union européenne.

A.5.1. Dans son mémoire en réplique, le Conseil des ministres indique que suite à l'arrêt du 8 avril 2014 rendu par la Cour de justice de l'Union européenne dans l'affaire C-293/12, tout juge est tenu de considérer la directive 2006/24/CE comme invalide dès lors que l'arrêt a autorité de chose jugée *erga omnes* avec effet rétroactif. Dès lors, en l'absence de mesures d'harmonisation en matière de rétention des données, les Etats membres sont eux-mêmes compétents pour régler cette problématique. L'invalidation de la directive par l'arrêt de la Cour aurait pour effet que la compatibilité de la loi attaquée avec cette directive ne doit plus être vérifiée. Les articles 2 et 3 de la loi attaquée, dans lesquels il est annoncé que la loi transpose partiellement en droit belge la directive, perdraient donc leur validité. Or, le recours introduit par l'Ordre des barreaux francophones et germanophone ne vise pas à obtenir l'annulation de ces dispositions, qui peuvent être séparées du reste de la loi attaquée, en sorte que leur irrégularité n'affecterait pas l'article 5 de la loi attaquée.

A.5.2. Le Conseil des ministres souligne encore que l'arrêt de la Cour de justice de l'Union européenne porte sur la protection de la vie privée et le respect de la liberté d'expression et non sur le respect de l'article 6 de la Convention européenne des droits de l'homme. L'intérêt de cet arrêt serait donc limité au regard du moyen unique soulevé par l'Ordre des barreaux francophones et germanophone.

A.5.3. D'après le Conseil des ministres, c'est le caractère proportionné de la directive qui n'a pas trouvé grâce aux yeux de la Cour de justice de l'Union européenne. Celle-ci n'a pas pour autant dit pour droit que la conservation de métadonnées impliquait en soi une violation du secret professionnel ni que la conservation de telles données relatives à des personnes qui ne font pas l'objet de poursuites pénales serait impossible.

A.5.4. Le Conseil des ministres ajoute que si une législation complémentaire devait s'imposer en ce qui concerne les communications couvertes par le secret professionnel, celle-ci devrait être intégrée dans le Code d'instruction criminelle et non dans la loi attaquée.

A.5.5. Le Conseil des ministres note encore qu'il existe de nombreuses différences entre la directive invalidée et la loi attaquée, en sorte que les considérants de l'arrêt de la Cour de justice de l'Union européenne du 8 avril 2014 ne sont pas transposables au présent recours.

Ainsi le Conseil des ministres souligne-t-il que la loi attaquée prévoit explicitement qu'elle s'applique 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.

Contrairement à ce que la Cour de justice a jugé dans son arrêt au considérant 37, l'exposé des motifs de la loi attaquée précise que la personne concernée conserve ses droits et devra être informée par les fournisseurs de la conservation de ses données pendant une période maximale de douze mois. Elle pourra également accéder à ces données et, le cas échéant, les faire rectifier, le tout sans préjudice d'une plainte devant la Commission de la protection de la vie privée ou d'une requête devant le président du tribunal de première instance.

Contrairement à ce que la Cour de justice a également énoncé aux considérants 60 à 62 de son arrêt, la loi attaquée limite le droit de consulter les métadonnées conservées ainsi que les personnes habilitées à les consulter. La loi attaquée limite également la durée de conservation des métadonnées à douze mois.

Il est encore souligné que la loi attaquée et son arrêté d'exécution prévoient un certain nombre de garanties contrairement à ce qu'a dénoncé la Cour de justice de l'Union européenne dans le considérant 66 de son arrêt, à propos de la directive.

Le Conseil des ministres en conclut que l'arrêt de la Cour de justice de l'Union européenne, au regard du recours introduit à la Cour, serait nettement plus limité que ce que la partie requérante laisse entendre.

A.5.6. Pour ce qui est de l'examen du moyen unique, le Conseil des ministres renvoie à son premier mémoire et ajoute, en ce qui concerne la première branche du moyen, que l'arrêt de la Cour de justice n'examine pas la directive sous l'angle de l'article 6 de la Convention européenne des droits de l'homme. Il ne pourrait être déduit du considérant 58 de l'arrêt que la conservation de métadonnées implique une violation du secret professionnel.

Le Conseil des ministres ajoute encore que si une réglementation doit être prévue, elle doit être intégrée dans le Code d'instruction criminelle.

Quant à la conservation des métadonnées, il faudrait également observer qu'elle ne résulte pas uniquement de la loi attaquée. Ainsi les données concernées seraient-elles actuellement conservées à des fins de facturation, et l'obligation de conservation des données de trafic et des données d'identification d'utilisateur final en vue de la poursuite et de la répression d'infractions pénales, de l'utilisation malveillante d'un réseau ou d'un service de communication électronique ou d'appel malveillant et l'information des services de renseignement et de sécurité existeraient déjà.

Quant à la distinction que les parties requérantes voudraient voir appliquer dans la loi entre les titulaires d'un secret professionnel et les autres utilisateurs, le Conseil des ministres indique qu'il n'y a pas que les avocats qui sont tenus par le secret professionnel. Or, la liste des personnes tenues par un tel secret serait difficile à dresser tant elle est longue.

Le Conseil des ministres ajoute également par rapport à son mémoire qu'au regard de l'article 6 de la Convention européenne des droits de l'homme, il ne faut pas perdre de vue que toute utilisation des métadonnées récoltées en application de la loi attaquée fera tôt ou tard l'objet d'un contrôle par un magistrat neutre, indépendant et impartial.

A.5.7. Quant à la deuxième branche du moyen unique, la différence de traitement dont l'absence est jugée inconstitutionnelle par la partie requérante serait impossible à mettre en œuvre. Le Conseil des ministres constate que la partie requérante ne semble pas insister sur ce point.

