Numéros du rôle : 6590, 6597, 6599 et 6601
Arrêt n° 96/2018 du 19 juillet 2018

A R R E T

En cause : les recours en annulation de la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques, introduits par l'Ordre des barreaux francophones et germanophone, par l'ASBL « Académie Fiscale » et Jean Pierre Riquet, par l'ASBL « Liga voor Mensenrechten » et l'ASBL « Ligue des Droits de l'Homme » et par Patrick Van Assche et autres.

La Cour constitutionnelle,

composée des présidents J. Spreutels et A. Alen, et des juges L. Lavrysen, J.-P. Snappe, J.-P. Moerman, E. Derycke, T. Merckx-Van Goey, P. Nihoul, F. Daoût et R. Leysen, assistée du greffier P.-Y. Dutilleux, 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 10 janvier 2017 et parvenue au greffe le 11 janvier 2017, 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 la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques (publiée au *Moniteur belge* du 18 juillet 2016).

b. Par requête adressée à la Cour par lettre recommandée à la poste le 16 janvier 2017 et parvenue au greffe le 17 janvier 2017, un recours en annulation de la même loi a été introduit par l'ASBL « Académie Fiscale » et Jean Pierre Riquet.

c. Par requête adressée à la Cour par lettre recommandée à la poste le 17 janvier 2017 et parvenue au greffe le 18 janvier 2017, un recours en annulation de la même loi a été introduit par l'ASBL « Liga voor Mensenrechten », assistée et représentée par Me J. Vander Velpen, avocat au barreau d'Anvers, et l'ASBL « Ligue des Droits de l'Homme », assistée et représentée par Me R. Jespers, avocat au barreau d'Anvers.

d. Par requête adressée à la Cour par lettre recommandée à la poste le 18 janvier 2017 et parvenue au greffe le 19 janvier 2017, un recours en annulation de la même loi a été introduit par Patrick Van Assche, Christel Van Akeleyen et Karina De Hoog, assistés et représentés par Me D. Pattyn, avocat au barreau de Bruges.

Ces affaires, inscrites sous les numéros 6590, 6597, 6599 et 6601 du rôle de la Cour, ont été jointes.

Le Conseil des ministres, assisté et représenté par Me S. Depré et Me E. de Lophem, avocats au barreau de Bruxelles (dans les affaires n^{os} 6590 et 6597) et assisté et représenté par Me J. Vanpraet et Me Y. Peeters, avocats au barreau de Bruges (dans les affaires n^{os} 6599 et 6601), a introduit des mémoires, les parties requérantes, à l'exception des parties requérantes dans l'affaire n° 6597, ont introduit des mémoires en réponse et le Conseil des ministres a également introduit des mémoires en réplique.

Par ordonnance du 1er mars 2018, 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 21 mars 2018 et les affaires mises en délibéré.

A la suite des demandes de plusieurs parties à être entendues, la Cour, par ordonnance du 21 mars 2018, a fixé l'audience au 25 avril 2018.

A l'audience publique du 25 avril 2018 :

- ont comparu :

. Me E. Lemmens, Me J.-F. Henrotte et Me P. Limbrée, avocat au barreau de Liège, pour la partie requérante dans l'affaire n° 6590;

. Me J. Vander Velpen et Mr. R. Jespers, pour les parties requérantes dans l'affaire n° 6599;

. Me D. Pattyn, pour les parties requérantes dans l'affaire n° 6601;

. Me E. de Lophem, qui comparaissait également *loco* Me S. Depré, pour le Conseil des ministres dans les affaires n^{os} 6590 et 6597;

. Me J. Vanpraet, pour le Conseil des ministres dans les affaires n^{os} 6599 et 6601;

. Me J. Van Cauter, avocat au barreau de Gand, pour « Child Focus », partie intervenante à l'audience;

- 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° 6590, soutient que les dispositions attaquées portent 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, de l'identifier, d'identifier ses clients ainsi que les dates et heures de la communication.

A.1.2. L'ASBL « Académie Fiscale », première partie requérante dans l'affaire n° 6597, s'est donné pour objet social, entre autres, d'assurer la représentation officielle des intérêts généraux de l'ensemble des professionnels comptables, juridiques et fiscaux au point de vue juridique, économique, fiscal, administratif et social, et ce vis-à-vis de toutes les instances politiques, professionnelles, interprofessionnelles et autres, européennes, internationales, nationales et régionales, ainsi que d'assurer en particulier la représentation et la défense des intérêts communs des fiscalistes et des conseillers fiscaux auprès d'instances diverses. Elle a également pour objet social d'assurer la représentation et la défense des intérêts communs des contribuables ou groupes définis de contribuables belges ou étrangers, sans jamais pouvoir assurer la défense des intérêts particuliers d'un contribuable. A son estime, la disposition attaquée dans son recours est susceptible d'affecter directement et défavorablement la situation des comptables fiscalistes, des experts-comptables et des conseillers

fiscaux ainsi que celle des contribuables ou assujettis que ces professions défendent dans la mesure où la consultation des métadonnées conservées permet de déterminer si un professionnel comptable et fiscal a été consulté, d'identifier ce professionnel, d'identifier ses clients ainsi que les dates et heures de leurs communications.

A.1.3. La seconde partie requérante dans l'affaire n° 6597 est une personne physique, professionnelle dans le domaine de la fiscalité et donc soumise au secret professionnel en vertu des règles déontologiques dues à son inscription au tableau des conseillers fiscaux de l'Institut des experts-comptables et conseillers fiscaux.

A.1.4. L'ASBL « Liga voor Mensenrechten » et l'ASBL « Ligue des Droits de l'Homme », parties requérantes dans l'affaire n° 6599, renvoient à leurs statuts et justifient leur intérêt à demander l'annulation des dispositions attaquées par le fait que celles-ci seraient de nature à porter atteinte à de nombreux droits fondamentaux tels que le droit au respect de la vie privée, le droit à la protection des données personnelles, le droit à la fiabilité des communications, le droit à la liberté personnelle, le droit à la liberté d'expression, d'association et de réunion, la liberté de la presse, le droit de propriété, le droit à un procès équitable, le droit à un recours effectif, le principe de la légalité en matière pénale, le principe de proportionnalité, la sécurité juridique, le principe du raisonnable et celui de la présomption d'innocence.

A.1.5. Les parties requérantes dans l'affaire n° 6601 sont des personnes physiques, habitants du Royaume, qui font usage sur le territoire belge de différents services de communications électroniques par suite d'un contrat conclu avec un opérateur, tels la téléphonie fixe, les services mobiles et l'accès internet à haut débit. Elles sont par ailleurs conseillers communaux au conseil communal de Brecht et indiquent bénéficier en cette qualité d'un droit renforcé à la liberté d'expression tel qu'il est garanti par l'article 10 de la Convention européenne des droits de l'homme et par l'article 11 de la Charte des droits fondamentaux de l'Union européenne.

Elles justifient leur intérêt à demander l'annulation de la loi attaquée par le fait que celle-ci impose de conserver les données à caractère personnel qui les concernent, ces données pouvant être traitées et communiquées à diverses autorités. La loi attaquée affecterait de la sorte directement et défavorablement le droit à la protection de leur vie privée et de leurs données à caractère personnel. Les parties requérantes critiquent également le fait que la loi attaquée modifie le Code d'instruction criminelle et règle un aspect essentiel de la forme dans laquelle une personne peut être poursuivie au sens de l'article 12 de la Constitution, de sorte que toute personne physique qui se trouve sur le territoire belge a en permanence intérêt à ce que les règles relatives au traitement des données à caractère personnel dans le cadre de la procédure pénale respectent et garantissent le droit à un procès équitable et le principe de légalité en matière pénale.

Quant au fond

Quant aux affaires n^{os} 6590 et 6597

A.2. Un moyen unique dans l'affaire n° 6590 est pris de la violation des articles 10 et 11 de la Constitution, combinés ou non 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.

A.3.1. L'Ordre des barreaux francophones et germanophone fait grief à la loi 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.

Il est relevé que l'absence de distinction entre les personnes dont les communications sont soumises au secret professionnel et les autres a récemment été critiquée par la Cour de justice de l'Union européenne dans un arrêt du 21 décembre 2016 (CJUE, arrêt *Tele2 Sverige AB*, C-203/15 et *Secretary of State for the Home Department*, C-698/15).

A.3.2. Selon la partie requérante, aucun élément ne justifie par ailleurs que l'obligation généralisée de conservation des données s'applique tant aux justiciables qui font l'objet d'une mesure d'enquête ou de poursuite pour des faits susceptibles de donner lieu à des condamnations pénales qu'aux justiciables qui ne font pas l'objet d'une telle mesure. D'après la partie requérante, cette obligation généralisée n'a pas été modifiée par la loi attaquée, qui a simplement modalisé l'accès aux données collectées. Si ces modalités doivent être précisées par le pouvoir exécutif, la délégation accordée à celui-ci doit être considérée comme excessive. La partie requérante ajoute que, bien que les termes employés par la nouvelle loi soient formellement différents, les catégories de données qui sont visées sont semblables à celles qui font l'objet 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, annulé par l'arrêt de la Cour n° 84/2015, du 11 juin 2015. Il est soutenu que si la loi attaquée visait à répondre à cette annulation, les obligations de conservation qu'elle impose sont à nouveau excessives par rapport aux objectifs du législateur.

La partie requérante insiste sur le fait que la situation discriminatoire qu'elle dénonce est autant préjudiciable aux avocats qu'aux justiciables, le secret professionnel de l'avocat étant d'intérêt général. Il s'agit ainsi 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. Il est rappelé que le secret professionnel de l'avocat constitue un principe qui touche directement aux droits à un procès équitable et au respect de la vie privée. Il ne peut donc y être porté atteinte que dans des cas exceptionnels moyennant le respect de garanties adéquates et suffisantes contre les abus.

La partie requérante dénonce le fait que les justiciables ne pourront jamais avoir la certitude de pouvoir consulter un avocat en toute confiance sans que l'existence et les circonstances de cette consultation ne soient révélées ou ne puissent être invoquées à leur encontre. Des poursuites pénales pourraient ainsi être diligentées par les autorités compétentes sur la base de données confidentielles consultées.

D'après la partie requérante, contrairement à ce qu'a soutenu le législateur dans les travaux préparatoires, 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 de secrets professionnels via un mécanisme de filtre à l'entrée. En effet, le législateur pourrait facilement contraindre les opérateurs de communications à prendre note de la qualité du titulaire de secrets professionnels de leurs clients et à partager cette information entre eux. Des bases de données pourraient ainsi être créées et utilisées par les opérateurs qui ne verseraient pas les métadonnées générées par les communications entrantes et sortantes des avocats des autres titulaires du secret professionnel dans les bases de données ainsi constituées.

A.3.3. La partie requérante relève encore que la loi attaquée encadre uniquement l'accès aux données et précise quelles sont les catégories de données accessibles aux différentes catégories de personnes pouvant prétendre y avoir accès mais ne modifie en rien la portée généralisée de l'obligation de conservation des données. S'il s'agit d'une amélioration par rapport à la loi du 30 juillet 2013, les droits garantis par l'article 6 de la Convention européenne des droits de l'homme et par l'article 47 de la Charte des droits fondamentaux de l'Union européenne n'en sont pas pour autant respectés dès lors que la disposition attaquée n'offre pas la possibilité d'un quelconque contrôle juridictionnel, à aucun stade de la procédure.

A.3.4. La partie requérante relève que l'article 4, § 3, de la loi attaquée prévoit en substance que les données sont conservées pendant une durée de douze mois. L'article 8 de la loi introduit toutefois dans l'article 46*bis*, § 1er, du Code d'instruction criminelle une exception concernant les infractions qui ne sont pas de nature à entraîner un emprisonnement principal d'un an ou plus. Dans ce cas de figure en effet, les données requises ne peuvent concerner que les six mois précédant la demande.

Les articles 9, § 2, et 14, § 2, de la loi attaquée concernent par ailleurs à nouveau l'accès aux données et non leur durée de conservation à proprement parler. Or, d'après la partie requérante, la durée de conservation des données est en soi excessive. D'une part, les infractions qui ne sont pas de nature à entraîner un emprisonnement principal d'un an ou plus sont peu nombreuses. D'autre part, l'Etat belge ne justifie pas la durée retenue, tout particulièrement en ce qui concerne les métadonnées relatives aux communications des avocats.

Alors que dans son arrêt n° 84/2015, la Cour avait relevé, en ce qui concerne la durée de conservation des données, que la loi n'opérait aucune distinction entre les catégories de données en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées, la loi attaquée n'opère toujours aucune distinction entre les catégories de données, si ce n'est en réduisant l'accès à certaines données en fonction de la peine qui peut être prononcée.

L'Ordre des barreaux francophones et germanophone insiste également sur le fait qu'il en est d'autant plus ainsi que les points de départ des délais de conservation ne sont pas non plus mis en relation avec des circonstances justifiant éventuellement cette conservation. Le Conseil d'Etat a d'ailleurs souligné dans son avis que les données d'identification de l'article 46*bis* pouvaient *de facto* être conservées pour une durée beaucoup plus longue que douze mois, dès lors que le délai de conservation commence à courir à « la date à partir de laquelle une communication est possible pour la dernière fois à l'aide du service utilisé ».

A.3.5. D'après la partie requérante, la loi attaquée viole encore les dispositions visées au moyen en ce que l'obligation généralisée de conservation des données s'applique tant aux justiciables qui font l'objet d'une mesure d'enquête ou de poursuite pour des faits susceptibles de donner lieu à des condamnations pénales qu'aux justiciables qui ne font pas l'objet de telles mesures. La justification apportée par le législateur à cet égard ne peut convaincre puisque le droit pénal repose sur le principe de présomption d'innocence avec pour corollaire que la charge de la preuve repose sur le ministère public et que le doute profite à la personne poursuivie. Il ne serait dès lors pas pertinent d'invoquer le fait que la mesure peut tout aussi bien bénéficier à la victime d'une infraction.

La partie requérante ajoute qu'aucune information n'est donnée quant à la réelle utilité de ce mécanisme de conservation des données dans la prévention, la détection et la répression de ces infractions graves. L'Etat belge se contente d'affirmations générales quant à l'utilité présupposée de la mesure et la nécessité de l'appliquer de manière générale et indifférenciée à l'ensemble de la population belge, ce qui serait totalement disproportionné à l'objectif poursuivi.

L'Ordre des barreaux francophones et germanophone se fonde sur les travaux préparatoires de la loi pour indiquer que le Gouvernement feint de ne pas comprendre la référence à d'autres mécanismes moins attentatoires à la vie privée de l'ensemble des citoyens comme les méthodes de repérage existantes en droit belge ou de « *quick freeze* » qui visent une décision obligeant les opérateurs à conserver des données à propos de personnes identifiées dans une zone géographique ou une période temporelle délimitée. Le raisonnement de l'Etat belge reposerait en réalité sur une volonté politique de poursuivre à tout prix dans la voie de la conservation générale des données sous prétexte d'un contexte de risque terroriste et malgré l'inconstitutionnalité du système de surveillance généralisé mis en place. La partie requérante ajoute que la loi viole d'autant plus les dispositions visées au moyen qu'il existerait un risque non négligeable que les bases de données pertinentes soient gérées avec légèreté par les opérateurs réticents face au contrôle qu'entraîne cette nouvelle obligation.

Il ne pourrait être objecté que les opérateurs conserveraient déjà les données en question pour des raisons de facturation. En effet, cet argument contredit le nouvel article 126, § 2, *in fine*, qui interdit auxdits opérateurs d'utiliser les données conservées pour d'autres finalités que celles qui sont prévues par la loi, en ce compris donc pour la facturation de leurs services. En outre, si les opérateurs conservent et traitent effectivement certaines données à des fins de facturation, la loi querellée leur impose de conserver des éléments qu'ils ne conserveraient pas, pas sous cette forme et, en toute hypothèse, pas pendant la même durée.

A.3.6. La partie requérante ajoute qu'aucun mécanisme de contrôle n'est actuellement prévu pour permettre aux titulaires et aux bénéficiaires du secret professionnel de s'opposer à la collecte, à la conservation ou à la prise de connaissance de données couvertes par le secret professionnel de l'avocat. Or, cette prise de connaissance des données, même si elles ne sont pas produites par après à l'appui d'un dossier, suffit à porter atteinte au secret professionnel.

A.3.7. Enfin, la partie requérante indique que les fournisseurs de services pourront conserver les données concernées à l'étranger, sur tout le territoire européen, et ce malgré le caractère sensible et confidentiel de

certaines données, ce qui aggrave considérablement le risque qu'elles puissent être accessibles à des tierces personnes ou divulguées.

A.4.1. Dans l'affaire n° 6597, les parties requérantes prennent un moyen unique de la violation des articles 10 et 11 de la Constitution, combinés ou non avec les articles 6 et 8 de la Convention européenne des droits de l'homme, ainsi qu'avec les articles 7, 8, 11 et 47 de la Charte des droits fondamentaux de l'Union européenne.

A.4.2. Les parties requérantes font grief 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 professionnels comptables et fiscaux et les autres utilisateurs de ces services sans tenir compte du statut particulier des professionnels comptables et fiscaux, du caractère fondamental du secret professionnel auquel ils sont soumis et de la nécessaire relation de confiance qui doit les unir à leurs clients. Il est également reproché aux dispositions attaquées de traiter de manière identique les justiciables qui font l'objet de mesures d'enquête ou de poursuite pour des faits susceptibles de s'inscrire dans la finalité de la conservation des données électroniques litigieuses et ceux qui ne font pas l'objet de telles mesures. Les arguments développés dans la requête sont similaires à ceux qui ont été développés dans l'affaire n° 6590.

A.5.1. Dans son mémoire, le Conseil des ministres commence par exposer en quoi la loi attaquée répondrait aux critiques qui ont été formulées par la Cour de justice de l'Union européenne et par la Cour relativement à l'ancienne réglementation applicable.

A.5.2. Quant au moyen unique soulevé dans l'affaire n° 6590, le Conseil des ministres indique que le requérant critique l'habilitation excessive que donnerait la loi au pouvoir exécutif en ce qui concerne la définition des données devant être conservées par les opérateurs sans toutefois préciser quelles dispositions ou principes seraient violés. Or, d'après le Conseil des ministres, le législateur se serait montré particulièrement prudent sur ce point. En effet, la loi identifie avec précision le type de métadonnées visées et « délègue la précision à apporter avec une grande prudence également puisqu'elle prévoit que l'arrêté devra être délibéré en Conseil des ministres et être précédé d'avis spécifiques », notamment celui du régulateur sectoriel (l'Institut belge des services postaux et des télécommunications; ci-après : l'IBPT).

A.5.3. Le Conseil des ministres soutient ensuite que le secret professionnel de l'avocat, s'il relève de l'ordre public, n'est pas absolu. Le principe de proportionnalité « doit permettre d'apprécier les limites posées par la nécessité ou d'autres principes ou valeurs en conflit, le cas échéant, avec ce secret professionnel ».

A.5.4. Le Conseil des ministres observe que la critique relative à la proportionnalité de la loi attaquée s'articule en treize points dans la requête en annulation, auxquels il s'efforce de répondre dans l'ordre.

A.5.5. Il rappelle d'abord que la loi attaquée répond aux enseignements de la jurisprudence, en particulier l'arrêt n° 84/2015 de la Cour ainsi que les arrêts *Digital Rights* et *Tele2 Sverige* de la Cour de justice de l'Union européenne.

A.5.6. Le Conseil des ministres souligne ensuite que la loi attaquée ne porte pas sur la collecte des données. En effet, celle-ci ne résulte pas tant de la loi que du contrat entre l'opérateur et son client, ce qui suppose l'accord de ce dernier. Il pourrait du reste difficilement être imaginé techniquement qu'un client qui souhaite passer un appel refuse à son opérateur de savoir quel est le destinataire de cet appel. Le Conseil des ministres indique encore qu'il serait inexact de soutenir, comme le fait la partie requérante, que la loi attaquée ne prévoit aucune limite à la conservation des données, puisqu'une durée de conservation est expressément prévue par la loi.

A.5.7. En ce qui concerne l'accès aux données, la loi attaquée prévoit des limites relatives au secret professionnel, notamment celui de l'avocat. Il est encore indiqué que la loi ne vise que les métadonnées à l'exclusion du contenu des communications (appel ou e-mail, par exemple). Elle n'affecte dès lors pas réellement la confidentialité des échanges entre l'avocat et son client. Il serait au contraire disproportionné de faire échapper totalement au dispositif légal les communications de et vers les titulaires de professions soumises au secret professionnel. En effet, ce n'est pas parce qu'une adresse mail est utilisée par un titulaire du secret

professionnel que tous les messages qui parviennent à cette adresse ou en proviennent sont effectivement protégés par le secret professionnel. Le Conseil des ministres indique qu'il ne faut pas perdre de vue que les titulaires du secret professionnel sont eux-mêmes susceptibles de commettre des infractions graves.

A.5.8. A l'égard des justiciables qui ne pourraient plus se confier à leur avocat en confiance, le Conseil des ministres indique que le législateur a pris toutes les précautions pour que l'objectif poursuivi, dont la légitimité n'est pas contestée, puisse être rencontré sans porter une atteinte disproportionnée au droit à la vie privée et au droit à un procès équitable.

A.5.9. Quant au fait de conserver des données selon que l'intéressé soit détenteur d'un secret professionnel ou non, le Conseil des ministres rappelle que les travaux préparatoires ont souligné les difficultés techniques de telles solutions et le fait que d'autres Etats membres de l'Union n'ont pu trouver de formule technique de différenciation des personnes. En outre, une telle différenciation ne protégerait pas tant le secret professionnel lui-même que la personne de celui qui, par profession, est dépositaire de secrets. Cette différenciation aurait pour effet d'exclure du champ d'application de la loi non seulement ce qui relève du secret professionnel mais également ce qui n'en relève pas du tout sous prétexte que les informations recueillies utiliseraient le même canal que les informations qui relèveraient du secret professionnel.

A.5.10. A la critique liée à l'absence de possibilité de recours contre la décision prescrivant la mesure de consultation des données conservées ainsi que des mesures prises sur la base de cette décision, le Conseil des ministres répond que l'accès aux données conservées fait effectivement l'objet d'un contrôle juridictionnel dans le cadre de l'enquête pénale qui est exercée par la Commission BIM, composée de magistrats indépendants, dans le cas où ce sont les services de renseignement qui ont accès aux informations.

A.5.11. En ce qui concerne la durée de conservation des données, le Conseil des ministres souligne que la loi prévoit une gradation basée en substance sur la gravité de l'infraction. Quant à l'objection de la partie requérante selon laquelle les durées visées aux articles 9 et 14 de la loi concernent l'accès aux informations plutôt que leur conservation en tant que telle, le Conseil des ministres soutient que cette objection est peu pertinente dès lors que l'obligation de conservation précède logiquement l'accès aux informations conservées. Seule la demande d'accès permettra de déterminer la gravité de l'infraction ou de la menace visée aux articles 9 et 14 précités. Le Conseil des ministres ajoute que, dès lors que la loi prévoit que l'accès aux informations concernées est modulé par la gravité de l'infraction ou de la menace, il est difficile de déterminer *a priori*, catégorie d'informations par catégorie d'informations, quelle en sera l'utilité pour une enquête particulière. Le Conseil des ministres ajoute enfin que la partie requérante n'indique pas pourquoi les délais ainsi prévus par la loi seraient en soi disproportionnés.

A.5.12. Sur l'absence de distinction légale entre les justiciables selon qu'ils font ou non l'objet d'une enquête ou de poursuites, le Conseil des ministres relève que le dispositif de la loi attaquée permet précisément aux enquêteurs, dans un cadre soigneusement déterminé, d'accéder à certaines métadonnées concernant une personne faisant l'objet d'une telle enquête. Cela suppose que ces métadonnées aient été conservées en amont de l'enquête et donc à un moment où il n'était pas possible d'opérer la différenciation visée par le requérant.

A.5.13. Quant au fait que les opérateurs pourraient traiter avec légèreté les données qui ont été conservées, le Conseil des ministres soutient qu'une telle information ne repose sur aucune base sérieuse et souligne que le respect par les opérateurs de communications électroniques de leurs obligations légales fait l'objet d'un contrôle par le régulateur sectoriel, en l'occurrence l'IBPT, ce contrôle étant assorti de sanctions qui peuvent aller jusqu'au retrait d'une licence.

A.5.14. Le Conseil des ministres précise qu'aucun système préventif alternatif ne pourrait éviter que des données qui relèvent du secret professionnel soient conservées et, le cas échéant, que l'on puisse y avoir accès, comme le prévoit la loi. Le Conseil des ministres ajoute que, pour déterminer si une information relève du secret professionnel, il faut nécessairement la traiter au préalable. Les alternatives envisagées par la partie requérante ne permettraient pas d'échapper à cette réalité. Sur le fait que les informations recueillies pourraient être conservées à l'étranger, le Conseil des ministres rappelle que la loi prévoit expressément que les informations qu'elle vise doivent être conservées dans l'Union européenne.

A.6. Sur le moyen unique soulevé dans l'affaire n° 6597, le Conseil des ministres formule trois brèves observations complémentaires aux arguments formulés en réponse au moyen unique dans le recours en annulation n° 6590.

Il relève que le moyen invoque la violation de l'article 11 de la Charte des droits fondamentaux de l'Union européenne mais que la partie requérante n'expose pas en quoi la liberté d'expression se trouverait mise en péril par la loi attaquée. Le Conseil des ministres observe, dans un deuxième temps, que les parties requérantes se fondent sur l'arrêt de la Cour n° 10/2008, du 23 janvier 2008, pour affirmer que le secret professionnel des professionnels comptables et fiscaux constitue un principe général de droit qui participe du respect des droits fondamentaux. Or, d'après le Conseil des ministres, dans cet arrêt la Cour n'envisageait que le secret professionnel de l'avocat, distinguant cette profession des autres professions libérales le cas échéant soumises au secret professionnel. Dans un troisième temps, le Conseil des ministres s'interroge sur la manière dont la collecte, la conservation et l'accès aux métadonnées peut concrètement porter atteinte au secret professionnel des personnes concernées. Les parties requérantes ne s'expliqueraient pas sur ce point dans leur requête.

A.7.1. Dans son mémoire en réponse, la partie requérante dans l'affaire n° 6590 soutient que, contrairement à ce qu'affirme le Conseil des ministres, la loi attaquée n'est pas conforme aux enseignements de la jurisprudence européenne et de la Cour. Les discriminations et atteintes alléguées seraient en outre disproportionnées par rapport au but poursuivi par le législateur.

L'Ordre des barreaux francophones et germanophone relève que dans l'arrêt du 21 décembre 2016, *Tele2 Sverige AB*, C-203/15, et *Secretary of State for the Home Department*, C-698/15, la Cour de justice de l'Union européenne a précisé qu'une réglementation nationale permettant à titre préventif la conservation ciblée des données relatives au trafic et des données de localisation à des fins de lutte contre la criminalité grave pouvait être admise dans la mesure strictement nécessaire énoncée dans cet arrêt. D'après la partie requérante, la conservation ciblée préconisée par la Cour de justice de l'Union européenne correspondrait précisément à celle que le législateur a en l'espèce estimée à tort impossible. Un commentaire doctrinal récent de cet arrêt de la Cour de justice de l'Union européenne conclurait d'ailleurs à l'inadéquation de la législation belge avec les conclusions de la Cour.

D'après la partie requérante, la thèse défendue par le législateur dans les travaux préparatoires et par le Conseil des ministres dans son mémoire reviendrait pour l'essentiel à affirmer qu'ils ne partagent pas l'avis de la Cour de justice de l'Union européenne et/ou celui de la Cour.

A.7.2. Quant à l'argument du Conseil des ministres selon lequel il serait impossible de déterminer *a priori* des catégories de personnes qui ne seraient pas susceptibles d'être concernées ou impliquées de manière plus ou moins indirecte par les infractions graves, que ce soit en tant que victime, suspect ou témoin, cela ne permettrait pas de justifier une ingérence aussi grave dans la vie privée des citoyens. Il en irait d'autant plus ainsi que la Cour de justice de l'Union européenne a condamné la généralisation de cette mesure et a fourni plusieurs pistes d'éléments objectifs qui peuvent fonder une application ciblée de ladite mesure. L'issue logique devrait être de ne pas mettre en place une mesure qui visera l'ensemble des citoyens mais au contraire de s'abstenir de mettre en place une mesure généralisée.

A.7.3. D'après la partie requérante, le Conseil des ministres admet que le législateur n'a pas pu répondre à l'ensemble des critiques formulées par la jurisprudence pour considérer que la directive 2006/24/CEE était illégale. Il indique toutefois qu'un seul élément ne pourrait suffire à constituer une violation du principe de proportionnalité au sens de la jurisprudence de la Cour de justice et de celle de la Cour. Or, ce présupposé serait inexact et contraire à l'arrêt de la Cour de justice de l'Union européenne du 21 décembre 2016.

A.7.4. Quant à l'accès aux données, la partie requérante indique qu'elle ne partage pas l'analyse du Conseil des ministres et de la section de législation du Conseil d'Etat lorsqu'ils soutiennent que le renforcement des règles entourant l'accès aux données conservées suffirait à justifier la conservation généralisée de données. Si la Cour de justice considère qu'une réglementation autorisant la conservation généralisée de données et ne prévoyant aucune limitation objective à l'accès aux données n'est pas conforme au droit européen, en aucun cas, elle n'aurait à l'inverse jugé que des critères d'accès aux données ne puissent être admis de manière à rendre la réglementation valide.

A.7.5. En toute hypothèse, la loi querellée encadrerait uniquement l'accès aux données mais n'offrirait toujours aucune possibilité de contrôle juridictionnel à quelque stade que ce soit de la procédure. La partie requérante relève à cet égard que la possibilité d'un contrôle judiciaire relatif à l'accès à des données dans le cadre d'une enquête pénale ou la possibilité d'un contrôle par la Commission BIM en matière de services de renseignements concernent uniquement l'accès aux données et non leur collecte ou leur conservation et ne pourraient en aucun cas se confondre avec un recours ouvert au tiers concerné par ces données. En effet, cette forme d'autocontrôle n'offre pas les mêmes garanties.

A.7.6. D'après l'Ordre des barreaux francophones et germanophone, il ressortirait clairement du recours que l'habilitation excessive donnée au pouvoir exécutif et l'absence de définition suffisante des données devant être conservées participe de la disproportion de la mesure et donc de la violation des dispositions visées au moyen. Le fait que l'habilitation conférée au Roi soit pour partie d'ordre technique ne serait pas de nature à justifier que le législateur n'ait pratiquement fixé aucune limite quant aux données susceptibles d'être conservées.

A.7.7. En ce qui concerne l'absence totale de prise en compte du secret professionnel, la partie requérante soutient que la conservation des données est intimement liée à leur collecte, et cette conservation ainsi que la consultation des données participent bel et bien au caractère disproportionné de la mesure.

A.7.8. A l'argument du Conseil des ministres selon lequel la loi querellée n'affecterait pas réellement la confidentialité des échanges entre un avocat et son client, la partie requérante répond que les données récoltées, même si elles ne concernent pas le contenu des échanges, permettent de dresser une réelle carte d'identité digitale de la personne concernée. Il sera ainsi possible, pour les autorités, de déterminer si une personne suspectée d'avoir commis une infraction a pris contact avec un avocat pénaliste, de connaître la date, l'heure, la durée de la communication, ainsi que le matériel de communication des utilisateurs, le lieu d'utilisation du matériel mobile, etc. Ainsi, la consultation des métadonnées conservées permet de prendre connaissance du fait qu'un avocat a été contacté et de déterminer l'identité de cet avocat et de son interlocuteur. Ces données sont encore plus précises que celles qui figurent dans l'agenda professionnel d'un avocat qui est pourtant une pièce confidentielle.

A.7.9. Quant à la durée de la conservation des données, d'après la partie requérante, l'existence d'une gradation basée sur la gravité de l'infraction n'impliquerait pas automatiquement que la durée de conservation des données soit proportionnée à l'objectif poursuivi. En effet, comme l'a souligné la section de législation du Conseil d'Etat dans son avis sur l'avant-projet de loi, les données d'identification de l'article 46*bis* du Code d'instruction criminelle peuvent *de facto* être conservées pour une durée beaucoup plus longue que douze mois. Le législateur n'aurait pas répondu autrement à cet argument qu'en affirmant d'autorité que ce ne serait pas toujours le cas en pratique. Il ressortirait d'une analyse des données fournies par l'IBPT que la majorité des demandes sont formulées dans les trois mois de l'enregistrement des données. L'expérience de 2014 et de 2015 tendrait à démontrer que les délais de conservation fixés dans la loi ne correspondent même pas à des besoins réels des services de renseignement ou de la justice, ce qui constituerait une preuve du caractère excessif du délai fixé par la loi.

A.7.10. En ce qui concerne l'absence de différence de traitement entre les personnes concernées par une enquête ou des poursuites pénales et les autres justiciables, la partie requérante rappelle que la Cour de justice de l'Union européenne exige que la mesure soit délimitée quant au public et aux situations potentiellement concernées, la réglementation nationale devant être fondée sur des éléments objectifs qui permettent « de viser un public dont les données sont susceptibles de révéler un lien, au moins indirect, avec des actes de criminalité graves, de contribuer d'une manière ou une autre à la criminalité grave ou de prévenir un risque grave pour la sécurité publique ». Or, tel ne serait pas le cas en l'espèce.

A.7.11. Quant à l'augmentation des coûts engendrés par la conservation des données, il serait peu probable que les opérateurs de communications électroniques recourent à une augmentation répercutée sur les consommateurs plutôt qu'à des sous-traitants moins onéreux. Or, l'augmentation d'intermédiaires et la

multiplication des transferts entraîneraient mécaniquement une augmentation de la surface d'attaque. Si les opérateurs de communications électroniques pouvaient être tenus responsables *a posteriori* d'une fuite de données, le dommage serait tout de même réalisé et probablement irréparable.

A.7.12. La partie requérante ajoute encore que la loi attaquée permet aux opérateurs de communications électroniques de transférer des données collectées à des fins de conservation et pour des raisons de sous-traitance vers d'autres Etats membres de l'Union européenne. Or, les réglementations nationales applicables dans d'autres Etats membres autorisent par exemple les services de renseignements à obtenir des opérateurs de communications électroniques ou des prestataires de service de la société de l'information nationaux des informations sur les données que ces prestataires manipulent. La partie requérante cite l'exemple de la loi française. Cet exemple serait de nature à démontrer que la conservation et le traitement des données dans un autre Etat membre doté d'une telle législation, et dont il n'est pas exclu que les intérêts économiques, industriels ou scientifiques soient opposés à ceux de la Belgique, pourraient créer un risque spécifique pour les données des citoyens belges, risque auquel ces données ne seraient pas exposées si elles étaient conservées en Belgique.

A.7.13. A l'affirmation du Conseil des ministres selon laquelle il ne serait pas possible de mettre en place un système généralisé qui éviterait l'atteinte au secret professionnel, la partie requérante répond que la déduction logique aurait dû alors être de ne pas mettre en place la loi querellée dans la mesure où celle-ci contrevenait à un droit fondamental.

A.8.1. Dans son mémoire en réplique, le Conseil des ministres souligne dans un premier temps que la législation nationale en Suède et au Royaume-Uni qui a été examinée par la Cour de justice dans son arrêt du 21 décembre 2016 avait pour objectif la lutte contre la criminalité grave tandis que la loi attaquée s'est donné un objectif plus large. Par conséquent, le constat opéré par la Cour de justice de l'inadéquation ou de la disproportion d'une législation nationale par rapport à l'objectif de lutte contre la criminalité grave ne peut être transposé *mutatis mutandis* à une législation nationale dont l'objectif est différent.

A.8.2. Subsidiairement, le Conseil des ministres suggère que la Cour adresse à la Cour de justice une question préjudicielle qui pourrait être formulée de la manière suivante :

« L'article 15, paragraphe 1, de la directive 2002/58/CE, lu en combinaison avec le droit à la sécurité, garanti par l'article 6 de la Charte des droits fondamentaux de l'Union européenne, et le droit au respect des données personnelles, tel que garanti par les articles 7, 8 et 52, § 1, de la Charte des droits fondamentaux de l'Union européenne, doit-il être interprété en ce sens qu'il s'oppose à une réglementation nationale telle que celle en cause, qui prévoit une obligation générale pour les opérateurs et fournisseurs de services de communications électroniques de conserver les données de trafic et de localisation au sens de la directive 2002/58/CE, générées ou traitées par eux dans le cadre de la fourniture de ces services; réglementation nationale qui n'a pas seulement pour objectif la recherche, la détection et la poursuite de faits de criminalité grave, mais également la garantie de la sécurité nationale, de la défense du territoire et de la sécurité publique, la recherche, la détection et la poursuite d'autres faits que ceux de criminalité grave ou la prévention d'un usage interdit des systèmes de communication électronique, ou la réalisation d'un autre objectif identifié par l'article 13, § 1, de la directive 95/46/CE; réglementation nationale qui est en outre sujette à de strictes garanties sur le plan de la conservation des données et de l'accès à celles-ci ? ».