A.5.8. Sur les deux branches réunies du moyen unique, le Conseil des ministres commence par indiquer, en ce qui concerne la durée de la conservation des données, que la loi attaquée n'exploite pas la même durée de vingt-quatre mois qui est autorisée par la directive européenne puisque cette durée est fixée dans la loi à douze mois. Le Conseil des ministres indique également que « si la conservation des métadonnées permet dans de nombreux cas d'identifier l'auteur d'une infraction, cela signifie par la même occasion qu'elle permet d'innocenter toutes les autres personnes qui sont concernées par l'enquête ».

Dans l'affaire n° 5859

A.6. Avant d'exposer les moyens de leur requête, les parties requérantes dans l'affaire n° 5859 font un résumé de la directive 2006/24/CE et exposent son incidence sur l'article 8 de la Convention européenne des droits de l'homme. Elles donnent ensuite un aperçu de la procédure pendante devant la Cour de justice de l'Union européenne ainsi que de certains éléments de droit comparé.

Les parties requérantes font valoir que de nombreuses lois mettant en œuvre la directive ont donné lieu à des annulations prononcées par les cours constitutionnelles de divers pays, ce qui serait de nature à démontrer que la directive elle-même est problématique. Elles soulignent également que lors de l'introduction de la requête, la Commission européenne avait émis de nombreuses critiques à l'encontre de ladite directive. Quant à la loi attaquée, il est relevé que le projet de loi n'a pas été soumis à l'avis de la Commission de la protection de la vie privée et que la section de législation du Conseil d'Etat a émis de nombreuses critiques à l'égard de cette loi.

A.7. Les parties requérantes prennent un premier moyen de la violation 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 de l'Union européenne.

A.8.1. La première branche du moyen est dirigée contre l'article 5 de la loi attaquée. D'après les parties requérantes, ledit article 5 serait contraire aux articles 10, 11 et 22 de la Constitution, à l'article 8 de la Convention européenne des droits de l'homme, aux articles 7, 8, 11 et 52 de la Charte des droits fondamentaux de l'Union européenne et à l'article 5, § 4, du Traité de l'Union européenne. Les parties requérantes indiquent que cette branche du moyen renvoie à l'avis de l'avocat général de la Cour de justice de l'Union européenne rendu le 12 avril 2013 dans les affaires jointes C-293/12 et C-594/12. De larges extraits de cet avis sont reproduits dans la requête, desquels il est déduit que l'article 5 de la loi du 30 juillet 2013 prévoit des délais qui violent tant le principe de légalité que le principe de proportionnalité et doit en conséquence être annulé.

A.8.2. Dans son mémoire, le Conseil des ministres affirme que l'invalidité de la directive 2006/24/CE n'implique pas que la loi attaquée ne soit pas valable.

Selon le Conseil des ministres, l'article 5 de la loi du 30 juillet 2013 définit de manière suffisamment claire pour quels faits punissables l'obligation de conservation a été instaurée.

En réponse aux griefs des parties requérantes quant au délai de conservation des données de douze mois, le Conseil des ministres fait valoir que ce délai poursuit un but pertinent, à savoir l'équilibre entre l'optimisation de l'instruction en matière répressive et la charge de travail pour les fournisseurs de services et réseaux de télécommunications. Le Conseil des ministres estime que ce délai n'a pas de conséquences manifestement disproportionnées.

A.8.3. Les parties requérantes répondent que l'article 5 de la loi du 30 juillet 2013 ne satisfait pas à la notion d'« infractions graves » de la directive 2006/24/CE. Selon elles, la référence aux articles 46*bis* et 88*bis* du Code d'instruction criminelle ne suffit pas.

En ce qui concerne la durée de conservation des données, elles relèvent que la Cour de justice a, par son arrêt précité du 8 avril 2014 (points 63-64), critiqué le fait que, d'une part, entre les catégories de données, il n'est établi aucune distinction en rapport avec son utilité pour réaliser le but poursuivi ou selon les personnes concernées et que, d'autre part, le délai de conservation varie d'au moins six mois à au plus vingt-quatre mois, sans qu'il soit précisé que ce délai doit être fixé sur la base de critères objectifs. La loi attaquée utilise un seul délai pour quatre buts différents (article 126, a), b), c) et d), de la loi du 13 juin 2005 relative aux communications électroniques).

A.8.4. Dans son mémoire en réplique, le Conseil des ministres relève que la critique des parties requérantes porte sur l'accès aux données et non sur leur conservation.

Les articles 46*bis* et 88*bis* du Code d'instruction criminelle contiennent, selon le Conseil des ministres, suffisamment de garanties relatives à la vie privée. Dans un arrêt du 11 octobre 2000, la Cour de cassation a jugé que cette dernière disposition satisfait aux exigences émises par l'article 8 de la Convention européenne des droits de l'homme. Quoi qu'il en soit, dans le cadre de l'examen du fond, le juge dira si la preuve a été obtenue régulièrement.

Selon le Conseil des ministres, il n'est pas possible d'établir une distinction, en ce qui concerne la durée de la conservation des données, en fonction des objectifs de la conservation. Il est impossible de savoir à l'avance quelle personne commettra une infraction visée dans une des quatre catégories de faits énumérées dans la loi. Le Conseil des ministres énumère plusieurs éléments dont il apparaît selon lui qu'un délai de douze mois repose effectivement sur des critères objectifs.

A.9.1. Dans une deuxième branche du premier moyen, les parties requérantes dans l'affaire n° 5859 soutiennent que l'article 5 de la loi du 30 juillet 2013 viole les articles de la Constitution visés au moyen, lus ou non en combinaison avec les autres dispositions mentionnées et en particulier les articles 10, 11, 19, 22 et 25 de la Constitution, l'article 8 de la Convention européenne des droits de l'homme ainsi que les articles 7, 8 et 52.1 de la Charte des droits fondamentaux de l'Union européenne.

A.9.2.1.1. Dans un point a), les parties requérantes soutiennent que la nature et l'ampleur des données conservées violent le droit au respect de la vie privée. Il ne serait pas démontré qu'une telle ingérence dans la vie privée répondrait à un besoin social contraignant et respecterait les principes de nécessité et de proportionnalité.

Se fondant sur la jurisprudence de la Cour de justice de l'Union européenne et de la Cour européenne des droits de l'homme, les parties requérantes soutiennent qu'en l'espèce, il s'agit de la conservation de données de communications souvent sensibles de personnes qui ne sont même pas inculpées et ce, sans la moindre distinction entre ces personnes. En imposant une obligation de rétention de données « en blanc », la transposition de la directive 2006/24/CE opérée par l'article 5 de la loi attaquée irait bien au-delà du but originel de la directive et ne répondrait dès lors pas au contrôle de nécessité.

D'après les parties requérantes, la législation attaquée signifierait une modification fondamentale dans les rapports entre l'autorité et le citoyen en ce que toute communication téléphonique et par internet de tous les citoyens serait contrôlée. Cette situation serait contraire à la conception générale partagée dans les démocraties occidentales selon laquelle la vie privée est considérée comme un droit de défense du citoyen à l'encontre de l'intrusion injustifiée dans sa vie privée par l'autorité. Les parties requérantes renvoient à l'arrêt de la Cour constitutionnelle allemande du 2 mars 2010 ainsi qu'aux arrêts de la Cour suprême de Chypre, de la Cour administrative bulgare, de la Cour constitutionnelle de Roumanie et de la Cour constitutionnelle de la République tchèque qui ont conclu à une annulation pour inconstitutionnalité en raison de la violation du droit au respect de la vie privée, du droit à l'autodétermination informationnelle, du secret des lettres, de la liberté d'expression, et de la sécurité et de l'intégrité des communications téléphoniques et postales.

D'après les parties requérantes, la conservation des données prévue par la loi viole le principe de légalité en dehors des cas d'urgence. Il n'existerait aucun besoin social impérieux qui puisse justifier une telle conservation intégrale de toutes les données de tous les citoyens sans distinction. Tandis que l'objectif de la nouvelle législation serait de lutter contre la criminalité, la loi et l'exposé des motifs ne préciseraient pas en des termes suffisamment précis, clairs et univoques, en quelles hypothèses l'ingérence dans la vie privée serait prévue.

A.9.2.1.2. En ce qui concerne le point a) de la deuxième branche du premier moyen, le Conseil des ministres répond que la Cour constitutionnelle procède, tout comme la Cour de justice, à un contrôle de proportionnalité. La jurisprudence de la Cour européenne des droits de l'homme citée portait sur la conservation de données pour une durée indéterminée, alors qu'il s'agit en l'espèce d'un délai de douze mois.

Le Conseil des ministres conteste ensuite que la loi attaquée ait un but policier. Le législateur a pu régler l'accès aux données dans le cadre des compétences des services de renseignement, dès lors que cette matière n'est pas harmonisée au niveau européen. Ensuite, dans son arrêt du 8 avril 2014 (point 41), la Cour de justice a aussi jugé que le but poursuivi par la directive 2006/24/CE est légitime. Si les données n'étaient pas conservées, les services judiciaires devraient plus souvent recourir à des mesures d'instruction plus invasives.

A.9.2.1.3. Les parties requérantes répliquent que l'arrêt de la Cour européenne des droits de l'homme du 4 décembre 2008 qu'elles citent est pertinent parce que, dans cet arrêt, la conservation de profils ADN d'inculpés a été considérée comme une limitation disproportionnée du droit à la vie privée. L'article 5 attaqué de la loi du 30 juillet 2013 va encore plus loin parce que l'on conserve des données de chacun et pas seulement d'inculpés. Selon elles, le fait qu'il s'agissait, dans l'affaire soumise à la Cour européenne, d'un délai de conservation indéterminé et qu'il s'agit en l'espèce d'un délai de douze mois n'est pas crucial dans le cadre de cette affaire.

Les parties requérantes relèvent que le législateur n'était pas tenu de prévoir la conservation de données pour les services de renseignement aussi.

En ce qui concerne l'arrêt de la Cour de justice du 8 avril 2014 cité par le Conseil des ministres, les parties requérantes répondent qu'il y est uniquement dit que l'article 8 de la Convention européenne des droits de l'homme admet une ingérence en vue de la protection de l'ordre public et de la prévention de faits punissables.

A.9.2.1.4. S'agissant de la circonstance que l'arrêt de la Cour européenne des droits de l'homme du 4 décembre 2008 concernait uniquement des inculpés, le Conseil des ministres répond que les autorités publiques ne savent pas au préalable quelles personnes pourraient commettre des infractions à l'avenir.

Le Conseil des ministres observe qu'avant l'adoption de la disposition attaquée, il existait aussi des règles auxquelles les services de renseignement et de sécurité devaient se conformer pour consulter des données, ce qui implique que ces données étaient également conservées.

Le Conseil des ministres persiste à affirmer que la loi attaquée n'est pas contraire à l'arrêt de la Cour de justice du 8 avril 2014. Par ailleurs, ni la Cour de justice ni les parties requérantes n'ont indiqué comment il faudrait régler la conservation de données selon des modalités qui tiennent compte notamment de la nature de l'infraction. Il est d'ailleurs impossible de le faire, puisque personne ne peut prédire qui commettra quelle infraction.