A.8.3. Le Conseil des ministres observe, dans un deuxième temps, que dans l'arrêt précité de la Cour de justice, celle-ci suggère que ne serait pas contraire au droit de l'Union, et notamment à la Charte des droits fondamentaux de l'Union européenne, une réglementation qui autoriserait la collecte, la conservation et l'accès des autorités nationales compétentes aux données relatives aux communications électroniques si cette réglementation était ciblée. D'après le Conseil des ministres, cette porte ouverte par la Cour de justice serait théorique. En effet, la Cour n'a pas été amenée dans cet arrêt à examiner la conformité d'une réglementation concrète qui correspondrait à ces caractéristiques de ciblage. Or, le Conseil des ministres rappelle qu'il doute qu'un tel système puisse être mis en place sans emporter de violation du principe d'égalité entre citoyens.

A.8.4. A titre plus subsidiaire, le Conseil des ministres soutient que certaines dispositions particulières de la loi attaquée ne doivent en toute hypothèse pas être annulées dans la mesure où elles ont un objet qui dépasse celui de la loi attaquée. Il s'agit plus particulièrement de l'article 2, alinéa 1er, a, de la loi, qui complète la loi du

13 juin 2005 relative aux communications électroniques en précisant la notion d'opérateur, ainsi que des articles 12 à 16 de la loi, qui concernent les modifications de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, à l'exception de la modification concernant les articles 18/3, § 2, 10°, et 18/8 de cette loi. Le Conseil des ministres souligne à cet égard que les recours portent sur la loi attaquée de manière générale mais ne formulent aucun grief relatif à ces dispositions en particulier.

A.8.5. A titre infiniment subsidiaire, le Conseil des ministres demande à la Cour de maintenir les effets de la loi attaquée si elle venait à être annulée.

Quant aux affaires n^{os} 6599 et 6601

En ce qui concerne l'obligation générale de conservation des données

A.9.1. Un premier moyen dans l'affaire n° 6599 est pris de la violation des articles 10, 11, 12, 15, 22 et 29 de la Constitution, lus isolément et/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, avec l'article 17 du Pacte international relatif aux droits civils et politiques, avec les principes généraux de sécurité juridique, de proportionnalité et d'autodétermination en matière d'information ainsi qu'avec l'article 5, § 4, du Traité de l'Union européenne.

A.9.2. Le premier moyen dans l'affaire n° 6601 est pris de la violation de l'article 8 de la Convention européenne des droits de l'homme, des articles 7, 8, 11.4 et 52 de la Charte des droits fondamentaux de l'Union européenne, des articles 10, 11, 19 et 22 de la Constitution, de l'article 2, a, de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ainsi que des articles 1, 2, 3, 5, 6, 9 et 15 de la directive 2002/58/CE 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.

D'après les parties requérantes, l'obligation de conservation générale et indifférenciée des données d'identification, des données de connexion et de localisation et des données de communication personnelle imposée par la loi attaquée aux fournisseurs de services de téléphonie, en ce compris par internet, d'accès à internet, de courrier électronique par internet, aux opérateurs qui fournissent des réseaux publics de communications électroniques ainsi qu'aux opérateurs qui fournissent un de ces services, constituerait une ingérence dans le droit à la protection de la vie privée qui ne serait pas strictement nécessaire dans une société démocratique pour sauvegarder la sécurité nationale, c'est-à-dire la sûreté de l'Etat, la défense nationale, la sécurité publique ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisation non autorisée du système de communication électronique comme visé à l'article 13, § 1er, de la directive 95/46/CE.

A.9.3. Les parties requérantes dans l'affaire n° 6599 renvoient à l'arrêt de la Cour de justice de l'Union européenne du 8 avril 2014 dans les affaires *Digital Rights Ireland* et *Seitlinger* et relèvent que, dans la doctrine, certains ont affirmé qu'un stockage général de données de tous les utilisateurs sans distinction était devenu impossible à la suite de cet arrêt.

Elles relèvent également que, par son arrêt du 11 juin 2015, la Cour a annulé la législation belge relative à la conservation des données 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. La Cour a suivi les grandes lignes du raisonnement tenu par la Cour de justice de l'Union européenne dans l'arrêt *Digital Rights Ireland* précité. A la suite de l'arrêt d'annulation rendu par la Cour, une loi de réparation a vu le jour. D'après les parties requérantes, le nouvel avant-projet de loi ne tenait pas compte de l'essence de la jurisprudence de la Cour de justice de l'Union européenne et de la Cour dès lors qu'il partait de l'hypothèse que les arrêts précités n'empêchaient nullement de conserver les données de tous les citoyens de manière non ciblée et non différenciée.

Les parties requérantes indiquent encore que l'avant-projet et le projet de loi ont maintenu, outre l'obligation générale de conservation des données, qui, en soi, ne satisfait déjà pas à la condition de proportionnalité, une période de conservation qui s'élève en principe à douze mois, soit le double du délai

minimum de six mois qui s'applique à la conservation de données. L'approche disproportionnée poursuivie par l'article 126 annulé de la loi relative aux communications électroniques a par ailleurs été maintenue dans la mesure où les données conservées peuvent également être utilisées par les services de renseignement et dans la mesure où cette option demeure ouverte pour à peu près n'importe quelle infraction. L'exposé des motifs a indiqué clairement qu'il était impossible pour le législateur de répondre aux exigences de la Cour de justice de l'Union européenne et de la Cour constitutionnelle. Il serait en effet irréalisable de fixer dans la future loi des critères objectifs et concrets qui permettent d'opérer une distinction entre des citoyens suspects et des citoyens non suspects ainsi que de limiter pour cette dernière catégorie l'obligation de conservation à une période donnée dans une zone géographique donnée et à des groupes déterminés.

Les parties requérantes relèvent encore que, dans son arrêt du 21 décembre 2016, la Cour de justice de l'Union européenne a affirmé que le droit de l'Union, en l'espèce la directive « vie privée et communications électroniques » lue à la lumière de la Charte des droits fondamentaux de l'Union européenne, s'opposait à une réglementation nationale prévoyant une conservation générale et indifférenciée des données. Après avoir cité plusieurs passages de l'arrêt, les parties requérantes concluent qu'à supposer qu'une telle obligation générale de conservation ne puisse en soi être considérée comme dépassant les limites du strict nécessaire, elle doit en tout cas être entourée de toutes les garanties que la Cour de justice de l'Union européenne a citées dans l'arrêt *Digital Rights Ireland* et dans l'arrêt *Tele2 Sverige AB*. Dans cette dernière affaire, l'avocat général a souligné que ces garanties étaient impératives, cumulatives et minimales.

A.9.4. Les parties requérantes dans l'affaire n° 6601 indiquent que la Cour peut examiner si le législateur a respecté les engagements internationaux qui découlent de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et 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, ces obligations constituant un ensemble indissociable avec les garanties contenues dans l'article 22 de la Constitution. Ici encore, les parties requérantes se réfèrent à l'arrêt de la Cour de justice de l'Union européenne du 21 décembre 2016. Elles soulignent que l'obligation de conservation des données prévue par la loi attaquée correspond en grande partie à l'obligation de conservation des données prévue par la directive relative à la conservation des données, ainsi que l'a constaté la Cour de justice au considérant 97 de l'arrêt précité. Les données qui font l'objet de cette obligation de conservation contiennent, en effet - comme c'était le cas sous la directive concernant la conservation des données -, les données qui permettent de distinguer la source et la destination de la communication, les données qui permettent de localiser tant la source que la destination de la communication, les données relatives à la date, au moment et à la durée de la communication et les données permettant d'établir le type de communication et le type d'appareil utilisé.

Les parties requérantes dans l'affaire n° 6601 en concluent que l'obligation générale de conservation des données prévue par la loi attaquée constitue une atteinte particulièrement grave au droit au respect de la vie privée et familiale et au droit à la protection des données à caractère personnel, indépendamment du fait que les données conservées ne portent pas sur le contenu de la communication. L'obligation de conservation et l'accès aux données conservées ont également une incidence sur l'utilisation de moyens de communication électronique et donc sur la façon dont les utilisateurs de ces moyens de communication font usage de leur liberté d'expression. C'est la raison pour laquelle les parties requérantes invoquent également les dispositions internationales et constitutionnelles qui garantissent cette liberté d'expression au titre de normes de référence qui auraient été violées. Compte tenu de la gravité de l'atteinte à ces droits fondamentaux, seule la lutte contre la criminalité grave pourrait justifier cette mesure. Or, comme la Cour de justice l'a considéré au point 103 de son arrêt du 21 décembre 2016, la lutte contre la criminalité grave ne peut en soi justifier une conservation générale et indifférenciée de toutes les données de trafic et de toutes les données de localisation. Cela reviendrait, en effet, à ce que la conservation de ces données devienne la règle alors que, selon les articles 5 et 15 de la directive relative à la vie privée et aux communications électroniques, l'interdiction de conserver ces données est la règle tandis que leur conservation constitue une exception.

L'obligation de conservation des données prévue dans la loi attaquée ne serait pas limitée à ce qui est strictement nécessaire, soit en ce qui concerne les catégories de données à conserver, soit en ce qui concerne les moyens de communication concernés, les personnes et la durée de la conservation. La délégation au Roi pour déterminer les données à conserver par type de catégories et les exigences auxquelles doivent répondre les

données ne préciserait pas suffisamment quelles sont les données qui doivent être conservées et n'établirait pas davantage les conditions essentielles auxquelles ces données doivent satisfaire.

Les parties requérantes soulignent enfin que si l'exposé des motifs de la loi se réfère à l'importance des données de communication pour les instructions en matière de terrorisme, de pédopornographie, de disparition inquiétante, de commerce illégal de stupéfiants, de vente de médicaments contrefaits sur internet, d'incitation à la haine ou à la violence, de harcèlement, de piratage de comptes bancaires et de vol d'identité, l'avocat général Henrik Saugmandsgaard a observé dans ses conclusions du 19 juillet 2016 que plusieurs études mettaient en question la nécessité d'une obligation générale de conservation en vue de la lutte contre la criminalité grave.

A.10.1. Dans son mémoire, le Conseil des ministres indique que les griefs formulés dans le premier moyen dans l'affaire n° 6599 et la première branche du premier moyen dans l'affaire n° 6601 sont identiques et doivent dès lors être examinés ensemble.

A.10.2. Il rappelle l'objectif du législateur par un renvoi aux travaux préparatoires de la loi attaquée. Il conclut que cet objectif diffère de la situation concrète qui a été examinée par la Cour de justice de l'Union européenne dans l'arrêt *Digital Rights Ireland* du 8 avril 2014 et dans l'arrêt *Tele2 Sverige AB* du 21 décembre 2016. En effet, dans ces arrêts, la Cour de justice de l'Union européenne devait se prononcer sur la question de savoir si l'obligation de conservation des données générales et indifférenciées était nécessaire et proportionnée au regard de la lutte contre la criminalité grave. Il n'est dès lors pas sans intérêt en l'espèce de souligner que la loi attaquée poursuit un autre but. Il s'agit de garantir l'intégrité du système pénal de même que d'améliorer la confiance du citoyen dans le fonctionnement de la justice par la recherche de la vérité, dans l'intérêt de la victime, de l'inculpé et de toutes les personnes concernées.

A.10.3. Pour le Conseil des ministres, il existe un rapport raisonnable de proportionnalité entre l'obligation générale de conservation des données et l'objectif poursuivi par le législateur qui serait en outre parfaitement conforme à l'article 15, alinéa 1er, de la directive 2002/58/CE. Si chaque citoyen n'est, en effet, pas potentiellement un criminel, chaque citoyen peut potentiellement être confronté à la criminalité, que ce soit en tant que victime, en tant que prévenu ou en tant que témoin et dès lors avoir un intérêt à la recherche de la vérité. L'obligation générale de conservation des données n'empêche pas que, sur le plan de la conservation elle-même, des garanties nécessaires à la protection de la vie privée soient introduites, de même que sur le plan de l'accès aux données en fonction du critère de gravité de la criminalité dans la période durant laquelle les données sont demandées. Le Conseil des ministres cite les garanties qui sont contenues à son estime dans l'article 26 de la loi attaquée en ce qui concerne la conservation des données pour assurer le respect de la sphère privée des personnes. Il en conclut que, compte tenu de cette garantie, l'obligation prescrite par la loi n'a pas un caractère disproportionné. D'après le Conseil des ministres, la loi attaquée n'est pas en contradiction avec la jurisprudence de la Cour de justice de l'Union européenne ni avec celle de la Cour.

A.10.4. Le Conseil des ministres insiste encore sur le fait que la Cour a conclu au caractère disproportionné de l'atteinte au droit au respect de la vie privée par la loi du 30 juillet 2013 en raison de la combinaison de quatre éléments : le fait que la conservation des données concernait toutes les personnes, l'absence de différence de traitement en fonction des catégories de données conservées et de leur utilité, l'absence ou l'insuffisance de règles, ce qui constituerait une ingérence dans le droit à la protection de la vie privée.

Or, ni la Cour de justice de l'Union européenne ni la Cour n'ont jugé que l'un de ces quatre éléments pouvait suffire à conclure au caractère disproportionné de la mesure. Le contrôle du principe de proportionnalité suppose en effet une approche globale.

A.10.5. Après avoir rappelé l'exposé des motifs de la loi attaquée, le Conseil des ministres conclut que tant la Commission de la protection de la vie privée que le Conseil d'Etat, section législation, ont remis un avis favorable en ce qui concerne l'obligation généralisée de conservation des données à condition qu'elle soit accompagnée de garanties suffisantes sur le plan de l'accès aux données, des délais de conservation, et de la protection et de la sécurité des données, de manière à ce que l'ingérence dans le droit à la protection de la vie privée soit limitée à ce qui est strictement nécessaire.

Contrairement à ce que soutiennent les parties requérantes, l'arrêt de la Cour de justice de l'Union européenne du 21 décembre 2016 ne remettrait nullement en cause ce constat.

A.11.1. D'après les parties requérantes dans l'affaire n° 6599, l'opinion émise par le Conseil des ministres ne repose pas sur une analyse objective des deux arrêts prononcés par la Cour de justice de l'Union européenne. Il ressortirait en effet de ces arrêts que la Cour n'admet pas une obligation générale de conservation des données, indépendamment des garanties éventuelles qui peuvent accompagner cette obligation en ce qui concerne l'accès, les délais, la sécurité ou la protection de ces données. La Cour européenne aurait en effet jugé la directive 2006/24/CE dans son ensemble et sous tous ses aspects et aurait estimé qu'elle présentait un caractère disproportionné non seulement sur le plan de la conservation des données mais également sur le plan de leur accès.

Le Conseil des ministres aurait également passé sous silence les critiques formulées par le Conseil d'Etat à l'encontre de la loi en projet.

A.11.2. Les parties requérantes dans l'affaire n° 6599 soutiennent que, dans son arrêt du 21 décembre 2016, la Cour de justice a jugé que l'obligation générale de conservation des données portait atteinte de manière disproportionnée au droit au respect de la vie privée et au droit à la protection des données à caractère personnel. Par cet arrêt, la Cour de justice aurait clairement rejeté l'interprétation souple de la loi préconisée par le Conseil des ministres, le Conseil d'Etat et la Commission de la protection de la vie privée. Cette jurisprudence serait dans la lignée de l'arrêt *Schrems*, du 6 octobre 2015, C-362/14.

A.11.3. Les parties requérantes dans l'affaire n° 6599 ajoutent enfin que, contrairement à ce que soutient le Conseil des ministres, les garanties qui ont été considérées par la Cour de justice de l'Union européenne comme nécessaires pour accompagner l'obligation de conservation des données dans les considérants 60 à 68 de son arrêt *Digital Rights Ireland* sont effectivement cumulatives, de sorte que l'absence de l'une d'elles peut emporter le caractère disproportionné de la mesure.

A.12.1. Dans leur mémoire en réponse, les parties requérantes dans l'affaire n° 6601 relèvent qu'une loi « portant modification de l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 16/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité » a été adoptée le 1er septembre 2016, avec une date d'entrée en vigueur fixée au 17 décembre 2016. La Commission de la protection de la vie privée aurait remis un avis favorable à propos de la loi en projet, indiquant toutefois que le législateur aurait négligé le principe de légalité. L'avis remis par le Conseil d'Etat irait dans le même sens. Cette loi a été exécutée par un arrêté royal du 27 novembre 2016 « relatif à l'identification de l'utilisateur final de services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée ».

D'après les parties requérantes, les données d'identification et les documents qui sont rassemblés dans le chef du consommateur final des cartes prépayées constitueraient des données d'identification et des moyens de communication au sens de l'article 126, § 3, de la loi du 13 juin 2005 et devraient donc être conservés sur la base de la loi attaquée.

A.12.2. Elles soutiennent que, contrairement à l'opinion du Conseil des ministres, l'arrêt de la Cour de justice de l'Union européenne du 21 décembre 2016 concerne toute réglementation nationale de lutte contre la criminalité qui prévoit une obligation générale de conservation des données et pas seulement lorsqu'il s'agit de lutter contre la criminalité grave. Dans cet arrêt, la Cour de justice aurait opté pour une interprétation restrictive.

Bien que le législateur ait indiqué que chaque citoyen peut être confronté à ce type de criminalité en tant qu'inculpé, victime ou témoin potentiel, cela n'entacherait pas le constat que la réglementation en cause entre dans le champ d'application de l'article 15 de la directive relative à la communication privée et électronique. L'arrêt de la Cour de justice de l'Union européenne précité trouverait donc à s'appliquer à la loi attaquée.

A.12.3. Les parties requérantes dans l'affaire n° 6601 ajoutent encore qu'une obligation générale et indifférenciée de conservation des données dépasse les limites de ce qui est nécessaire pour lutter contre la criminalité.

Le renvoi vers les avis du Conseil d'Etat et de la Commission de la protection de la vie privée ne serait pas utile puisque ceux-ci se fondent sur une interprétation souple de la jurisprudence européenne alors que celle-ci a jugé disproportionnée l'obligation de conservation générale des données.

A.13.1. Dans son mémoire en réplique, le Conseil des ministres indique, à titre préliminaire, que le recours ne peut porter que sur l'article 126 de la loi sur les communications électroniques, tel qu'inséré par la loi attaquée. En portant des critiques à l'encontre de la loi du 1er septembre 2016, les parties requérantes dans l'affaire n° 6601 invoqueraient un moyen nouveau qui n'est pas recevable dès lors qu'il est soulevé dans leur mémoire en réponse.

A.13.2. Le Conseil des ministres note également que bien que le premier moyen dans l'affaire n° 6601 vise l'article 2 dans son ensemble, aucun grief n'est dirigé contre l'article 2, alinéa 1er, a), de sorte qu'à l'égard de ce dernier, le moyen serait irrecevable.