A.9.2.2.1. Dans un point b), les parties requérantes dénoncent le fait qu'il n'est pas créé de réglementation distincte pour la directive 2002/58/CE et pour la directive 2006/24/CE. L'article 2 de la loi attaquée prévoit en effet que cette loi constitue la transposition des deux directives alors qu'elles poursuivent des objectifs différents. Cette différence a d'ailleurs été soulignée par la section de législation du Conseil d'Etat dans son avis du 27 mai 2013. Celui-ci a notamment souligné que l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques proposé allait beaucoup plus loin que les objectifs visés dans la directive 2006/24/CE. Le texte n'a toutefois pas été modifié malgré l'avis du Conseil d'Etat.

A.9.2.2.2. En ce qui concerne la critique des parties requérantes au point b), le Conseil des ministres estime que les parties requérantes semblent critiquer la manière dont la loi a été élaborée, alors que la Cour constitutionnelle n'est pas compétente pour se prononcer à ce sujet.

Le législateur pouvait effectivement adopter une loi qui transpose deux directives. La loi précise aussi suffisamment clairement quelles personnes ont accès aux données.

A.9.2.2.3. Les parties requérantes répondent qu'elles critiquent le contenu même de la loi et non pas son élaboration. Le Conseil d'Etat avait observé à juste titre que les deux directives qui ont été transposées ont un tout autre contenu, que la loi attaquée a mélangé.

La directive 2002/58/CE admet dans certains cas et à certaines conditions une limitation de la vie privée en raison, notamment, de la sécurité de l'Etat, tandis que la directive 2006/24/CE instaure une obligation générale de conserver des données dans le cadre de la lutte contre les « infractions graves ». Il s'agit, selon les parties requérantes, d'une différence fondamentale que le Conseil d'Etat a relevée, mais que le Conseil des ministres réduit à une question de procédure.

Les parties requérantes constatent que le parallélisme entre les deux régimes est évident aux yeux du Conseil des ministres, alors que notamment le Conseil d'Etat l'a précisément critiqué. La nécessité alléguée d'un rattachement entre les bases de données illustre le fait que la confusion des restrictions est générée sur les quatre terrains.

A.9.2.2.4. Le Conseil des ministres soutient que le législateur n'a pas utilisé la directive 2006/24/CE pour justifier la conservation de données sur instruction des services de renseignement. Le législateur n'est évidemment pas tenu d'instaurer une obligation générale de conservation pour, notamment, les missions des services de renseignement. Le législateur a simplement fait usage de sa liberté politique pour créer un cadre légal pour l'obligation de conservation des opérateurs, obligation qui existait déjà.

A.9.2.3.1. Dans un point c), les parties requérantes allèguent la violation des principes de légalité et de proportionnalité par l'article 126, § 2, d), de la loi du 13 juin 2005 relative aux communications électroniques. Tel qu'il résulte de la loi attaquée, combinée avec la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, cette disposition 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, mais également dans la liberté d'expression et de culte, dans la liberté de presse, dans le droit de se réunir et de s'associer serait disproportionnée.

La combinaison de ces deux dispositions législatives aurait pour effet que sur simple demande du chef de service des services de renseignement et de sécurité, toutes les données téléphoniques et internet pourraient être demandées rétroactivement jusqu'à douze mois pour toute personne répondant à une des qualifications des compétences de la sûreté de l'Etat alors qu'aucune distinction ne serait établie entre les diverses activités qui

relèvent de la mission de ces services, ce qui pourrait aboutir à des abus de pouvoir au détriment d'individus ou d'organisations critiques à l'égard du gouvernement ou du système politique. La loi pourrait également stimuler l'autocensure des citoyens dès lors qu'elle provoque un sentiment diffus de surveillance, ce qui peut exercer une influence décisive sur l'exercice par les citoyens européens de leur liberté d'expression et d'information.

A.9.2.3.2. A la critique exposée au point c) selon laquelle l'article 5 de la loi du 30 juillet 2013 pourrait donner lieu à des abus de pouvoir, le Conseil des ministres répond que la loi contient suffisamment de garanties afin d'éviter les abus et que les compétences des personnes concernées ont été définies clairement.

A.9.2.3.3. Les parties requérantes contestent que les garanties contre les abus soient proportionnées à l'obligation générale de conservation.

Elles relèvent que le chef des services de renseignement et de sécurité décide, sans la moindre restriction légale, qui peut consulter les données demandées. Les anciennes garanties prévues dans la loi sur les services de renseignement ne suffisent pas pour sécuriser les données qui sont conservées durant une longue période.

A.9.2.3.4. Le Conseil des ministres répète que la décision du chef de service d'accomplir un acte d'instruction doit être motivée et que cette décision relève du contrôle de la commission administrative créée par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

A.9.2.4.1. Dans un point d), les parties requérantes soutiennent que la loi est insuffisamment précise en ce qui concerne le pouvoir d'appréciation des autorités concernées. Il est reproché à l'article 126, § 2, a), de la loi du 13 juin 2005 relative aux communications électroniques de ne désigner aucune autorité compétente. Quant au d) de cette disposition, il ne mentionnerait pas directement le pouvoir d'appréciation des services de renseignement précités mais uniquement les missions de renseignement mêmes, ce qui constituerait une autre notion que le pouvoir d'appréciation de ces services.

A.9.2.4.2. Le Conseil des ministres conteste que la loi soit insuffisamment précise s'agissant du pouvoir d'appréciation des autorités publiques concernées, dès lors que ce pouvoir d'appréciation ne porte pas sur la conservation des données qui est réglée par l'article 5 attaqué de la loi du 30 juillet 2013, mais sur l'accès à ces données, qui est réglé par le Code d'instruction criminelle et par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

A.9.2.4.3. Les parties requérantes répondent qu'un régime existant d'accès aux données est appliqué en ce qui concerne la conservation générale des données, sans la moindre précision par rapport à ce stockage massif de données.

A.9.2.5.1. Dans un point e), il est soutenu que la loi ne prévoit pas de contrôle juridictionnel suffisant contre les atteintes arbitraires des autorités. La loi ne satisferait pas à la « qualité de la loi » compte tenu de ce que le stockage ou la destruction des données et le contrôle de leur sécurisation seraient entièrement laissés au fournisseur d'un réseau ou service de communication électronique sans qu'aucun mécanisme de contrôle n'ait été prévu. La loi prévoirait, en effet, tout au plus que l'accès aux données doit se faire par les membres de la Cellule de coordination de la justice. L'externalisation de la conservation des données ainsi dénoncée aurait également été critiquée par l'avocat général auprès de la Cour de justice de l'Union européenne.

A.9.2.5.2. Le Conseil des ministres répond que la Cellule de coordination de la justice est la seule qui se charge du stockage et de la destruction des données. Pour ce qui est du contrôle juridictionnel, le Conseil des ministres se réfère à ce qu'il a déjà exposé concernant les garanties relatives à la conservation des données et les sanctions pénales applicables en cas d'infractions aux prescriptions.

A.9.2.5.3. Les parties requérantes répliquent que la Cellule de coordination de la justice n'est pas un organe juridictionnel ou administratif indépendant.

Il n'y a pas de contrôle juridictionnel préalable de l'accès aux données et l'intervention d'un juge pénal porte uniquement sur la répression *post factum* des infractions.

A.9.2.6.1. 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. Tous les délits et les crimes peuvent en effet faire l'objet non seulement de la conservation mais également de l'exploitation des données à caractère personnel conservées. L'avocat général auprès de la Cour de justice aurait également dénoncé le caractère disproportionné de la directive sur ce point.

A.9.2.6.2. Le Conseil des ministres conteste que la notion de faits punissables ne réponde pas au principe de légalité en matière pénale et soit disproportionnée. Par référence aux articles 46*bis* et 88*bis* du Code d'instruction criminelle, le législateur a choisi de considérer toutes les infractions qualifiées en Belgique de crimes ou délits comme des « infractions graves » au sens de l'article 1er de la directive 2006/24/CE.

A.9.2.6.3. Selon les parties requérantes, il n'est pas satisfait au principe de légalité en matière pénale en faisant référence, pour la conservation générale des données, à tous les crimes et délits, ce que le citoyen doit en plus déduire des articles 46*bis* et 88*bis* du Code d'instruction criminelle.

A.9.2.7.1. Au point g), les parties requérantes dénoncent l'absence de définition des données à conserver par type de service ainsi que l'absence d'exigences auxquelles ces données doivent répondre. D'après les parties requérantes, il fallait à tout le moins inscrire dans la loi la distinction spécifique entre les données d'identification et les données de communication parce que, pour la première catégorie, il est prévu un délai de conservation illimité. Il ne serait pas justifié de conserver en fait toutes les données qui sont générées par internet ou par le téléphone en ce compris les données de communication que constituent les EMS (*enhanced media services*) et les MMS (*multimedia services*).

A.9.2.7.2. En ce qui concerne la critique, au point g), selon laquelle le législateur n'a pas lui-même décidé quelles données relatives au transfert de données, à la localisation et à l'identification sont visées, le Conseil des ministres répond qu'il était justifié, compte tenu de l'évolution rapide du secteur des télécommunications, que le Roi soit habilité à donner un contenu aux principes fixés par la loi, après l'avis de diverses instances, et à adapter le cas échéant la réglementation à court terme.

A.9.2.7.3. Selon les parties requérantes, leur critique n'est pas réfutée par des arguments pratiques relatifs à l'évolution rapide du secteur des télécommunications et par la circonstance que des organes consultatifs interviennent.

A.9.2.7.4. Pour le Conseil des ministres, l'évolution rapide du secteur reste effectivement un motif valable pour conférer une délégation au Roi. Le Conseil des ministres relève que l'arrêté royal du 19 septembre 2013 portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques n'a pas été attaqué au Conseil d'Etat.

A.9.2.8.1. Dans un point h), les parties requérantes dénoncent à nouveau le délai de conservation des données prévu par la loi attaquée.

A.9.2.8.2. En ce qui concerne la critique du délai de conservation des données, le Conseil des ministres relève l'avis du Conseil d'Etat et la réponse donnée au cours des travaux préparatoires.

Selon le Conseil des ministres, une conservation des données de plus de vingt-quatre mois après la dernière communication n'est pas possible, de sorte que l'article 6 de la directive 2006/24/CE est respecté.

Une éventuelle prorogation du délai par le législateur ou le Roi dépend d'une évaluation de l'application dans la pratique. Quoi qu'il en soit, la Cour ou le Conseil d'Etat pourraient exercer un contrôle à cet égard.

A.9.2.8.3. Les parties requérantes estiment que le Conseil des ministres ne répond pas à la question du Conseil d'Etat de savoir si le délai de conservation de vingt-quatre mois prévu dans la directive 2006/24/CE n'est pas dépassé en ce qui concerne la conservation des données d'identification.

Selon les parties requérantes, la modification du délai de conservation ne peut être laissée au Roi. L'évaluation doit se faire par la Chambre des représentants et c'est dès lors la Chambre qui doit procéder à une éventuelle adaptation.

A.9.2.8.4. Le Conseil des ministres reste d'avis que l'article 6 de la directive 2006/24/CE n'est pas violé, étant donné qu'une conservation des données de plus de vingt-quatre mois est impossible. Par ailleurs, la directive n'est plus applicable, dès lors qu'elle a été invalidée.

Selon le Conseil des ministres, s'il devait estimer qu'une prolongation éventuelle du délai de conservation par le Roi à dix-huit mois n'est pas justifiée, le législateur peut lui-même inscrire le délai de douze mois dans la loi et exclure la possibilité de proroger ce délai. Par ailleurs, il reste possible d'introduire un recours à la Cour ou au Conseil d'Etat.