A.13.3. Sur le fond, il soutient qu'il est impossible de lutter contre la criminalité grave telle que la cybercriminalité si l'on ne prévoit pas une obligation générale et indifférenciée de conservation des données de communication électronique. Il indique encore que la réglementation attaquée a un caractère proportionné et que le législateur a entendu chercher un équilibre entre le droit à la protection de la vie privée des personnes dont les données sont conservées, d'une part, et le droit à la sécurité de ces personnes ainsi que d'autres personnes tel qu'il est garanti par l'article 6 de la Charte des droits fondamentaux de l'Union européenne et l'article 5 de la Convention européenne des droits de l'homme, d'autre part. Il répète une fois encore qu'à son estime, il n'existe pas d'autre moyen pour atteindre les objectifs poursuivis par le législateur qu'imposer une obligation générale de conservation. Il serait, en effet, impossible de lutter de manière efficace contre la criminalité avec d'autres moyens. Toute différence de traitement qui serait introduite dans la réglementation serait constitutive de discrimination.

A.13.4. Pour le surplus, le Conseil des ministres conteste une fois encore les enseignements que tirent les parties requérantes de l'arrêt de la Cour n° 84/2015, prononcé ensuite de l'arrêt *Digital Rights Ireland* de la Cour de justice de l'Union européenne du 8 avril 2014, et soutient que la loi attaquée ne contrevient pas à la jurisprudence européenne.

A.13.5. En ordre subsidiaire, le Conseil des ministres suggère d'interroger la Cour de justice de l'Union européenne à propos de la compatibilité de la loi attaquée avec l'article 15, alinéa 1er, de la directive 2002/58/CE.

A.14.1. Dans la deuxième branche du premier moyen, invoquée à titre subsidiaire, les parties requérantes dans l'affaire n° 6601 soutiennent que l'obligation de conservation générale et indifférenciée des données conservées que la loi attaquée impose aux fournisseurs et aux opérateurs constitue une ingérence dans le droit à la protection de la vie privée qui n'est pas strictement nécessaire, appropriée et proportionnée dans une société démocratique pour sauvegarder la sûreté de l'Etat, la défense nationale, la sécurité publique ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisation non autorisée du système de communications électroniques comme le prévoit l'article 13, § 1er, de la directive 95/46/CE, du fait de la combinaison de l'obligation générale de conservation des données avec l'absence de garanties permettant de limiter cette ingérence à ce qui est strictement nécessaire.

La section de législation du Conseil d'Etat et la Commission de la protection de la vie privée ont relevé que l'arrêt de la Cour de justice de l'Union européenne du 8 avril 2014 pouvait être interprété de deux manières : dans une première interprétation, l'illégalité de l'obligation de conservation générale et indifférenciée des données résulterait de l'absence de garanties suffisantes relatives à l'accès aux données conservées et au délai de conservation; dans une deuxième interprétation, l'obligation de conservation serait illégale, précisément en raison de son caractère général et indifférencié. Il est à noter que le Conseil d'Etat et la Commission de la protection de la vie privée se sont fondés sur la première de ces deux interprétations. L'exposé des motifs de la loi reconnaît également que l'obligation de conservation générale et indifférenciée des données ne correspondait pas à l'arrêt de la Cour du 11 juin 2015 ainsi qu'à l'arrêt de la Cour de justice de l'Union européenne du 8 avril 2014 mais estime que cela peut être compensé par une réglementation plus stricte concernant les autres aspects, à savoir une différenciation sur la base des catégories des données conservées et de leur utilité, des règles relatives à l'accès des autorités aux données concernées et des règles en matière de sécurité des données auprès des fournisseurs ou des opérateurs. Il est soutenu que, dans la mesure où la Cour déclarerait la première branche du

moyen non fondée, il y aurait lieu de constater que l'obligation de conservation générale des données ne répond pas davantage à l'interprétation souple qui a été faite de l'arrêt de la Cour de justice de l'Union européenne du 8 avril 2014 en raison de l'absence de garanties pour limiter cette ingérence dans le droit à la protection de la vie privée et des données à caractère personnel à ce qui est strictement nécessaire.

A.14.2. Les parties requérantes précisent que les deuxième, troisième et quatrième moyens prouvent que cette obligation générale de conservation telle qu'elle est instaurée par la loi attaquée n'est pas entourée de garanties suffisantes en matière d'accès aux données, en matière de délai de conservation et en matière de protection et de sécurité des données, de sorte que la loi attaquée viole les dispositions visées au moyen. Les parties requérantes se fondent sur les conclusions de l'avocat général Henrik Saugmandsgaard précédant l'arrêt de la Cour de justice de l'Union européenne précité, selon lequel toutes les garanties que la Cour cite aux points 60 à 68 de l'arrêt auraient un caractère contraignant et devraient par conséquent accompagner l'obligation générale de conservation des données pour limiter à ce qui est strictement nécessaire l'atteinte aux droits reconnus par la directive 2002/58/CE et par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne.

A.15. Dans son mémoire, le Conseil des ministres répète la position qu'il a défendue à propos de la première branche du moyen, à savoir qu'une obligation générale et indifférenciée de conservation des données ne viole pas, en soi, les dispositions visées au moyen, à condition que cette obligation s'accompagne de garanties nécessaires sur le plan de la sécurité, de la conservation, de l'accès aux données, du délai de conservation et de la protection et la sécurité des données qui impliquent une ingérence dans le droit à la protection de la vie privée limitée à ce qui est strictement nécessaire. Le Conseil des ministres répète également que l'arrêt de la Cour de justice de l'Union européenne du 21 décembre 2016 n'impose pas que ces garanties aient un caractère cumulatif. Le Conseil des ministres cite la doctrine à l'appui de son argumentation.

A.16. Dans leur mémoire en réponse, les parties requérantes relèvent que c'est à juste titre que le Conseil des ministres renvoie aux conclusions de l'avocat général Henrik Saugmandsgaard.

D'après les parties requérantes, la doctrine citée par le Conseil des ministres constate exclusivement que la Cour de justice de l'Union européenne ne s'est pas prononcée sur la question de savoir quelle garantie a un caractère contraignant et qu'en conséquence l'ensemble des garanties ont un caractère cumulatif.

A.17. Dans son mémoire en réplique, le Conseil des ministres renvoie à l'argumentation qu'il a développée dans son mémoire en ce qui concerne la deuxième branche du premier moyen dans l'affaire n° 6601.

En ce qui concerne l'accès aux données conservées

A.18.1. Le troisième moyen dans l'affaire n° 6599 est pris 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, avec l'article 17 du Pacte international relatif aux droits civils et politiques, avec les principes généraux de sécurité juridique, de proportionnalité et de droit à l'autodétermination en matière d'information ainsi qu'avec l'article 5, § 4, du Traité de l'Union européenne. Le moyen concerne l'accès aux données conservées.

A.18.2. Dans la première branche du moyen, les parties requérantes dans l'affaire n° 6599 font grief à la loi attaquée de permettre à six autorités différentes d'accéder aux données conservées et non de limiter cet accès strictement aux autorités qui sont impliquées dans la lutte contre la criminalité, à tout le moins contre la criminalité grave. Les parties requérantes contestent en particulier qu'un accès puisse être accordé aux services d'urgence, à l'officier de police judiciaire de la cellule des personnes disparues et au service de médiation pour les télécommunications.

A.18.3. Dans la deuxième branche du moyen, les parties requérantes dans l'affaire n° 6599 reprochent à la loi attaquée de permettre aux autorités judiciaires d'accéder aux données conservées en vue de la recherche, de l'instruction et de la poursuite d'infractions pour l'exécution de mesures visées aux articles 46*bis* et 88*bis* du

Code d'instruction criminelle, dans les conditions visées par l'article concerné, sans que cet accès soit limité à la criminalité grave énumérée à l'article 90*ter* du même Code.

A.18.4. La troisième branche du moyen critique l'accès aux données conservées par les services de renseignement. D'après les parties requérantes dans l'affaire n° 6599, le terrain d'action des services de renseignement et de sécurité a été défini de façon trop large. La conservation de données qui est instaurée par la loi se rapporte aux données de communication de tous les citoyens et celles-ci peuvent être réclamées suivant le caractère de la menace potentielle pour une période de six, de neuf ou de douze mois antérieure à la décision d'accès. La méthode de collecte de données d'identification et de données de communication est respectivement une méthode ordinaire et une méthode spécifique pour les services de renseignement et de sécurité qui peut être opérée sur simple demande du dirigeant du service et aussi de son délégué pour la méthode ordinaire et ce sans l'autorisation de la commission des magistrats.

La combinaison de la loi sur la conservation des données et de la loi sur les services de renseignements et de sécurité implique que sur simple demande du dirigeant du service, avec un effet rétroactif de douze mois, toutes les données téléphoniques et internet peuvent être demandées pour toute personne répondant à l'une des qualifications des compétences de la Sûreté de l'Etat. La loi attaquée peut donc aboutir à des abus de pouvoir au détriment d'individus ou d'organisations critiques à l'égard du gouvernement ou du système politique. La liberté de la presse serait également mise en péril par le fait que les services de renseignement et de sécurité peuvent demander toutes les communications téléphoniques et internet des journalistes d'investigation qui apparaissent sur le radar des services de sécurité. La loi attaquée pourrait également susciter ou renforcer l'autocensure chez le citoyen qui a le vague sentiment d'être surveillé, ce qui peut avoir un impact sur l'exercice de sa liberté d'opinion et d'information et constituer de la sorte une ingérence par rapport à l'article 11 de la Charte des droits fondamentaux de l'Union européenne.

A.18.5. Dans la cinquième branche du moyen, il est reproché à l'article 126, § 2, alinéas 2 et 3, de la loi du 13 juin 2005, inséré par l'article 4 de la loi attaquée, de prévoir que les fournisseurs et opérateurs font en sorte que les données conservées soient accessibles de manière illimitée et que toute autre information nécessaire concernant ces données puisse être transmise sans délai et aux seules autorités compétentes, de sorte qu'il n'y a aucune description précise des circonstances et des conditions relatives à l'octroi d'un accès. Il manquerait aussi la stipulation d'une quelconque condition matérielle ou procédurale, les fournisseurs étant simplement obligés de répondre favorablement à toute demande des six autorités désignées. Or, dans son arrêt *Tele2 Sverige AB*, la Cour de justice de l'Union européenne aurait affirmé que la réglementation nationale doit prévoir des garanties appropriées, c'est-à-dire des règles claires et précises indiquant en quelles circonstances et sous quelles conditions les fournisseurs doivent accorder aux autorités nationales compétentes l'accès aux données. Le même arrêt préciserait également qu'un accès ne saurait en principe être accordé qu'aux données de personnes soupçonnées de projeter, de commettre ou d'avoir commis une infraction grave ou encore d'être impliquées d'une manière ou d'une autre dans une telle infraction. L'arrêt affirmerait encore qu'il est essentiel que l'accès soit subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante, qui décide, à la suite d'une demande motivée des autorités. Or, il est constaté que, dans la loi attaquée, aucune règle de procédure n'a été élaborée, et qu'aucune autorité n'a été désignée ni au sein des fournisseurs ni en dehors de ceux-ci qui puisse apprécier la demande de réception de données. Ni la cellule de coordination ni le préposé ni le responsable du traitement n'ont la moindre compétence à cet égard.

Il est encore souligné qu'aucun des deux n'a une quelconque fonction de contrôle voire une fonction préalable de contrôle de l'octroi de l'accès aux six autorités citées. Aucun des deux ne répond non plus à la notion d'instance judiciaire ou d'autorité administrative ou d'autorité administrative indépendante.

Les parties requérantes ajoutent que pour autant que l'Institut puisse être considéré comme une autorité administrative indépendante, il n'est pas compétent pour exercer un contrôle préalable de l'octroi d'un accès par les opérateurs et fournisseurs aux autorités compétentes. Les opérateurs et les fournisseurs ne sont pas soumis à l'institut.

A.18.6. Dans une cinquième (lire : sixième) branche du moyen, il est reproché à la loi attaquée de ne prévoir aucune obligation d'avertir des personnes qu'un accès à leurs données privées a été accordé. La loi ne prévoit pas non plus un droit de recours spécifique en cas de violation de ce droit.

A.19. Dans son mémoire, le Conseil des ministres renvoie à l'article 15, alinéa 1er, de la directive 2002/58/CE. Il relève que la Cour de justice de l'Union européenne, dans son arrêt du 21 décembre 2016, aussi bien dans l'affaire C-203/15 que dans l'affaire C-698/15, a seulement examiné la portée de cette disposition en ce qui concerne la conservation des données et leur accès pour l'information, l'enquête et la poursuite de la criminalité grave. La Cour de justice ne s'est en revanche pas prononcée sur la conservation des données et leur accès en ce qui concerne d'autres objectifs qui sont énumérés dans cette disposition. Le Conseil des ministres renvoie également à l'arrêt *Digital Rights Ireland* de la Cour de justice de l'Union européenne du 8 avril 2014 relatif à la directive 2006/24/CE qui s'est prononcé sur la conservation des données et leur accès uniquement en ce qui concerne l'information, l'enquête et la poursuite de la criminalité grave. Il ne pourrait ainsi être déduit de l'arrêt de la Cour de justice de l'Union européenne du 21 décembre 2016 que les autorités ne peuvent accéder aux données conservées lorsqu'il s'agit de lutter contre la criminalité grave. La loi attaquée aurait en effet un champ d'application plus large.

D'après le Conseil des ministres, la loi attaquée est conforme à l'article 15, alinéa 1er, de la directive 2002/58/CE, y compris lorsqu'il s'agit de conserver des données et de les communiquer aux autorités compétentes pour l'examen, l'enquête et la poursuite d'autres formes de criminalité que la criminalité grave, lorsque la vie ou l'intégrité physique de personnes ou de biens est en danger, ou lorsqu'il est fait un emploi irrégulier des systèmes de communications électroniques. Le Conseil des ministres soutient que la section de législation du Conseil d'Etat, dans son avis relatif à l'avant-projet de loi, a appuyé ce point de vue.

A.20. Dans leur mémoire en réponse, les parties requérantes dans l'affaire n° 6599 soutiennent que si la Cour de justice de l'Union européenne, dans son arrêt du 21 décembre 2016, s'est exprimée à propos de l'article 15, alinéa 1er, de la directive 2002/58/CE en matière de criminalité grave, cela n'implique pas que les principes qu'elle a dégagés ne puissent également pas s'appliquer à la criminalité plus légère.

D'après les parties requérantes, par analogie à ce qu'a décidé la Cour de justice de l'Union européenne, la conservation et l'accès aux données en ce qui concerne les services de sécurité doivent être limités aux dangers les plus graves pour la sûreté de l'Etat. Les parties requérantes relèvent que l'arrêt *Tele2 Sverige AB* utilise le terme « risque sérieux pour la sécurité publique ». D'après les parties requérantes, la loi attaquée ne respecte pas ces critères « par le fait qu'elle vise des méthodes habituelles et spécifiques et que celles-ci concernent les atteintes moins sérieuses à la sûreté que des méthodes particulières ».

A.21. En ce qui concerne le contrôle préalable d'une autorité indépendante, les parties requérantes dans l'affaire n° 6599 soulignent une fois encore que l'intervention de la Commission BIM fondée sur l'article 18/3, § 6, constitue un contrôle de légalité *a posteriori*, de même que celui qui est opéré par le Comité permanent en application de l'article 43/2 de la loi organique des services de renseignement et de sécurité. Ces contrôles *a posteriori* ne justifient nullement qu'il ne soit pas répondu à l'exigence d'un contrôle préalable par une instance juridictionnelle ou une autorité administrative indépendante.

A.22.1. En réponse aux deuxième, troisième et quatrième branches du deuxième moyen dans l'affaire n° 6601, le Conseil des ministres rappelle que, dans son arrêt du 21 décembre 2016, la Cour de justice de l'Union européenne a jugé que le législateur national devait adopter des règles claires et strictes sur les circonstances dans lesquelles et les conditions auxquelles l'accès aux données conservées peut être autorisé.

A.22.2. Quant à la prétendue absence de contrôle juridictionnel, le Conseil des ministres soutient que dans le cadre d'une instruction pénale, un tel contrôle peut effectivement être réalisé par des instances judiciaires telles que le procureur du Roi ou le juge d'instruction de même que par la Commission BIM dans le cadre d'une enquête menée pour l'obtention de renseignements.

A.22.3. Le Conseil des ministres relève encore qu'il ressort de l'article 126, § 2, de la loi sur les communications électroniques que les données doivent être limitées aux recherches simples et doivent être accessibles depuis la Belgique, ce qui signifie que les fournisseurs et les opérateurs qui fournissent les services de communications en Belgique ne doivent délivrer les données qu'à l'égard des demandes formulées par les autorités belges sur le territoire belge sans qu'elles doivent envoyer une commission rogatoire.

A.22.4. Quant au fait que d'autres autorités que les autorités judiciaires peuvent avoir accès aux données conservées, le Conseil des ministres renvoie à l'avis du Conseil d'Etat sur ce sujet.

A.22.5. Le Conseil des ministres conteste ensuite le point de vue des parties requérantes selon lequel la loi permettrait un accès aux données conservées sans conditions matérielles ou procédurales. Il cite les articles 9, 13 et 14 de la loi attaquée pour justifier sa position. Il renvoie également à l'article 126, § 2, alinéa 1er, 4°, 5° et 6°, de la loi sur les communications électroniques. Il ressortirait également de l'exposé des motifs de la loi que le législateur a établi des règles claires et strictes sur les circonstances et les conditions dans lesquelles l'accès aux données conservées peut être autorisé.

A.22.6. En ce qui concerne l'absence prétendue de contrôle juridictionnel, le Conseil des ministres renvoie encore à l'article 126, § 1er, alinéa 1er, de la loi sur les communications électroniques tel qu'il a été inséré par l'article 4 de la loi attaquée et insiste sur le fait que la loi sur la protection de la vie privée du 8 décembre 1992 est une loi générale qui est donc applicable également à la conservation des données à caractère personnel ainsi qu'à leur accès dans le cadre de la loi attaquée. Ce point de vue serait expressément confirmé par l'exposé des motifs de la loi attaquée. Les personnes concernées disposent donc de toutes les garanties qui sont prévues par l'article 9 de la loi du 8 décembre 1992 précitée.

A.23.1. Dans leur mémoire en réponse, les parties requérantes dans l'affaire 6601 indiquent, en ce qui concerne la deuxième branche du moyen, qu'elles ne contestent pas qu'en application de l'article 88*bis* du Code d'instruction criminelle, tel que modifié par l'article 9 de la loi attaquée, l'accès aux données conservées est soumis à une ordonnance du juge d'instruction, de sorte qu'il existe bien une instance juridictionnelle qui protège l'accès à ces données. En revanche, le procureur du Roi ne constitue pas une instance juridictionnelle ou une autorité administrative indépendante.

A.23.2. Quant à l'accès aux données conservées par les services de renseignement et de sécurité, les parties requérantes ont fait remarquer dans leur recours en annulation que cet accès relève des méthodes spécifiques employées par ces services pour rassembler les données. L'accès aux données n'est nullement soumis à un avis préalable de la Commission BIM. L'avis de cette Commission est en effet limité à un contrôle de légalité postérieur opéré sur la base de l'article 18/3, § 6, de la loi du 30 novembre 1998.

A.23.3. En ce qui concerne la troisième branche du moyen, les parties requérantes font valoir que le Conseil des ministres ne conteste rien de ce qui est critiqué dans la requête à propos de l'accès aux données et des conditions qui sont prescrites par la loi pour cet accès.

Les parties requérantes relèvent que 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 ne règle pas les conditions matérielles et procédurales pour l'accès aux données conservées par les autorités visées par la loi autres que les services de renseignement et de sécurité. Le principe de légalité exclut en tout état de cause que ces règles soient fixées par un arrêté royal. En outre, cet arrêté royal renvoie à la loi du 30 novembre 1998 telle qu'elle a été modifiée par la loi attaquée.

Quant aux garanties qui sont invoquées par le Conseil des ministres lorsqu'il renvoie à l'exposé des motifs de la loi attaquée, aucune de ces garanties ne ferait obstacle au constat que la loi attaquée ne prévoit pas de conditions matérielles et procédurales pour l'accès aux données conservées.

A.23.4. En ce qui concerne la quatrième branche du moyen, les parties requérantes font valoir que l'accès aux données conservées sur la base de la loi attaquée relève du traitement des données à caractère personnel au sens de l'article 3, §§ 4 et 5, de la loi du 8 décembre 1992. Selon ces dispositions, les personnes concernées ne bénéficient pas des droits consacrés par les articles 9 et suivants de la même loi, en particulier le droit à l'information et le droit à la rectification de toute donnée à caractère personnel inexacte. Les personnes à l'égard desquelles des données conservées ont été fournies disposent seulement, en vertu de l'article 13 de la loi du 8 décembre 1992, d'un accès indirect aux données dans la mesure où la Commission de la protection de la vie privée exerce au nom de l'intéressé les droits consacrés par les articles 10 et 12 de la loi du 8 décembre 1992. Ni cette loi ni son arrêté d'exécution du 13 février 2001 ne prévoient toutefois à l'égard des autorités qui ont eu un

accès aux données conservées en vertu de la loi attaquée une obligation d'information ou un contrôle juridictionnel de nature à vérifier la régularité en fait ou en droit de cet accès.

A l'argument du Conseil des ministres selon lequel les personnes concernées par la fourniture de données conservées disposeraient d'un droit de recours, les parties requérantes renvoient à l'arrêt de la Cour n° 108/2016, du 14 juillet 2016. Elles soulignent que ce droit de recours suppose que les personnes concernées aient un accès aux données conservées afin que ce droit de recours soit efficace et effectif. Dès lors que les autorités concernées n'ont pas d'obligation d'information, ce droit de recours ne peut revêtir ces deux caractéristiques.

A.23.5. En ce qui concerne la cinquième branche du moyen, les parties requérantes renvoient aux arguments qu'elles ont développés dans le cadre du premier moyen, troisième branche, de leur requête.

A.24.1. Dans son mémoire en réplique, le Conseil des ministres soutient que le procureur du Roi est bien une instance juridictionnelle au sens de la jurisprudence de la Cour de justice de l'Union européenne. Il renvoie à l'article 151, § 1er, alinéa 1er, dernière phrase, de la Constitution pour justifier que le ministère public constitue bien une entité indépendante lorsqu'il exerce ses compétences d'enquête dans le cadre du Code d'instruction criminelle et offre la garantie que l'exercice de ses compétences ne porte pas atteinte de manière déraisonnable au droit à la protection de la vie privée.

Le Conseil des ministres insiste également sur le contrôle qui est exercé par la Commission BIM et le Comité I. Il ajoute, en ce qui concerne la troisième branche du moyen, que d'après la jurisprudence de la Cour, le droit au respect de la vie privée tel que consacré par l'article 22 de la Constitution admet des ingérences de l'autorité dans les cas et conditions prévus par la loi. Il est soutenu qu'en l'espèce, la loi règle effectivement les éléments essentiels des conditions matérielles et procédurales pour l'accès aux communications électroniques et délègue au Roi l'exécution des règles principales fixées par la loi.

A.24.2. Quant à la quatrième branche du moyen, le Conseil des ministres renvoie aux arguments qu'il a développés dans son mémoire et répète que les personnes concernées bénéficient des droits consacrés par la loi relative à la protection de la vie privée du 8 décembre 1992.

En ce qui concerne la conservation des données des médecins, des avocats et des journalistes

A.25.1. Dans la troisième branche du premier moyen, les parties requérantes dans l'affaire n° 6601 soutiennent à titre subsidiaire, au cas où la Cour déclarerait les deux premières branches du moyen non fondées, que l'obligation de conservation générale et indifférenciée des données viole les normes de référence invoquées au moyen en ce que la loi impose également la conservation de données de personnes qui bénéficient du secret professionnel et de personnes ayant par ailleurs une obligation de confidentialité, ainsi que de données de communication qui constituent des données à caractère personnel sensibles. Les parties requérantes reprochent à la loi attaquée d'établir uniquement une distinction limitée et insuffisante au niveau de l'accès aux données conservées pour autant qu'il s'agisse de données d'un avocat, d'un médecin ou d'un journaliste. Elles indiquent que l'article 458 du Code pénal a un champ d'application plus étendu que celui des personnes qui exercent ces trois professions. Elles ajoutent que certaines personnes, autorités et organisations ne sont pas soumises au secret professionnel tandis que la communication avec celles-ci doit néanmoins pouvoir bénéficier d'une certaine confidentialité en application 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.

A.25.2. Les parties requérantes soutiennent encore que la conservation de données qui constituent des données à caractère personnel sensibles au sens de la loi du 8 décembre 1992 viole en outre le principe d'égalité et de non-discrimination tel qu'il est garanti par les articles 10, 11 et 22 de la Constitution. En effet, tandis que la loi précitée prévoit des conditions spéciales en vue du traitement des données à caractère personnel sensibles, ces données, qui constituent également des données d'identification, de connexion et de localisation et des données de communication personnelles au sens de l'article 126, § 3, de la loi du 13 juin 2005 tel qu'il a été inséré par la loi attaquée, ne sont pas soumises à ces conditions particulières en matière de traitement, ce qui créerait une différence de traitement qui ne serait pas raisonnablement et objectivement justifiée.

A.25.3. Les mêmes parties requérantes adressent une critique semblable à l'égard de la loi dans la cinquième branche du deuxième moyen. Elles exposent que les données à caractère personnel sensibles sont celles qui font apparaître l'origine raciale ou ethnique, les conceptions politiques, la conviction religieuse ou philosophique ou l'appartenance à un syndicat, qui concernent la vie sexuelle ou la santé et les données à caractère personnel concernant des litiges soumis au cours et tribunaux ainsi qu'aux juridictions administratives en matière d'inculpation, de poursuite ou de condamnation concernant des infractions ou en ce qui concerne des sanctions administratives ou des mesures de sûreté. Elles relèvent que la loi attaquée ainsi que l'article 46*bis* du Code d'instruction criminelle prévoient, grâce aux autorités judiciaires et aux services de renseignement et de sécurité, des garanties générales relatives à l'accès à toutes les données conservées, en particulier en ce qui concerne une obligation de motivation faisant apparaître le caractère proportionné et la subsidiarité de l'accès. La loi attaquée prévoit, pour le surplus, des garanties spéciales exclusivement en ce qui concerne l'accès aux données conservées d'un avocat, d'un médecin ou d'un journaliste. Le journaliste bénéficie également de la protection offerte par la loi du 7 avril 2005 relative à la protection des sources journalistiques. La loi attaquée ne prévoit toutefois pas des garanties spéciales telle que par exemple une obligation renforcée de motivation si l'accès porte sur les données d'autres personnes bénéficiant du secret professionnel ou qui ont une obligation de confidentialité ou sur des données de communication qui constituent des données à caractère personnel sensibles.

A.26. Le quatrième moyen dans l'affaire n° 6599 est pris de la violation des articles 10, 11, 12, 15, 22 et 29 de la Constitution pris isolément ou en combinaison avec les articles 5, 6, 8, 9, 10, 11, 14, 15, 17 et 18 de la Convention européenne des droits de l'homme, avec les articles 7, 8, 11, 47 et 52 de la Charte des droits fondamentaux de l'Union européenne, avec l'article 17 du Pacte international relatif aux droits civils et politiques, avec les principes généraux de sécurité juridique, de proportionnalité et d'autodétermination en matière d'information, ainsi qu'avec l'article 5, paragraphe 4, du Traité de l'Union européenne.

Les parties requérantes exposent que le secret professionnel des avocats a pour fondement la nécessaire relation de confiance entre l'avocat et son client. Ce droit est protégé sous deux angles : d'une part, à partir de l'article 6 de la Convention européenne des droits de l'homme qui garantit le droit à un procès équitable, d'autre part, à partir de l'article 8 de la même Convention qui rend le droit au respect de la vie privée également applicable à des activités professionnelles. Il est reproché à la loi attaquée de traiter les avocats, les médecins et les journalistes de la même manière que tous les autres intéressés, du moins en ce qui concerne la conservation des métadonnées, sans qu'il soit tenu compte du statut particulier et du secret professionnel de ces catégories. Or, les données qui doivent être conservées par un avocat, un médecin ou un journaliste sont confidentielles. Le manque de distinction dans la loi touche également le justiciable qui ne peut plus compter sur le fait de pouvoir consulter un avocat en toute confiance. Il en est de même pour les patients qui consultent des médecins et pour les sources qui fournissent d'importantes informations aux journalistes.

Les parties requérantes constatent que la loi attaquée organise un certain encadrement en ce qui concerne l'accès aux données conservées d'avocats, de médecins et de journalistes mais pour ce qui concerne la conservation proprement dite des métadonnées, aucune distinction n'est opérée. Les parties requérantes ajoutent que le délai général de conservation de douze mois est en soi disproportionné. Quant au délai d'accès, la loi établit seulement une distinction en ce qui concerne la nature de l'infraction et la menace mais pas en ce qui concerne la nature des données conservées. De plus, la loi n'établit aucune distinction par rapport à la conservation de données entre, d'une part, des justiciables qui font l'objet de soupçons, d'enquêtes ou de poursuites et, d'autre part, des justiciables qui ne font nullement l'objet de telles mesures. La conservation généralisée de données, y compris pour des personnes qui n'ont aucun lien avec la criminalité, pas même en tant que personnes soupçonnées, violerait donc le principe de proportionnalité. Cette violation serait confirmée par les arrêts de la Cour de justice de l'Union européenne *Digital Rights Ireland* et *Tele2 Sverige AB* ainsi que par les conclusions de l'avocat général Pedro Cruz Villalón précédant l'arrêt *Digital Rights Ireland* de même que par l'arrêt de la Cour n° 84/2015, du 11 juin 2015.

A.27.1. Dans son mémoire le Conseil des ministres renvoie au point 105 de l'arrêt de la Cour de justice de l'Union européenne du 21 décembre 2016 ainsi qu'à l'arrêt de la Cour n° 84/2015. Il cite également plusieurs extraits de l'exposé des motifs de la loi attaquée pour démontrer que le législateur a examiné toutes les possibilités pour rencontrer la jurisprudence de la Cour de justice de l'Union européenne ainsi que celle de la Cour. A son estime, une différenciation sur le plan de l'application de l'obligation de conservation des données était impossible. En effet, le but légitime poursuivi par le législateur n'aurait pu être atteint. Le Conseil des ministres relève que pour se conformer à l'arrêt de la Cour, le législateur a choisi de renforcer la protection pour des appels déterminés au niveau de la réglementation en matière d'accès aux données conservées. Le législateur a également prévu des garanties en vue de protéger le secret professionnel des avocats, des médecins et le secret des sources des journalistes. Le Conseil des ministres fait encore remarquer que la conservation des données et

leur accès n'ont pas de rapport avec le contenu de ces données. Il en ressort que la loi attaquée ne va pas au-delà de ce qui est strictement nécessaire et justifié dans une société démocratique.

A.27.2. Quant à l'obligation de conservation des données dans le chef des personnes qui ont une obligation de confidentialité ou à l'égard de données de communication qui constituent des données à caractère personnel sensibles, le Conseil des ministres relève qu'il ressort de la jurisprudence de la Cour ainsi que de celle de la Cour de justice de l'Union européenne que ces deux juridictions ont émis une réserve uniquement à l'égard de la conservation des données pour des personnes qui sont soumises au secret professionnel.

A.27.3. Le Conseil des ministres relève encore que la loi du 8 décembre 1992 est une loi générale qui s'applique à la conservation des données à caractère personnel, également dans le cadre de la loi attaquée. Les parties requérantes resteraient en défaut de démontrer en quoi les règles spécifiques prévues aux articles 6, 7 et 8 de cette loi seraient donc exclues.

A.28.1. Dans leur mémoire en réponse, les parties requérantes dans l'affaire n° 6601 indiquent que c'est à tort que le Conseil des ministres soutient que la loi attaquée n'exclut pas l'application des articles 6, 7 et 8 de la loi du 8 décembre 1992. En effet, le nouvel article 126, §§ 1er et 3, de la loi du 13 juin 2005 oblige l'ensemble des fournisseurs et des opérateurs à conserver les données d'identification, de connexion, de localisation et les données de communication personnelles indépendamment du fait qu'il s'agit de données à caractère personnel sensibles. Ces dispositions ne dispensent dès lors pas les fournisseurs et les opérateurs de leur obligation de conservation, même lorsqu'il s'agit de données qui ont ce caractère. Les parties requérantes ajoutent que l'article 3, § 4, de la loi du 8 décembre 1992 exclut expressément de son champ d'application les données conservées par les services de renseignement et de sûreté de l'Etat. Les parties requérantes relèvent enfin que l'interdiction de traiter les données à caractère personnel consacrée par les articles 6, 7 et 8 de la loi du 8 décembre 1992 contient des dérogations au paragraphe 2 de ces dispositions. Parmi ces dérogations figurerait le traitement des données à caractère personnel visé par la loi attaquée.

A.28.2. Quant au fait que des garanties complémentaires seraient prévues par la loi attaquée, les parties requérantes indiquent que ces garanties ne concernent pas les personnes soumises au secret professionnel autres que les avocats, les médecins et les journalistes.

A.28.3. A l'argument selon lequel l'obligation de conservation des données concerne l'accès à ces données et n'a pas de rapport avec leur contenu, les parties requérantes répondent que par son arrêt n° 108/2016, du 14 juillet 2016, la Cour s'est prononcée sur le droit à la protection de la vie privée. Le principe de proportionnalité impliquerait une obligation positive plus stricte lorsqu'il s'agit de données à caractère personnel sensibles. Il s'agirait, en effet, de prendre des mesures qui assurent le respect des données de communication entre les citoyens et les personnes qui bénéficient du secret professionnel ainsi qu'entre les citoyens et les personnes dans le chef desquelles une obligation de confiance existe.

Le Conseil des ministres ne conteste pas que par la conservation des données de communication avec les personnes, les autorités et les organisations, un profil des personnes concernées peut être établi. La loi du 1er septembre 2016, qui permet aussi de rassembler des données relatives aux consommateurs finaux de cartes prépayées, permet également l'établissement de tels profils, de sorte que l'usage de services de communication électronique et de la conservation des données peut permettre de tirer des conclusions en rapport avec les opinions politiques, les convictions religieuses et philosophiques des personnes concernées. Il serait de la sorte porté atteinte à la liberté d'opinion de ces personnes.

A.28.4. Les parties requérantes dans l'affaire n° 6601 ajoutent enfin que la loi attaquée, lue en combinaison avec la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, permet que soient communiquées les données conservées, avec le risque d'établissement de profils de personnalité et les abus que peuvent commettre ces services.

A.29. Dans leur mémoire en réponse, les parties requérantes dans l'affaire n° 6599 renvoient, en ce qui concerne le quatrième moyen, aux arguments qu'elles ont développés dans leur requête en annulation ainsi qu'au mémoire en réponse de l'Ordre des barreaux francophones et germanophone introduit dans l'affaire n° 6590.

A.30. Dans son mémoire en réplique, le Conseil des ministres renvoie à l'argumentation qu'il a développée dans son mémoire. Il rappelle que d'après la jurisprudence de la Cour de justice de l'Union européenne et celle

de la Cour, les données des personnes qui sont soumises à une obligation de confiance *sensu lato* ne doivent pas répondre à des conditions de conservation aussi strictes que celles qui tombent sous le régime du secret professionnel. Le Conseil des ministres répète que les obligations prescrites par les articles 6, 7 et 8 de la loi du 8 décembre 1992 sont entièrement applicables aux données à caractère personnel visées par la loi attaquée, dans la mesure où la loi du 8 décembre 1992 a un caractère général, tandis que la loi attaquée comporte des dispositions spécifiques.

En ce qui concerne le délai de conservation des données

A.31. Dans la troisième branche du deuxième moyen, les parties requérantes dans l'affaire n° 6599 reprochent au législateur de ne pas avoir justifié de façon concluante les raisons pour lesquelles les données doivent être conservées pendant douze mois et, en principe, pendant une période beaucoup plus longue en ce qui concerne les données d'identification de l'utilisateur ou de l'abonné et pour ce qui concerne les moyens de communication dans la mesure où ce délai s'étend jusqu'à douze mois après qu'une communication est intervenue pour la dernière fois à l'aide du service utilisé.

Les parties requérantes relèvent que d'autres pays européens appliquent des délais de conservation plus courts. Elles renvoient à un arrêt de la Cour constitutionnelle allemande qui a annulé la loi allemande sur la conservation des données ainsi qu'à l'arrêt de la Cour de justice de l'Union européenne *Digital Rights Ireland*.

Les parties requérantes relèvent également que le Conseil d'Etat s'est prononcé en faveur d'un délai général de conservation plus court moyennant la possibilité de faire activer par le Roi un délai de conservation plus long en cas de menace potentielle.

A.32.1. Les parties requérantes dans l'affaire n° 6601 contestent également la longueur du délai de conservation des données dans le troisième moyen. Celui-ci est pris de la violation de l'article 8 de la Convention européenne des droits de l'homme, des articles 7, 8, 11.4 et 52, paragraphe 1er, de la Charte des droits fondamentaux de l'Union européenne, des articles 10, 11, 19 et 22 de la Constitution, de l'article 2, a), de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, ainsi que des articles 1, 2, 3, 5, 6, 9 et 15 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).

A.32.2. Dans la première branche du moyen, les parties requérantes reprochent à la loi attaquée de prévoir pour les catégories respectives de données conservées un même délai de conservation, ce qui constitue un traitement égal de catégories inégales de données conservées qui ne serait pas raisonnablement justifié et serait, partant, discriminatoire. Les parties requérantes citent les considérants 60 à 68 de l'arrêt de la Cour de justice de l'Union européenne du 8 avril 2014 qui concernent ce délai de conservation. Il découlerait de cette jurisprudence que la loi attaquée ne serait conforme aux normes de référence invoquées au moyen que pour autant que le délai de conservation soit différencié selon les catégories de données, selon son utilité pour le but poursuivi ou selon les personnes concernées et pour autant qu'il soit limité à ce qui est strictement nécessaire.