A.10. Dans un deuxième moyen, les parties requérantes dans l'affaire n° 5859 dénoncent la violation des articles 5, 10 et 11 de la Convention européenne des droits de l'homme ainsi que de l'article 2 du Quatrième Protocole additionnel à cette Convention. Elles dénoncent également la violation des articles 9, 12 et 19 du Pacte international relatif aux droits civils et politiques, de même que des articles 10, 11, 12, 19, 25, 26 et 27 de la Constitution et du principe de proportionnalité.

A.11.1. Dans une première branche du moyen, il est soutenu que la loi attaquée porte atteinte à la libre expression de l'information et des idées et à la liberté de la presse. Les parties requérantes dénoncent le fait que quatre services très divers ont la possibilité de demander des données de communication conservées douze mois et des données d'identité conservées durant une période en principe illimitée. Il n'est même pas précisé quels sont les services visés à l'article 126, § 2, a), b) et d), de la loi du 13 juin 2005 relative aux communications électroniques, ce qui devrait être déduit par le citoyen. Seul le service sous l'article 126, § 2, c), serait désigné, à savoir le Service de médiation pour les télécommunications. Il pourrait en être déduit que le procureur du Roi, les services de police, le juge d'instruction, les chefs de service de la sûreté de l'Etat et de la sûreté de l'armée et éventuellement également le Service de médiation pour les télécommunications, les services d'urgence téléphoniques quels qu'ils soient pourraient demander les données à caractère personnel qui ont été conservées. La légalité et la proportionnalité ne seraient donc pas assurées tant en ce qui concerne les données qui peuvent être conservées et consultées relativement à la poursuite d'infractions pénales qu'en ce qui concerne les compétences étendues des services de renseignement et de sécurité belges.

D'après les parties requérantes, si le citoyen doit tenir compte du fait que les données sont conservées afin de savoir avec qui il communique, quand et combien de temps il communique, cette information pouvant ensuite être traitée en dehors du cadre du service à des fins multiples, il ne pourra plus communiquer librement. Les parties requérantes appuient leur argumentation avec la jurisprudence de la Cour constitutionnelle allemande et celle de la Cour constitutionnelle roumaine.

A.11.2. Le Conseil des ministres répond que cette branche critique aussi l'accès aux données, alors que la loi attaquée règle uniquement la conservation des données.

Les dispositions de l'article 126, § 2, a), b), c) et d), de la loi du 13 juin 2005 relative aux communications électroniques ne constituent pas la transposition de la directive 2006/24/CE, mais constituent la mise en œuvre de la compétence du législateur pour donner accès aux données, sur la base de l'article 15 de la directive 2002/58/CE. La législation à laquelle il est fait référence indique clairement quelles personnes peuvent demander l'accès aux données et à quelles personnes l'information peut être procurée.

Le Conseil des ministres ajoute que les données sont à présent aussi conservées pour la facturation et pour la recherche d'infractions et d'appels malveillants et pour les services de renseignement.

Les données conservées ne peuvent être communiquées que lorsqu'une personne est soupçonnée d'être impliquée dans un des faits énumérés à l'article 126, § 2, précité.

Selon le Conseil des ministres, la conservation des données ne va pas au-delà de ce qui est nécessaire pour protéger la sécurité publique et la liberté d'expression n'est dès lors pas violée.

Les données sont conservées en vue de la sécurité publique. L'équilibre entre le but recherché et la protection du droit à la vie privée et à la liberté d'expression est assuré.

Le Conseil des ministres observe que les citoyens innocents ont aussi intérêt à ce que les données puissent aboutir à une identification rapide tant des citoyens innocents que des citoyens coupables. Il ne saurait dès lors être question d'une atteinte manifestement déraisonnable aux droits fondamentaux invoqués au moyen.

Selon le Conseil des ministres, il n'y a, en l'occurrence, pas d'effet de dissuasion dont il est question dans l'arrêt de la Cour constitutionnelle allemande cité par les parties requérantes. L'accès aux données reste limité à des cas bien précis qui intéressent la protection de la sûreté publique et le contenu des données n'est pas conservé.

A.11.3. Les parties requérantes répondent que les arguments du Conseil des ministres ont déjà été rejetés par la Cour de justice dans son arrêt du 8 avril 2014. L'enseignement de cet arrêt peut également être transposé à la loi attaquée.

Les parties requérantes relèvent que les données qui sont conservées pour la facturation ont un autre contenu, poursuivent un autre but et sont d'une autre envergure que les données qui doivent être conservées sur la base de la loi attaquée. Les données de facturation ne contiennent qu'une fraction de ce qui doit être conservé selon la loi attaquée. Dans la pratique, ces données ne sont conservées que durant trois mois et sont ensuite stockées sur un serveur qui n'est plus directement accessible à l'opérateur.

L'ancien article 126 de la loi du 13 juin 2005 relative aux communications électroniques, qui constituait une mise en œuvre de la directive 2002/58/CE, était d'une autre nature et ne visait pas une conservation générale des données pour les quatre objectifs visés dans l'actuel article 126.

Les parties requérantes persistent à affirmer que les arguments du Conseil des ministres ne sauraient justifier une conservation générale de toutes les données.

A.11.4. Dans son mémoire en réplique, le Conseil des ministres fait valoir que les parties requérantes n'indiquent pas en quoi les données qui sont conservées pour la facturation seraient différentes de celles qui doivent être conservées en vertu de la loi attaquée.

Le Conseil des ministres relève que le délai de prescription pour le recouvrement de factures impayées dans le secteur des télécommunications est de cinq ans et que les données sont donc conservées plus longtemps que ce qu'affirment les parties requérantes.

Par ailleurs, par le passé, les données étaient également conservées dans le cadre d'instructions judiciaires. L'importance de la consultation des données ne fait que croître en raison de l'informatisation de la société. Selon le Conseil des ministres, le citoyen qui est censé connaître la loi ne se sentira pas privé de sa liberté d'expression.

A.12.1. Dans une deuxième branche du deuxième moyen, les parties requérantes soutiennent que la non-compensation du coût de la conservation des données donnerait lieu à une diminution du nombre de services gratuits et donc à une diminution du nombre de données qui peuvent circuler librement. La limitation de la libre circulation des idées et des opinions limiterait ainsi injustement et de manière disproportionnée la liberté d'expression consacrée par l'article 10 de la Convention européenne des droits de l'homme.

A.12.2. Selon le Conseil des ministres, le législateur a choisi de ne pas prévoir un mécanisme d'indemnités supplémentaires parce que les frais de la conservation des données, comme le prévoit la loi attaquée, ne constituent qu'une petite partie des frais réalisés dans le cadre de l'identification et de l'interception, que règle la loi, des données électroniques.

Le Conseil des ministres rappelle que les données sont déjà conservées pour la facturation et pour la recherche d'infractions et d'appels malveillants et pour les services de renseignement.

A.12.3. Les parties requérantes répondent qu'il n'est pas prouvé que les obligations relatives à la conservation des données de communications pour une période d'un an et des données d'identification durant une période couvrant sans doute des dizaines d'années ne constitueraient qu'une petite partie des frais.

A.13.1. Dans une troisième branche du deuxième moyen, les parties requérantes dénoncent l'atteinte par la loi attaquée au secret professionnel des médecins, avocats, journalistes et ecclésiastiques ainsi qu'aux activités politiques et commerciales qui requièrent la confidentialité. Or, le secret professionnel et le secret des sources seraient des droits fondamentaux protégés par la Constitution qui sont d'une importance capitale pour la sauvegarde d'un Etat de droit démocratique. Une atteinte à ces droits ne serait admissible que dans des circonstances tout à fait exceptionnelles lorsque la nécessité et l'urgence peuvent être démontrées et si des garanties procédurales strictes sont prévues, ce qui ne serait pas le cas en l'espèce.

A.13.2. Selon le Conseil des ministres, la distinction que les parties requérantes établissent suivant que les communications électroniques sont soumises au secret professionnel ou non n'est pas pertinente. En effet, la conservation des données ne porte pas sur le contenu de la communication mais uniquement sur les données visées à l'article 5 de la loi du 30 juillet 2013. Par conséquent, le contenu reste protégé par le secret professionnel.

Par ailleurs, les données étaient également conservées pour la facturation et pour d'autres raisons.

Le Conseil des ministres fait valoir que le secret professionnel ne peut être levé que si le praticien de la profession est soupçonné d'avoir lui-même commis une infraction.

A.13.3. Les parties requérantes répondent que des conclusions précises peuvent être tirées des données conservées et que, de la sorte, le secret des sources et le secret professionnel peuvent être violés.

A.13.4. Le Conseil des ministres estime que l'instauration d'un régime spécifique de conservation des données pour des personnes tenues au secret professionnel constituerait une nouvelle forme de conservation des données. Un tel système d'exceptions rendrait le système général lui-même impraticable. En outre, les opérateurs seraient obligés de déterminer eux-mêmes quelles personnes sont tenues au secret professionnel.

A.14. Dans le troisième moyen, les parties requérantes dans l'affaire n° 5859 allèguent la violation des articles 6 et 13 de la Convention européenne des droits de l'homme, de l'article 14 du Pacte international relatif aux droits civils et politiques ainsi que des articles 10 et 11 de la Constitution et du principe général de la présomption d'innocence.

A.15.1. Dans une première branche du moyen, les parties requérantes dénoncent la violation de la présomption d'innocence par des déclarations ou décisions qui insinueraient la faute d'une personne, inciteraient le public à croire en la faute de cette personne ou anticiperaient l'appréciation des faits par le juge compétent. Ainsi, les utilisateurs de communications téléphoniques et d'internet se trouveraient dans une position manifestement moins favorable que les utilisateurs de correspondance non électronique qui ne font pas l'objet d'une obligation générale de conservation. Il se pourrait également qu'une personne autre que le véritable utilisateur fasse usage des services de télécommunication ou soit victime d'un vol d'identité, ce qui impliquerait que des communications potentiellement suspectes ne soient pas imputées au véritable utilisateur du service. Dans de tels cas, les citoyens seraient ainsi confrontés à un renversement de la charge de la preuve, une présomption de faute étant établie à charge de l'utilisateur de communications téléphoniques et d'internet, alors qu'une telle présomption n'existe pas dans le chef des utilisateurs de la correspondance traditionnelle non électronique.

A.15.2. Le Conseil des ministres répète que la conservation de données n'implique pas leur consultation. Il n'est pas possible de savoir à l'avance qui commettra une infraction.

Selon le Conseil des ministres, la présomption d'innocence n'est pas renversée par la loi attaquée et il n'est pas question d'un contrôle préventif par les autorités publiques.

Le Conseil des ministres estime qu'il n'y a pas de différence de traitement entre les opérateurs et les services de courrier électronique. Ces derniers entrent aussi dans le champ d'application de la loi attaquée.

Selon le Conseil des ministres, la différence de traitement par rapport aux services postaux conventionnels porte sur une catégorie incomparable. Les données d'identification du courrier ordinaire ne peuvent être conservées sans méconnaître le secret des lettres. L'enveloppe ne doit pas mentionner l'expéditeur et la lettre même ne doit pas mentionner un nom.