Les parties requérantes font remarquer que l'article 126, § 3, de la loi du 13 juin 2005, tel qu'il a été inséré par l'article 4 de la loi attaquée, fait une distinction entre les données d'identification, de connexion, de localisation et les données de communication personnelles, ces données étant soumises au même délai de conservation de douze mois. La loi prévoit uniquement une différenciation pour ce qui concerne l'accès aux données, et le délai d'accès est déterminé en fonction de la nature des données, en fonction de la gravité de l'infraction dans le cadre de l'accès par les autorités judiciaires et en fonction de la nature de la menace potentielle dans le cadre de l'accès pour les services de renseignement et de sécurité. La loi attaquée ne différencie donc pas le délai de conservation selon les catégories de données, selon l'utilité pour le but poursuivi ou selon les personnes concernées et ne se limite pas à ce qui est strictement nécessaire. Le législateur n'a pas tenu compte sur ce point de la remarque qui a été formulée par l'avis de la section de législation du Conseil d'Etat. Il est soutenu que la loi attaquée va en tout cas au-delà de ce qui est strictement nécessaire, raisonnable et proportionné pour sauvegarder la sécurité nationale, la défense et la sécurité publique ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisation non autorisée du système de communications électroniques comme le prévoit l'article 13, paragraphe 1er, de la directive 94/46/CE.

A.32.3. Dans la deuxième branche du moyen, il est reproché à la loi attaquée de ne pas obliger l'autorité qui a eu accès à des données à détruire ces données si elles ne présentent aucun lien avec le but pour lequel elles ont été recueillies. La loi attaquée n'impose la destruction irrévocable des données conservées qu'aux fournisseurs et opérateurs à l'issue du délai de conservation fixé à l'article 126, § 3, de la loi du 13 juin 2005, tel qu'il a été inséré par l'article 4 de la loi attaquée. Il n'y a en revanche aucune obligation de destruction irrévocable des données conservées pour les autorités qui ont accès aux données conservées dès qu'elles ne sont plus strictement nécessaires à la lutte contre la criminalité grave.

Combiné avec le nouvel article 21 de la loi du 30 novembre 1998 ainsi qu'avec l'arrêté royal du 3 juillet 2016 portant exécution de cet article 21, la loi attaquée a pour effet que les données peuvent être conservées directement, indirectement ou après un traitement dérivé même pour une très longue période, même si ces données ne sont pas strictement nécessaires en vue de la lutte contre la criminalité grave.

A.32.4. Les parties requérantes ajoutent dans la troisième branche du moyen qu'en prévoyant une exception à l'obligation de destruction incombant aux fournisseurs et opérateurs pour les données prévues aux articles 122 et 123 de la loi du 13 juin 2005, il est possible d'avoir indirectement accès aux données conservées après l'expiration des délais de conservation et d'accès prévus par la loi attaquée, de sorte que cette exception à cette obligation de destruction constitue une ingérence dans le droit à la protection de la vie privée qui n'est pas strictement nécessaire, raisonnable et proportionnée dans une société démocratique.

A.33.1. Dans son mémoire, le Conseil des ministres renvoie aux considérants 63 et 64 de l'arrêt de la Cour de justice de l'Union européenne du 8 avril 2014 ainsi qu'à l'arrêt de la Cour n° 84/2015 du 11 juin 2015. Il renvoie également à l'exposé des motifs de la loi attaquée dont il ressortirait que le législateur a examiné toutes les possibilités pour rencontrer la jurisprudence de la Cour ainsi que celle de la Cour de justice de l'Union européenne. D'après le Conseil des ministres, une différence de traitement sur le plan du délai de conservation des données serait apparue impossible après un examen approfondi de cette question. Il est apparu qu'un délai de douze mois est nécessaire pour lutter contre les infractions terroristes. Un délai de douze mois a d'ailleurs été fixé par l'article 88*bis*, § 1er, du Code d'instruction criminelle consacré aux enquêtes pénales en matière de terrorisme de même que par l'article 18/8, § 2, 3°, de la loi du 30 novembre 1998 « organique des services de renseignement et de sécurité » en ce qui concerne les menaces potentielles en matière de terrorisme.

A.33.2. Le Conseil des ministres relève encore que, d'après l'article 126, § 6, de la loi sur les communications électroniques, les ministres compétents doivent remettre dans les deux ans qui suivent l'entrée en vigueur de l'article 126, § 3, alinéa 4, de la même loi, un rapport d'évaluation à la Chambre des représentants sur l'application de cet article afin de déterminer si des aménagements sont nécessaires, en particulier en ce qui concerne la conservation des données et le délai de conservation. Il est encore indiqué que pour rencontrer l'arrêt de la Cour, le législateur a choisi de prévoir une différenciation sur le plan de l'accès aux données compte tenu de la nature de ces données, du sérieux des infractions et de la nature de la menace potentielle lorsque ces données sont rassemblées dans le cadre d'une enquête judiciaire ou dans le cadre d'une enquête relative à la sûreté de l'Etat. D'autres délais particuliers sont prévus à l'article 126, § 2, 4° et 5°. Il est aussi prévu que des délais pour l'accès aux données peuvent encore être adaptés dans l'avenir. Le Conseil des ministres en conclut que le délai de douze mois pour la conservation de données ne va pas au-delà de ce qui est strictement nécessaire pour atteindre l'objectif poursuivi par le législateur.

A.34. Dans leur mémoire en réponse, les parties requérantes dans l'affaire n° 6599 relèvent que le délai de douze mois a été jugé disproportionné par la doctrine. Il est également indiqué que, dans les statistiques de l'IBPT, il apparaît que la plupart des demandes interviennent dans une période de trois mois maximum, si bien que la période de douze mois n'est pas proportionnée. Le Conseil d'Etat a également souligné que le délai effectif de conservation des données dans le cadre des articles 46*bis* et 88*bis* du Code d'instruction criminelle peut être beaucoup plus long que douze mois dans la pratique.

D'après les parties requérantes, contrairement à ce que laissait entendre le Conseil des ministres, le Conseil d'Etat a émis des objections en ce qui concerne la réglementation, également sur le plan du délai de conservation des données. Quant au fait que des délais différents sont fixés pour l'accès aux données, l'existence d'une gradation à ce niveau n'implique pas que la durée de la conservation des données soit en proportion avec l'objectif poursuivi par le législateur.

A.35.1. Dans leur mémoire en réponse, les parties requérantes dans l'affaire n° 6601 soulignent qu'à plusieurs reprises l'exposé des motifs de la loi attaquée a reconnu que l'absence de différence de traitement en ce qui concerne le délai de conservation des données n'était pas conforme à la jurisprudence de la Cour et de la Cour de justice de l'Union européenne. Il ressortirait également de l'avis du Conseil d'Etat qu'aussi bien l'Allemagne que les Pays-Bas ont effectivement prévu un délai de conservation des données différencié. Il serait dès lors inexact d'affirmer que, d'un point de vue technique, il est impossible de différencier les délais de conservation des données.

Les parties requérantes contestent également l'argument du Conseil des ministres selon lequel le législateur n'a pas opté pour un délai général de conservation plus court avec possibilité pour le Roi d'allonger ce délai dans des circonstances de menace potentielle parce que certaines données ne seraient plus disponibles au moment de l'activation effective par le Roi de ce délai plus long, tandis que c'est précisément dans une situation de menace imminente qu'il est nécessaire de revenir en arrière durant la période la plus longue pour requérir des données.

Quant au fait qu'une évaluation périodique serait prévue à l'article 126, § 6, de la loi du 13 juin 2005, les parties requérantes indiquent qu'une telle évaluation ne modifie rien à l'inconstitutionnalité constatée et à l'incompatibilité de la réglementation avec le droit de l'Union européenne.

La circonstance que des délais différents sont fixés pour l'accès aux données ne permettrait pas de rencontrer les exigences posées de manière cumulative par la Cour de justice de l'Union européenne dans son arrêt du 8 avril 2014.

A.35.2. En ce qui concerne la deuxième branche du moyen, les parties requérantes dans l'affaire n° 6601 insistent sur le fait que l'article 126, § 4, de la loi du 13 juin 2005, tel qu'il a été inséré par l'article 4 de la loi attaquée, établit uniquement une obligation de destruction des données conservées à l'égard des fournisseurs et des opérateurs et non à l'égard de l'autorité qui a obtenu accès aux données conservées et qui les a traitées. Les parties requérantes ajoutent encore que la loi attaquée, lue en combinaison avec des réglementations sectorielles, a pour conséquence que les données conservées peuvent directement, indirectement ou après avoir été traitées, être conservées pour un délai très long alors que cela ne serait pas strictement nécessaire pour lutter contre la criminalité grave.

A.35.3. En ce qui concerne la troisième branche du moyen, les parties requérantes dans l'affaire n° 6601 soutiennent que ni les articles 46*bis* et 88*bis* du Code d'instruction criminelle, tels que modifiés par la loi attaquée, ni l'article 18/8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, modifié également par la loi attaquée, ne limitent l'accès aux données aux seules données conservées telles qu'elles sont visées par la loi attaquée. Une réglementation différenciée est prévue par ces dispositions. Elle concerne, en effet, d'autres données qui ne sont pas soumises au délai de conservation et d'accès fixé par la loi attaquée. Les données visées à l'article 88*bis*, § 1er, du Code d'instruction criminelle ainsi qu'à l'article 18/8, § 1er, de la loi du 30 novembre 1998 sont donc d'autres données que celles qui sont fixées par la loi attaquée et il peut seulement s'agir des données commerciales visées par les articles 122 et 123 de la loi du 13 juin 2005.

Les parties requérantes indiquent encore qu'en prévoyant une exception à l'obligation de détruire les données à l'égard des fournisseurs et des opérateurs pour ce qui concerne celles qui sont visées par les articles 122 et 123 de la loi du 13 juin 2005, il y a effectivement de manière indirecte un accès possible aux données conservées après le dépassement du délai de conservation et d'accès fixé par la loi attaquée.

A.36. Dans son mémoire en réplique, le Conseil des ministres note une fois encore que le fait qu'une différenciation sur le plan du délai de conservation des données était impossible n'est pas sans justification raisonnable. Aussi bien dans le cadre des enquêtes pénales que dans le cadre des services de renseignement, le délai concerné est apparu nécessaire. Il ressort des chiffres de l'IBPT que, pour l'année 2014, 15 % des demandes qui émanaient des autorités judiciaires et qui étaient fondées sur les articles 46*bis* et 88*bis* du Code d'instruction criminelle adressées à Base Company et Proximus avaient rapport à des données qui dataient de plus de neuf mois jusqu'à douze mois avant la demande. Il apparaît également des chiffres de la « Federal Computer Crime Unit » (FCCU) pour la période de 2012 à 2014 que 29 % des demandes avaient rapport aux données qui dataient de plus de neuf mois jusqu'à douze mois avant la demande. Les chiffres présentés par le Service général du renseignement et de la sécurité (SGRS) vont dans le même sens. Le Conseil des ministres présente un exemple concret pour justifier son argumentation. Il renvoie, pour le surplus, aux arguments qu'il a développés dans son mémoire.

En ce qui concerne la protection et la sécurité des données

A.37.1. Un deuxième moyen dans l'affaire n° 6599 est pris 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, avec l'article 17 du Pacte international relatif aux droits civils et politiques, avec les principes généraux de sécurité juridique, de proportionnalité et de droit à l'autodétermination en matière d'information, ainsi qu'avec l'article 5, paragraphe 4, du Traité sur l'Union européenne.

A.37.2. Dans la première branche du moyen, les parties requérantes critiquent le niveau de sécurisation et de protection des données conservées. Ainsi, si l'article 126, § 4, de la loi attaquée impose aux fournisseurs et aux opérateurs sept conditions en matière de protection, il ne garantit nullement qu'une autorité indépendante contrôle le respect dû au niveau de protection. L'intervention de l'Institut et celle de la Commission pour la protection de la vie privée qui sont mentionnées dans cette disposition portent uniquement sur la consultation par ces instances du journal, lequel est seulement prévu dans le cadre de la garantie mentionnée à l'article 126, § 4, alinéa 1er, 7°. Le journal doit ainsi assurer une traçabilité de l'exploitation des données conservées pour chaque demande d'obtention de ces données d'une autorité visée au paragraphe 2. En outre, l'intervention de ces instances n'a rien à voir avec les six autres conditions imposées par la loi pour garantir la protection des données conservées.

L'article 126/1, § 2, de la loi attaquée ne répondrait pas davantage à l'exigence de l'existence d'une autorité indépendante qui contrôle le respect dû au niveau de protection cité. Les parties requérantes ajoutent encore que les garanties prévues par la loi du 13 juin 2005 relative aux communications électroniques doivent être considérées comme d'anciennes garanties qui se rapportent à une conservation spécifique de données dans le cadre de lois antérieures à 2005 relatives à ce type de communication, à l'action publique et aux missions de renseignement. Ces garanties doivent dès lors être considérées en dehors de la loi attaquée.

A.37.3. Dans la deuxième branche du moyen, les parties requérantes critiquent le niveau de sécurité et de protection des données conservées par l'institution d'une cellule de coordination et d'un préposé spécifique à la protection des données à caractère personnel. Elles relèvent que les membres de la cellule de coordination, le responsable du traitement et le préposé à la protection des données à caractère personnel sont des membres du personnel ou sont à tout le moins désignés par ou constitués au sein de chaque opérateur ou fournisseur. Il s'agit donc de subordonnés qui sont dans une situation de dépendance vis-à-vis de l'opérateur ou du fournisseur. Or, un préposé ne peut être considéré comme une autorité administrative ou une instance judiciaire indépendante qui contrôle au préalable la protection et la sécurisation des données. Il en va de même pour la cellule de coordination qui est un organe purement exécutif composé de membres du personnel de l'opérateur ou du fournisseur. Enfin, les parties requérantes soulignent que l'article 126/1, § 2, alinéa 3, de la loi attaquée oblige les opérateurs et les fournisseurs à respecter l'article 114, § 2. Toutefois, l'intervention de l'Institut qui est prévue relève d'une simple possibilité et non d'une obligation à portée coercitive.

A.38.1. Le quatrième moyen dans l'affaire n° 6601 est pris de la violation de l'article 8 de la Convention européenne des droits de l'homme, des articles 7, 8, 11.4 et 52 de la Charte des droits fondamentaux de l'Union européenne, des articles 10, 11, 19 et 22 de la Constitution, de l'article 2 de la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ainsi que des articles 1, 2, 3, 5, 6, 9 et 15 de la directive 2002/58/CE 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.

D'après les parties requérantes, en n'excluant pas que lorsqu'ils déterminent le niveau de protection qu'ils offrent, les fournisseurs et opérateurs tiennent compte de considérations économiques et en ne prévoyant qu'une seule évaluation de la loi attaquée, en limitant cette évaluation aux dispositions relatives aux données à conserver et au délai de conservation et en ne prévoyant pas une évaluation périodique des dispositions relatives à la sécurisation et à la protection, la loi attaquée constitue une ingérence dans le droit à la protection de la vie privée qui, dans une société démocratique, n'est pas strictement nécessaire, raisonnable et proportionnée pour sauvegarder la sécurité nationale ou assurer la prévention, la recherche, la détection et la poursuite d'infractions

pénales ou d'utilisation non autorisée du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1er, de la directive 95/46/CE précitée.

A.38.2. Dans la deuxième branche du moyen, les parties requérantes dans l'affaire n° 6601 reprochent à la loi attaquée de n'établir aucune distinction s'agissant des données conservées qui sont communiquées aux services de renseignement et de sécurité étrangers, selon les catégories de données, selon leur utilité pour le but poursuivi (la menace potentielle) ou les personnes concernées. Cette communication ne serait dès lors pas limitée à ce qui est strictement nécessaire. Il est également reproché à la loi attaquée de ne pas entourer cette communication de garanties spéciales relatives à la protection et à la sécurisation des données.

A.39.1. Dans son mémoire, le Conseil des ministres soutient que les opérateurs et les fournisseurs ont l'obligation d'assurer le niveau de protection qui découle de la loi du 8 décembre 1992 et de son arrêté d'exécution du 13 février 2001. Le Conseil des ministres soutient également qu'à côté de cette obligation, la loi attaquée prévoit également un haut niveau de protection en ce qui concerne les données conservées par les fournisseurs et les opérateurs. Il s'agit, en effet, de prendre des mesures de protection technologiques au regard de ces données, de garantir la traçabilité des accès, d'annuler les données après l'écoulement du terme qui est fixé par la loi mais également de désigner un préposé pour la protection des données qui doit s'assurer du respect des différentes règles fixées par la loi. Sur le plan de la sécurisation des données, le Conseil des ministres insiste sur le fait que de nombreuses garanties seraient prévues par l'article 126 de la loi.

D'après le Conseil des ministres, c'est à tort que les parties requérantes dans l'affaire n° 6599 soutiennent que l'article 126, § 4, tel qu'inséré par la loi attaquée, impose sept conditions aux fournisseurs et opérateurs en matière de protection des données mais ne prévoit pas d'autorité indépendante qui contrôle leur respect. Selon le Conseil des ministres, l'IBPT de même que la Commission de la protection de la vie privée contrôlent la conservation des données par les fournisseurs et les opérateurs. L'article 145 de la loi sur les communications électroniques a également été modifié par la loi attaquée et prévoit une sanction pénale dans l'hypothèse d'un *hacking* externe et interne.

A.39.2. Le Conseil des ministres conteste également les arguments développés par les parties requérantes dans l'affaire n° 6601. A son estime, l'article 126, § 4, 2°, de la loi sur les communications électroniques rencontre les exigences émises par l'arrêt de la Cour de justice de l'Union européenne du 8 avril 2014 ainsi que par l'arrêt rendu par la même Cour le 21 décembre 2016.

Le Conseil des ministres insiste encore sur le fait que l'article 126, §§ 5 et 6, de la loi sur les communications électroniques prévoit une double évaluation de la loi.

A.40.1. Dans leur mémoire en réponse, les parties requérantes dans l'affaire n° 6599 estiment que le contrôle par une autorité indépendante est crucial pour assurer une sécurisation et une protection effectives de la conservation des données. Le législateur avait le choix entre créer une nouvelle autorité indépendante ou confier à des autorités existantes cette fonction de contrôle spécifique. En retenant la deuxième option, le législateur a mis en place un contrôle qui se révèle théorique compte tenu de la composition limitée de l'IBPT et de la Commission de la protection de la vie privée, des nombreuses tâches qu'ils ont à accomplir et des compétences qui leur sont reconnues. Par la loi attaquée, le contrôle exercé par l'IBPT ne constitue pas un contrôle effectif sur les providers et les opérateurs. Il y a lieu, en effet, de distinguer les garanties et le contrôle effectif. Les parties requérantes critiquent le fait que la loi n'ait pas confié une compétence de contrôle à une autorité indépendante disposant d'une compétence spécifique, dans le cadre de la conservation générale des données.