A.15.3. Les parties requérantes répliquent que le Conseil des ministres se fonde sur la thèse selon laquelle tout citoyen doit être considéré comme un suspect potentiel. Il est donc confirmé que la loi attaquée ne respecte pas la présomption d'innocence.

Selon les parties requérantes, le Conseil des ministres ne réfute pas la critique du caractère disproportionné de la mesure, que la Cour de justice a constaté par son arrêt du 8 avril 2014.

A.16.1. Les parties requérantes dénoncent, dans une deuxième branche du moyen, l'absence de voies de recours effectives. En effet, le caractère secret de la conservation et de la demande de données de communication et d'identification prévue par la loi attaquée aurait pour effet que l'on ne sait pas toujours qu'une infraction à un droit fondamental a eu lieu, contre laquelle une voie de recours adéquate peut être mise en œuvre. Les voies de recours prévues par la loi du 13 juin 2005 relative aux communications électroniques et la loi du 8 décembre 1992 relative à la protection de la vie privée ne seraient pas suffisantes dès lors qu'il s'agit en l'espèce d'une conservation générale de données à caractère personnel et non d'une conservation spécifique.

A.16.2. Le Conseil des ministres répond que l'obligation générale de conservation découle de la loi attaquée et que le citoyen est censé connaître la loi.

Il déclare ne pas apercevoir comment et contre quoi les parties requérantes souhaiteraient introduire un recours dans le cadre de cette obligation de conservation.

Selon le Conseil des ministres, la critique des parties requérantes porte à nouveau sur la consultation des données, qui est réglée par une autre législation.

A.16.3. Les parties requérantes répliquent que le Conseil des ministres ne répond pas au grief selon lequel la loi attaquée n'institue pas une voie de recours spécifique qui réponde à la gravité de l'ingérence dans la vie privée.

A.17. Dans un quatrième moyen, les parties requérantes dans l'affaire n° 5859 allèguent la violation de l'article 1 du Premier Protocole additionnel à la Convention européenne des droits de l'homme, des articles 10, 11 et 16 de la Constitution et du principe général de proportionnalité.

A.18.1. Il est soutenu, dans une première branche du moyen, que la loi attaquée a pour effet de créer une discrimination entre les petits Internet Service Providers (ISP) et les ISP étrangers, d'une part, et les grands ISP et les ISP qui opèrent en Belgique, d'autre part, dès lors que ces derniers ne peuvent contourner l'obligation de conservation des données tandis que les premiers peuvent se soustraire au coût considérable qu'implique une telle conservation. L'obligation légale ainsi imposée par la loi attaquée pourrait avoir pour conséquence une perte de clients pour les entreprises belges constitutive d'une atteinte à leur droit de propriété.

A.18.2. Le Conseil des ministres observe en premier lieu qu'un contrôle au regard des articles 10 et 11 de la Constitution ne peut dépasser le champ d'application territorial de la Constitution et de la loi, qui se limite à la Belgique.

Le Conseil des ministres fait valoir que les parties requérantes font allusion à une charge financière lourde, sans en apporter la moindre preuve.

Par ailleurs, 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 prévoit un système d'indemnités pour les actions fondées sur les articles 46*bis* et 88*bis* du Code d'instruction criminelle. Ces indemnités visent à compenser certains frais exposés en vue de la recherche et de la communication de données aux autorités judiciaires.

L'arrêté royal du 12 octobre 2010 déterminant les modalités de l'obligation de collaboration légale en cas de demandes concernant les communications électroniques par les services de renseignement et de sécurité prévoit que les fournisseurs peuvent recevoir certaines indemnités pour leurs services.

Le Conseil des ministres conclut qu'il est effectivement prévu une série de compensations financières pour les tâches des fournisseurs et que les frais ne constituent pas une charge disproportionnée. Il observe qu'aucun fournisseur n'a introduit un recours en annulation au Conseil d'Etat.

A.18.3. Les parties requérantes se réfèrent à titre de réplique à ce qu'elles ont exposé en ce qui concerne la deuxième branche du deuxième moyen concernant les coûts supplémentaires pour les fournisseurs.

A.19.1. Dans une deuxième branche du moyen, les parties requérantes dans l'affaire n° 5859 allèguent l'existence d'une atteinte au droit de propriété des *providers* en ce que la loi attaquée aurait les mêmes effets qu'une expropriation formelle sans qu'une compensation adéquate ne soit prévue. En effet, une obligation générale de conservation des données priverait les fournisseurs de leur droit de propriété si les appareils qui sont utilisés pour le service fourni ne peuvent être modernisés afin de couvrir les frais de la conservation des données.

A.19.2. Le Conseil des ministres souligne que la loi attaquée poursuit un but d'intérêt général, qui justifie un règlement du droit de propriété. Il se réfère à ce qu'il a déjà exposé concernant ce but.

Le Conseil des ministres se réfère également au régime d'indemnisation auquel il a déjà fait allusion dans le cadre de la première branche de ce moyen. Il conclut que la charge financière de la conservation des données n'est pas à ce point lourde qu'elle l'emporte sur les objectifs d'intérêt général qui sont poursuivis par la loi attaquée.

A.19.3. Les parties requérantes persistent à affirmer que l'obligation générale de conservation a une incidence à ce point importante sur le droit de propriété qu'il n'y a pas de juste équilibre entre l'exigence de l'intérêt général et les droits des fournisseurs.

- *B* -

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 90*decies* 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 46*bis* et 88*bis* 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 43*bis*, § 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 90*decies* 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 œuvre 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 3*ter* rédigé comme suit :

' § 3*ter*. 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 90*decies* du Code d'instruction criminelle

Art. 7. L'article 90*decies* 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 État 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 46*bis* à 88*bis* 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 États 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 États 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 90*decies* 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, Le président,

F. Meersschaut J. Spreutels