A.40.2. Les parties requérantes indiquent encore que les deux évaluations qu'invoque le Conseil des ministres ne constituent nullement une garantie complémentaire en ce qui concerne la protection et la sécurisation des données. Le rapport annuel est, en effet, un rapport uniquement statistique et est limité à l'article 90*decies* du Code d'instruction criminelle tandis que le rapport prévu par l'article 126, § 6, de la loi sur les communications électroniques doit servir de base à l'examen d'adaptations éventuellement nécessaires, indépendamment de la conservation des données et du délai de conservation. Les parties requérantes en concluent qu'il n'existe pas de garantie en ce qui concerne la protection et la sécurisation des données.

A.41.1. Dans leur mémoire en réponse, les parties requérantes dans l'affaire n° 6601 indiquent qu'il y a lieu d'interpréter l'article 126, § 4, 2°, de la loi du 13 juin 2005 de manière conforme à la Constitution, ce qui

exclut que les fournisseurs et les opérateurs puissent tenir compte de considérations économiques lorsqu'ils établissent le niveau de protection offert. Quant au fait que le Conseil des ministres renvoie à l'exposé des motifs pour indiquer qu'il existe une évaluation en vertu de l'article 126, § 6, de la loi du 13 juin 2005, cette explication serait contraire au texte de la loi lui-même qui prévoit une seule évaluation relative aux dispositions qui concernent la conservation des données et le délai de conservation, mais nullement en ce qui concerne la sécurisation et la protection des données conservées. Le Conseil des ministres reconnaîtrait d'ailleurs lui-même qu'il s'agit d'une seule évaluation qui n'est en conséquence pas périodique. Elle ne permet dès lors pas de tenir compte des évolutions technologiques et de l'état des affaires, tels que les développements que peuvent connaître l'existence ou l'application de programmes de surveillance, ou encore de l'évolution des bonnes pratiques.

A.41.2. Quant à l'atteinte au droit à la protection de la vie privée, les parties requérantes dans l'affaire n° 6601 répètent qu'une obligation de conservation générale et indifférenciée des données, de même que le traitement des données d'identification, de connexion et de localisation, ainsi que des données de communication personnelles, permettent d'établir un profil de personnalité pour chaque citoyen et de suivre son comportement. C'est également vrai pour les services de renseignement et de sécurité des Etats membres de l'Union européenne qui peuvent rassembler et traiter un grand nombre de données à caractère personnel dans le cadre des programmes de surveillance.

Les parties requérantes renvoient à une communication du 27 novembre 2013 faite par la Commission européenne au Parlement européen et au Conseil dans laquelle de nombreux abus ont été constatés dans le chef de citoyens européens et d'entreprises européennes et dans laquelle il a été remarqué que les personnes concernées n'avaient pas droit à une correction de ces données ni à un recours juridictionnel ou administratif.

A.42. Dans son mémoire en réplique, le Conseil des ministres renvoie aux arguments qu'il a développés dans son mémoire.

En ce qui concerne la conservation des données sur le territoire de l'Union européenne

A.43. La quatrième branche du deuxième moyen dans l'affaire n° 6599 renvoie aux conclusions de l'avocat général dans l'affaire *Tele2 Sverige AB* en ses points 238 à 241.

Les parties requérantes constatent qu'il n'existe actuellement aucune législation permettant à une autorité belge indépendante de contrôler dans d'autres pays de l'Union européenne les modalités de conservation des données stockées dans le cadre de l'obligation belge de conservation des données, par les fournisseurs et les opérateurs. La conservation des données ne répondrait pas, de ce fait, aux exigences de protection et de sécurisation.

A.44. Dans son mémoire, le Conseil des ministres répond qu'il ne peut être déduit des dispositions attaquées qu'il existerait une interdiction pour les services de renseignements et de sécurité belges de communiquer des données à des services de renseignements et de sécurité étrangers dans les conditions strictement définies par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

A.45. Dans leur mémoire en réponse, les parties requérantes dans l'affaire n° 6599 mettent en évidence qu'en réalité la quatrième branche de leur deuxième moyen vise le transfert de données vers d'autres Etats membres de l'Union européenne. Il est soutenu que la loi méconnaît l'existence de réglementations nationales qui imposent leurs propres obligations aux opérateurs et providers en ce qui concerne les services de sécurité et de renseignements.

A.46. Dans son mémoire en réplique, le Conseil des ministres renvoie aux arguments qu'il a développés dans son mémoire.

- B -

Quant à la loi attaquée et son contexte

B.1.1. Quatre recours sont introduits en vue de l'annulation de la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques.

B.1.2. Celle-ci dispose :

« CHAPITRE 1er. - *Disposition générale*

Article 1er. La présente loi règle une matière visée à l'article 74 de la Constitution.

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

Art. 2. A l'article 2 de la loi 13 juin 2005 relative aux communications électroniques, modifié en dernier lieu par la loi du 18 décembre 2015, et partiellement annulé par l'arrêt n° 84/2015 de la Cour constitutionnelle, 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) au lieu du 74°, annulé par l'arrêt n° 84/2015 de la Cour constitutionnelle, il est inséré 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. 3. L'article 125, § 2, de la même loi est abrogé.

Art. 4. Dans la même loi, à la place de l'article 126 annulé par l'arrêt n° 84/2015 de la Cour constitutionnelle, il est inséré un article 126 rédigé comme 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, en ce compris par internet, d'accès à l'Internet, de courrier électronique par Internet, les opérateurs fournissant des réseaux publics de communications électroniques ainsi que les opérateurs fournissant un de ces services, conservent les données

visées au paragraphe 3, qui sont générées ou traitées par eux dans le cadre de la fourniture des services de communications concernés.

Le présent article ne porte pas sur le contenu des communications.

L'obligation de conserver les données visées au paragraphe 3 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 ou traitées par les opérateurs 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. Seules les autorités suivantes peuvent obtenir, sur simple demande, des fournisseurs et opérateurs visés au paragraphe 1er, alinéa 1er, des données conservées en vertu du présent article, pour les finalités et selon les conditions énumérées ci-dessous :

1° les autorités judiciaires, en vue de la recherche, de l'instruction et de la poursuite d'infractions, pour l'exécution des mesures visées aux articles 46*bis* et 88*bis* du Code d'instruction criminelle et dans les conditions fixées par ces articles;

2° les services de renseignement et de sécurité, afin d'accomplir des missions de renseignement en ayant recours aux méthodes de recueil de données visées aux articles 16/2, 18/7 et 18/8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et dans les conditions fixées par cette loi;

3° tout officier de police judiciaire de l'Institut, en vue de la recherche, de l'instruction et de la poursuite d'infractions aux articles 114, 124 et au présent article;

4° les services d'urgence offrant de l'aide sur place, lorsque, à la suite d'un appel d'urgence, ils n'obtiennent pas du fournisseur ou de l'opérateur concerné les données d'identification de l'appelant à l'aide de la base de données visée à l'article 107, § 2, alinéa 3, ou obtiennent des données incomplètes ou incorrectes. Seules les données d'identification de l'appelant peuvent être demandées et au plus tard dans les 24 heures de l'appel;

5° l'officier de police judiciaire de la Cellule des personnes disparues de la Police Fédérale, dans le cadre de sa mission d'assistance à personne en danger, de recherche de personnes dont la disparition est inquiétante et lorsqu'il existe des présomptions ou indices sérieux que l'intégrité physique de la personne disparue se trouve en danger imminent. Seules les données visées au paragraphe 3, alinéas 1 et 2, relatives à la personne disparue et conservées au cours des 48 heures précédant la demande d'obtention des données peuvent être demandées à l'opérateur ou au fournisseur concerné par l'intermédiaire d'un service de police désigné par le Roi;

6° le Service de médiation pour les télécommunications, en vue de l'identification de la personne ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques, conformément aux conditions visées à l'article 43*bis*, § 3, 7°,

de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques. Seules les données d'identification peuvent être demandées.

Les fournisseurs et opérateurs visés au paragraphe 1er, alinéa 1er, font en sorte que les données visées au paragraphe 3, soient accessibles de manière illimitée à partir de la Belgique et que ces données et toute autre information nécessaire concernant ces données puissent être transmises sans délai et aux seules autorités visées au présent paragraphe.

Sans préjudice d'autres dispositions légales, les fournisseurs et opérateurs visés au paragraphe 1er, alinéa 1er, ne peuvent utiliser les données conservées en vertu du paragraphe 3 pour d'autres finalités.

§ 3. Les données visant à identifier l'utilisateur ou l'abonné et les moyens de communication, à l'exclusion des données spécifiquement prévues aux alinéas 2 et 3, sont conservées pendant douze mois à compter de la date à partir de laquelle une communication est possible pour la dernière fois à l'aide du service utilisé.

Les données relatives à l'accès et la connexion de l'équipement terminal au réseau et au service et à la localisation de cet équipement, y compris le point de terminaison du réseau, sont conservées pendant douze mois à partir de la date de la communication.

Les données de communication, à l'exclusion du contenu, en ce compris leur origine et leur destination, sont conservées pendant 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 à conserver par type de catégories visées aux alinéas 1 à 3 ainsi que les exigences auxquelles ces données doivent répondre.

§ 4. Pour la conservation des données visées au paragraphe 3, les fournisseurs et les opérateurs 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 pour répondre aux demandes des autorités visées au paragraphe 2 n'est effectué que par un ou plusieurs membres de la Cellule de coordination visée à l'article 126/1, § 1er;

4° conservent les données sur le territoire de l'Union européenne;

5° mettent en œuvre des mesures de protection technologique qui rendent les données conservées, dès leur enregistrement, illisibles et inutilisables par toute personne qui n'est pas autorisée à y avoir accès;

6° détruisent les données conservées de tout support lorsqu'est expiré le délai de conservation applicable à ces données fixé au paragraphe 3, sans préjudice des articles 122 et 123;

7° assurent une traçabilité de l'exploitation des données conservées pour chaque demande d'obtention de ces données d'une autorité visée au paragraphe 2.

La traçabilité visée à l'alinéa 1er, 7°, s'effectue à l'aide d'un journal. L'Institut et la Commission pour la protection de la vie privée peuvent consulter ce journal ou exiger une copie de tout ou partie de ce journal. L'Institut et la Commission pour la protection de la vie privée concluent un protocole de collaboration concernant la prise de connaissance et le contrôle du contenu du journal.

§ 5. 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 Chambre des représentants.

Ces statistiques comprennent notamment :

1° les cas dans lesquels des données 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, 1°, sont 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 du ministre et sur avis de l'Institut, les statistiques que les fournisseurs et opérateurs visés au paragraphe 1er, alinéa 1er, transmettent annuellement à l'Institut et celles que l'Institut transmet au ministre et au ministre de la Justice.

§ 6. Sans préjudice du rapport visé au paragraphe 5, alinéa 4, 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 3, alinéa 4, sur la mise en œuvre du présent

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. 5. Dans la même loi, un article 126/1 est inséré rédigé comme suit :

‘ Art. 126/1. § 1er. Au sein de chaque opérateur, et au sein de chaque fournisseur visé à l’article 126, § 1er, alinéa 1er, est constituée une Cellule de coordination, chargée de fournir aux autorités belges légalement habilitées, à leur demande, des données conservées en vertu des articles 122, 123 et 126, les données d’identification de l’appelant en vertu de l’article 107, § 2, alinéa 1er, ou les données qui peuvent être requises en vertu des articles 46*bis*, 88*bis* et 90*ter* du Code d’instruction criminelle et des articles 18/7, 18/8, 18/16 et 18/17 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Le cas échéant, plusieurs opérateurs ou fournisseurs peuvent créer une Cellule de coordination commune. En pareil cas, cette Cellule de coordination doit prévoir le même service pour chaque opérateur ou fournisseur.

Afin de faire partie de la Cellule de coordination, les membres doivent :

1° Avoir fait l’objet d’un avis de sécurité positif et non périmé conformément à l’article 22*quinquies* de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité;

2° Ne pas avoir fait l’objet d’un refus du ministre de la Justice, ce refus devant être motivé et pouvant intervenir en tout temps.

Un avis est considéré comme étant périmé 5 ans après son octroi.

Les opérateurs et fournisseurs qui ne fournissent aucun des services visés à l’article 126, § 1er, sont dispensés de la condition visée à l’alinéa 3, 1°.

Seuls les membres de la Cellule de coordination peuvent répondre aux demandes des autorités portant sur les données visées à l’alinéa 1er. Ils peuvent cependant, sous leur surveillance et dans la limite du strict nécessaire, obtenir une aide technique de préposés de l’opérateur ou du fournisseur.

Les membres de la Cellule de coordination et les préposés apportant une aide technique sont soumis au secret professionnel.

Chaque opérateur et chaque fournisseur visé à l’article 126, § 1er, alinéa 1er, veille à la confidentialité des données traitées par la Cellule de coordination et communique sans délai à l’Institut et à la Commission pour la protection de la vie privée les coordonnées de la Cellule de coordination et de ses membres ainsi que toute modification de ces données.

§ 2. Chaque opérateur et chaque fournisseur visé à l’article 126, § 1er, alinéa 1er, établit une procédure interne permettant de répondre aux demandes d’accès des autorités aux données à caractère personnel concernant les utilisateurs. Il met, sur demande, à la disposition

de l'Institut des informations sur ces procédures, sur le nombre de demandes reçues, sur la base juridique invoquée et sur sa réponse.

Chaque opérateur et chaque fournisseur visé à l'article 126, § 1er, alinéa 1er, est considéré comme responsable du traitement 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 pour les données traitées sur base de l'article 126 et du présent article.

Les opérateurs de réseaux publics de communications électroniques et les fournisseurs visés à l'article 126, § 1er, alinéa 1er, respectent l'article 114, § 2, pour l'accès aux données visées au paragraphe 1er et leur transmission aux autorités.

§ 3. Chaque fournisseur et chaque opérateur visés à l'article 126, § 1er, alinéa 1er, désigne un ou plusieurs préposés à la protection des données à caractère personnel, qui doit répondre aux conditions cumulatives énumérées au paragraphe 1er, alinéa 3.

Ce préposé ne peut pas faire partie de la Cellule de coordination.

Plusieurs opérateurs ou fournisseurs peuvent désigner un ou plusieurs préposés communs à la protection des données à caractère personnel. En pareil cas, ces préposés doivent assurer la même mission pour chaque opérateur ou fournisseur individuel.

Dans l'exercice de ses missions, le préposé à la protection des données à caractère personnel agit en toute indépendance, et a accès à toutes les données à caractère personnel transmises aux autorités ainsi qu'à tous les locaux pertinents du fournisseur ou de l'opérateur.

L'exercice de ses missions ne peut entraîner pour le préposé des désavantages. Il ne peut, en particulier, être licencié ou remplacé comme préposé à cause de l'exécution des tâches qui lui sont confiées, sans motivation approfondie.

Le préposé doit avoir la possibilité de communiquer directement avec la direction de l'opérateur ou du fournisseur.

Le préposé à la protection des données veille à ce que :

1° les traitements effectués par la Cellule de coordination soient exécutés conformément à la loi;

2° le fournisseur ou l'opérateur ne collecte et conserve que les données qu'il peut légalement conserver;

3° seules les autorités légalement habilitées aient accès aux données conservées;

4° les mesures de sécurité et de protection des données à caractère personnel décrites dans la présente loi et dans la politique de sécurité du fournisseur ou de l'opérateur soient mises en œuvre.

Chaque fournisseur et chaque opérateur visés à l'article 126, § 1er, alinéa 1er, communique sans délai à l'Institut et à la Commission pour la protection de la vie privée les

coordonnées des préposés à la protection des données à caractère personnel, ainsi que toute modification de ces données.

§ 4. Le Roi détermine, par arrêté délibéré en Conseil des ministres, après avis de la Commission pour la protection de la vie privée et de l'Institut :

1° les modalités de la demande et de l'octroi de l'avis de sécurité;

2° les exigences auxquelles la Cellule de coordination doit répondre, en prenant en compte la situation des opérateurs et fournisseurs recevant peu de demandes des autorités judiciaires, n'ayant pas d'établissement en Belgique ou opérant principalement de l'étranger;

3° les informations à fournir à l'Institut et à la Commission pour la protection de la vie privée conformément aux paragraphes 1 et 3 ainsi que les autorités qui ont accès à ces informations;

4° les autres règles régissant la collaboration des opérateurs et des fournisseurs visés à l'article 126, § 1er, alinéa 1er, avec les autorités belges ou avec certaines d'entre elles, pour la fourniture des données visées au paragraphe 1er, en ce compris, si nécessaire et par autorité concernée, la forme et le contenu de la demande. '.

Art. 6. A l'article 127 de la même loi, modifié par les lois des 4 février 2010, 10 juillet 2012 et 27 mars 2014, les modifications suivantes sont apportées :

1° dans le paragraphe 1er, les modifications suivantes sont apportées :

a) dans l'alinéa 1er, les mots ' , aux fournisseurs visés à l'article 126, § 1er, alinéa 1er, ' sont insérés entre les mots ' aux opérateurs ' et les mots ' ou aux utilisateurs finals ';

b) dans l'alinéa 2, les mots ' et des fournisseurs visés à l'article 126, § 1er, alinéa 1er, ' sont insérées entre les mots ' des opérateurs ' et les mots ' aux opérations ';

2° le paragraphe 6 est abrogé.

Art. 7. A l'article 145 de la même loi, modifié par les lois du 25 avril 2007 et du 27 mars 2014, les modifications suivantes sont apportées :

1° les mots ' 126, 126/1, ' sont insérés entre les mots ' 124, ' et le mot ' 127 ';

2° les mots ' , 126, 126/1 ' sont insérés entre les mots ' 47 ' et ' et 127 ';

3° au lieu du paragraphe 3*ter*, annulé par l'arrêt n° 84/2015 de la Cour constitutionnelle, 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, les divulgue ou en fait un usage quelconque. '.

CHAPITRE 3. - *Modifications du Code d'instruction criminelle*

Art. 8. Dans l'article 46*bis*, § 1er, du Code d'instruction criminelle, inséré par la loi du 10 juin 1998 et remplacé par la loi du 23 janvier 2007, les modifications suivantes sont apportées :

a) les mots ' le concours de l'opérateur d'un réseau de communication ' sont remplacés par les mots ' le concours de l'opérateur d'un réseau de communication ';

b) le paragraphe est complété par un alinéa rédigé comme suit :

' Pour des infractions qui ne sont pas de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde, le procureur du Roi, ou, en cas d'extrême urgence, l'officier de police judiciaire, ne peuvent requérir les données visées à l'alinéa 1er que pour une période de six mois préalable à sa décision. '.

Art. 9. Dans l'article 88*bis* du même Code, inséré par la loi du 11 février 1991, remplacé par la loi du 10 juin 1998 et modifié par les lois des 8 juin 2008 et 27 décembre 2012, les modifications suivantes sont apportées :

a) dans le paragraphe 1er, l'alinéa 1er est remplacé par ce qui suit :

' S'il existe des indices sérieux que les infractions sont de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde, et lorsque le juge d'instruction estime qu'il existe des circonstances qui rendent le repérage de communications électroniques ou la localisation de l'origine ou de la destination de communications électroniques nécessaire à la manifestation de la vérité, il peut procéder ou faire procéder, en requérant au besoin, directement ou par l'intermédiaire d'un service de police désigné par le Roi, le concours technique de l'opérateur d'un réseau de communication électronique ou du fournisseur d'un service de communication électronique :

1° au repérage des données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées;

2° à la localisation de l'origine ou de la destination de communications électroniques. ';

b) dans le paragraphe 1er, alinéa 2, les mots ‘ moyen de télécommunication ’ sont remplacés par les mots ‘ moyen de communication électronique ’ et les mots ‘ de la télécommunication ’ par les mots ‘ de la communication électronique ’;

c) dans le paragraphe 1er, l’alinéa 3 est remplacé par ce qui suit :

‘ Le juge d’instruction indique les circonstances de fait de la cause qui justifient la mesure, son caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d’enquête, dans une ordonnance motivée. ’;

d) dans le paragraphe 1er, l’alinéa 4, est remplacé par ce qui suit :

‘ Il précise également la durée durant laquelle elle pourra s’appliquer pour le futur, cette durée ne pouvant excéder deux mois à dater de l’ordonnance, sans préjudice de renouvellement et, le cas échéant, la période pour le passé sur laquelle l’ordonnance s’étend conformément au paragraphe 2. ’;

e) le paragraphe 1er est complété par un alinéa rédigé comme suit :

‘ En cas d’urgence, la mesure peut être ordonnée verbalement. Elle doit être confirmée dans les plus brefs délais dans la forme prévue aux alinéas 3 et 4. ’;

f) le paragraphe 2, dont le texte actuel formera le paragraphe 4, est remplacé par ce qui suit :

‘ § 2. Pour ce qui concerne l’application de la mesure visée au paragraphe 1er, alinéa 1er, aux données de trafic ou de localisation conservées sur la base de l’article 126 de la loi du 13 juin 2005 relative aux communications électroniques, les dispositions suivantes s’appliquent :

- pour une infraction visée au livre II, titre I*ter*, du Code pénal, le juge d’instruction peut dans son ordonnance requérir les données pour une période de douze mois préalable à l’ordonnance;

- pour une autre infraction visée à l’article 90*ter*, §§ 2 à 4, qui n’est pas visée au premier tiret ou pour une infraction qui est commise dans le cadre d’une organisation criminelle visée à l’article 324*bis* du Code pénal, ou pour une infraction qui est de nature à entraîner un emprisonnement correctionnel principal de cinq ans ou une peine plus lourde, le juge d’instruction peut dans son ordonnance requérir les données pour une période de neuf mois préalable à l’ordonnance;

- pour les autres infractions, le juge d’instruction ne peut requérir les données que pour une période de six mois préalable à l’ordonnance. ’;

g) l’article est complété par un paragraphe 3 rédigé comme suit :

‘ § 3. La mesure ne peut porter sur les moyens de communication électronique d’un avocat ou d’un médecin que si celui-ci est lui-même soupçonné d’avoir commis une infraction visée au paragraphe 1er ou d’y avoir participé, ou si des faits précis laissent

présumer que des tiers soupçonnés d'avoir commis une infraction visée au paragraphe 1er, utilisent ses moyens de communication électronique.

La mesure ne peut être exécutée sans que le bâtonnier ou le représentant de l'ordre provincial des médecins, selon le cas, en soit averti. Ces mêmes personnes seront informées par le juge d'instruction des éléments qu'il estime relever du secret professionnel. Ces éléments ne sont pas consignés au procès-verbal. ';

h) dans le paragraphe 2, qui est renuméroté en paragraphe 4, alinéa 1er, les mots ' Chaque opérateur d'un réseau de télécommunication et chaque fournisseur d'un service de télécommunication ' sont remplacés par les mots ' Chaque opérateur d'un réseau de communication électronique et chaque fournisseur d'un service de communication électronique '.

Art. 10. L'article 90*decies* du même Code, inséré par la loi du 30 juin 1994 et modifié par les lois des 8 avril 2002, 7 juillet 2002, 6 janvier 2003 et par la loi du 30 juillet 2013 annulée par l'arrêt de la Cour constitutionnelle n° 84/2015, est complété par un alinéa rédigé comme suit :

' A ce rapport est également joint le rapport dressé en application de l'article 126, § 5, alinéa 4, de la loi du 13 juin 2005 relative aux communications électroniques. '.

Art. 11. Dans l'article 464/25, § 2, alinéa 1er, du même Code, les mots ' l'article 88*bis*, § 2, alinéas 1er et 3 ' sont remplacés par les mots ' l'article 88*bis*, § 4, alinéas 1er et 3 '.

CHAPITRE 4. - *Modifications de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité*

Art. 12. A l'article 13 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, modifié par la loi du 4 février 2010, les modifications suivantes sont apportées :

1° dans le texte néerlandais de l'alinéa 1er, le mot ' inlichtingen ' est remplacé par le mot ' informatie ';

2° l'alinéa 3 est remplacé par ce qui suit :

' Les services de renseignement et de sécurité veillent à la sécurité des données ayant trait à leurs sources et à celles des informations et des données à caractère personnel fournies par ces sources. ';

3° l'article est complété par un alinéa rédigé comme suit :

' Les agents des services de renseignement et de sécurité ont accès aux informations, renseignements et données à caractère personnel recueillis et traités par leur service, pour autant que ceux-ci soient utiles dans l'exercice de leur fonction ou de leur mission. '.

Art. 13. Dans l'article 18/3 de la même loi, inséré par la loi du 4 février 2010, les modifications suivantes sont apportées :

a) dans le paragraphe 1er, l'alinéa 3, actuel formera le paragraphe 5;

b) dans le paragraphe 1er, alinéa 4, qui formera le paragraphe 7, le mot ' mettre ' est remplacé par les mots ' le suivi de la mise ';

c) le paragraphe 2, dont les alinéas 2 à 5 actuels formeront le paragraphe 6, est remplacé par ce qui suit :

' § 2. La décision du dirigeant du service mentionne :

1° la nature de la méthode spécifique;

2° selon le cas, les personnes physiques ou morales, les associations ou les groupements, les objets, les lieux, les événements ou les informations soumis à la méthode spécifique;

3° la menace potentielle qui justifie la méthode spécifique;

4° les circonstances de fait qui justifient la méthode spécifique, la motivation en matière de subsidiarité et de proportionnalité, en ce compris le lien entre le 2° et le 3°;

5° la période pendant laquelle la méthode spécifique peut être appliquée, à compter de la notification de la décision à la Commission;

6° le nom du (ou des) officier(s) de renseignement responsable(s) pour le suivi de la mise en œuvre de la méthode spécifique;

7° le cas échéant, le moyen technique employé pour mettre en œuvre la méthode spécifique;

8° le cas échéant, le concours avec une information ou une instruction judiciaire;

9° le cas échéant, les indices sérieux attestant que l'avocat, le médecin ou le journaliste participe ou a participé personnellement et activement à la naissance ou au développement de la menace potentielle;

10° dans le cas où il est fait application de l'article 18/8, la motivation de la durée de la période à laquelle a trait la collecte de données;

11° la date de la décision;

12° la signature du dirigeant du service. ';

d) le paragraphe 3 est remplacé par ce qui suit :

‘ § 3. Par méthode spécifique, une liste des mesures qui ont été exécutées est transmise à la commission à la fin de chaque mois.

Ces listes comprennent les données visées au § 2, 1° à 3°, 5° et 7°. ’;

e) l’article est complété par un paragraphe 8 rédigé comme suit :

‘ § 8. Le dirigeant du service met fin à la méthode spécifique lorsque la menace potentielle qui la justifie a disparu, lorsque la méthode n’est plus utile pour la finalité pour laquelle elle avait été mise en œuvre, ou quand il a constaté une illégalité. Il informe dans les plus brefs délais la Commission de sa décision. ’.

Art. 14. Dans l’article 18/8 de la même loi, inséré par la loi du 4 février 2010, les modifications suivantes sont apportées :

a) dans le paragraphe 1er, l’alinéa 1er est remplacé comme suit :

‘ Les services de renseignement et de sécurité peuvent, dans l’intérêt de l’exercice de leurs missions, au besoin en requérant à cette fin le concours technique de l’opérateur d’un réseau de communication électronique ou du fournisseur d’un service de communication électronique, procéder ou faire procéder :

1° au repérage des données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées;

2° à la localisation de l’origine ou de la destination de communications électroniques. ’;

b) dans le paragraphe 1er, alinéa 2, les mots ‘ données d’appel ’ sont remplacés par les mots ‘ données de trafic ’.

c) le paragraphe 2, dont le texte actuel formera le paragraphe 4, est remplacé par ce qui suit :

‘ § 2. Pour ce qui concerne l’application de la méthode visée au paragraphe 1er aux données conservées sur la base de l’article 126 de la loi du 13 juin 2005 relative aux communications électroniques, les dispositions suivantes s’appliquent :

1° pour une menace potentielle qui se rapporte à une activité qui peut être liée aux organisations criminelles ou aux organisations sectaires nuisibles, le dirigeant du service ne peut dans sa décision requérir les données que pour une période de six mois préalable à la décision;

2° pour une menace potentielle autre que celles visées sous le 1° et le 3°, le dirigeant du service peut dans sa décision requérir les données pour une période de neuf mois préalable à la décision;

3° pour une menace potentielle qui se rapporte à une activité qui peut être liée au terrorisme ou à l'extrémisme, le dirigeant du service peut dans sa décision requérir les données pour une période de douze mois préalable à la décision. '.

Art. 15. Dans l'article 43/3 de la même loi, inséré par la loi du 4 février 2010, les mots ' visées à l'article 18/3, § 2 ' sont remplacés par les mots ' visées à l'article 18/3, § 3 '.

Art. 16. Dans l'article 43/5, § 1er, alinéa 2, de la même loi, les mots ' visées à l'article 18/3, § 2 ' sont remplacés par les mots ' visées à l'article 18/3, § 3 '. ».

B.2.1. Par la loi attaquée, le législateur a entendu répondre à l'annulation, par l'arrêt de la Cour n° 84/2015, du 11 juin 2015, de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques, tel qu'il avait été modifié par 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 » (ci-après : la loi du 30 juillet 2013) (*Doc. parl*., Chambre, 2015-2016, DOC 54-1567/001, p. 4).

B.2.2. La loi du 30 juillet 2013 ainsi annulée constituait la transposition partielle en droit belge de 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 (*Journal officiel*, 13 avril 2006, L 105/54) et de 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 (*Journal officiel*, 31 juillet 2002, L 201/37) (article 2 de la loi).

B.2.3. L'annulation prononcée par la Cour repose sur les motifs qui suivent :

« 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.3. Il ressort des travaux préparatoires de la loi attaquée que le législateur a examiné en profondeur tant l'arrêt précité de la Cour n° 84/2015 du 11 juin 2015 que l'arrêt de la Cour de justice du 8 avril 2014, sur lequel il est basé.

L’objectif que le législateur poursuit par la loi attaquée du 29 mai 2016 est non seulement de lutter contre le terrorisme et la pédopornographie mais également de pouvoir utiliser les données conservées dans une grande variété de situations dans lesquelles ces données peuvent être à la fois le point de départ mais également une étape de l’enquête pénale (*Doc. parl.* Chambre, 2015-2016, DOC 54-1567/001, p. 6).

B.4.1. Il ressort de l'exposé des motifs de la loi attaquée que le législateur a considéré qu'il était impossible, à la lumière de l'objectif poursuivi, de mettre en place une obligation de conservation ciblée et différenciée, et qu'il a choisi d'assortir l'obligation de conservation générale et indifférenciée de garanties strictes, tant sur le plan de la protection de la conservation que sur le plan de l'accès, afin de limiter à un minimum l'ingérence dans le droit au respect de la protection de la vie privée. A cet égard, il a été souligné qu'il est tout simplement impossible d'opérer une différenciation *a priori* en fonction des personnes, des périodes temporelles et des zones géographiques.

B.4.2. Cette impossibilité est exposée en détail dans les travaux préparatoires :

« 7. La distinction en fonction des personnes, périodes temporelles et zones géographiques

Le premier des trois éléments dont la combinaison viole le principe de proportionnalité concerne le principe même de l’obligation de conservation des données. C’est le fait de conserver les données de toutes les personnes de manière indifférenciée. Après analyse approfondie, il ressort qu’il n’est pas possible d’opérer une différenciation *a priori* de cet élément.

Dans l'avis 33-2015 précité, la Commission [de la protection de la vie privée] va dans le même sens puisqu’elle indique que ‘ certains aspects des arrêts [de la Cour de justice et de la Cour constitutionnelle] lui paraissent difficilement applicables, en particulier la distinction en fonction des personnes, périodes temporelles et/ ou zones géographiques ’.

a) Toutes les personnes même si elles ne sont pas encore impliquées dans une enquête.

Limiter la conservation des données à celles concernant des personnes qui font déjà l’objet d’une enquête pénale ou de renseignement n’a pas de sens car cette possibilité existe déjà par ailleurs. Les autorités judiciaires comme les services de renseignement peuvent déjà imposer le ‘ repérage ’ des communications dans le cadre d’une enquête précise et donc obliger les opérateurs et fournisseurs d’accès à conserver les données pour le futur une fois qu’on a identifié la personne ou un service de communication dans une enquête pénale. L’objectif de l’article 126 LCE est de s’assurer qu’un certain nombre de données existeront

aussi pour une période limitée du passé. L'article 126 n'a donc de sens que s'il porte sur les personnes qui ne font pas encore nécessairement l'objet d'une enquête pénale ou de renseignement.

Cette dimension est indispensable comme le montrent les exemples repris au point 2.

Il faut par ailleurs rappeler que la mesure peut tout aussi bien bénéficier à la victime pour ses propres données (dans des affaires de harcèlement, par exemple, il s'agira de retourner dans le passé des données de la victime pour identifier l'origine d'un appel, un email ou un sms) que l'accusé (les données de localisation peuvent montrer que l'accusé n'était pas sur le lieu de l'infraction au moment où elle a été commise). Il peut aussi s'agir d'identifier des témoins, ce qui peut jouer à charge comme à décharge.

b) Pas de différenciation en fonction de la période temporelle, la zone géographique ou un cercle de personnes.

La Cour constitutionnelle, renvoyant à l'arrêt de la Cour de justice, note que l'article 126 attaqué ' 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 '.

Cette partie de l'arrêt de la Cour de justice a suscité beaucoup d'interrogations quant à sa portée. Le groupe de travail qui a préparé le présent projet de loi s'est lui aussi interrogé sur la possibilité de limiter l'impact de l'article 126 en travaillant sur les critères soulevés par la Cour de justice, c'est-à-dire une ' période temporelle ', ' une zone géographique déterminée ' ou encore ' un cercle de personnes '.

La conclusion est que cette partie de l'arrêt de la Cour de justice doit être lue comme une explication de la sensibilité du principe de conservation généralisée des données. Mais il n'est pas possible d'y puiser une solution pour appliquer une différenciation.

La référence à la ' période temporelle ' pourrait par exemple viser une situation spécifique et temporaire de menace pour l'ordre ou la sécurité publique. Mais, d'une part, ce type de critère n'est pas cohérent avec un grand nombre de situations et de types de criminalité pour lesquels la conservation des données s'avère décisive (par exemple, en matière de pédopornographie) et, d'autre part, là où il pourrait trouver à s'appliquer, ce type de critère négligerait le fait que la situation en question ne peut pas forcément être anticipée (par exemple, en cas de menace terroriste matérialisée par un attentat).

Quant à la référence à une ' zone géographique ' ou un ' cercle de personnes ', une activation de l'article 126 LCE sur la base de ce type de critère s'apparenterait à du profilage avec les risques de discrimination qui en découlent.

c) Pas d'exclusion de certaines professions

La Cour constitutionnelle note enfin, toujours concernant cette absence de différenciation entre les personnes dont les données sont conservées, que ' la loi s'applique sans aucune exception, également à des personnes dont les communications sont soumises au secret professionnel '.

Ici aussi, on s'est interrogé sur la possibilité de créer une différentiation pour faire suite à cette partie de l'arrêt. Il s'agirait d'exclure *a priori* certaines personnes, en fonction de leur profession, de la conservation des données.

Cette différentiation n'est pas possible. D'une part, s'il est vrai que certaines professions sont protégées en matière de collecte de la preuve ou de renseignement, cette protection n'est jamais absolue. D'autre part, il faut ici encore noter que la conservation des données ne peut pas être vue comme une mesure visant un accès *a posteriori* aux données nécessairement ' contre ' la personne. La donnée en question peut servir à disculper celle-ci ou encore être utile lorsque la personne en question est victime d'une infraction. Rappelons à nouveau que la conservation des données ne concerne pas le contenu des communications.

On verra toutefois plus loin que la protection de certaines professions est bien renforcée dans le présent projet de loi, mais au niveau de la réglementation de l'accès aux données conservées.

On peut conclure qu'il n'est pas possible de modaliser l'article 126 LCE sur la base du premier élément (l'absence de différentiation en fonction des personnes) repris par la Cour constitutionnelle et la Cour de justice. Tous les pays européens contactés sont arrivés à la même conclusion.

Ni l'arrêt de la Cour constitutionnelle ni celui de la Cour de justice de l'Union européenne ne concluent toutefois qu'un seul des quatre éléments suffit à constituer une violation du principe de proportionnalité. Si tel était le cas, et l'absence de différenciation entre les personnes constituant l'élément essentiel de la législation nationale et européenne annulée, on peut penser que la Cour de justice et la Cour constitutionnelle auraient uniquement examiné cet aspect et auraient conclu à la violation du droit au respect de la vie privée sans examiner les autres éléments.

Dans son avis précité sur le présent projet de loi, la Commission vie privée soutient cette interprétation et indique : ' comme indiqué dans l'exposé des motifs, aucun des deux arrêts ne conclut qu'un seul des quatre éléments suffit à constituer une violation du principe de proportionnalité. Si un élément déterminé des arrêts ne peut pas être retenu, il faut compenser cet élément par un régime plus strict sur les autres aspects. '

8. Les catégories de données

La Cour constitutionnelle note que ‘ […] 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 ’.

Le présent projet de loi introduit une distinction sur la base de 3 catégories de données.

La première catégorie concerne les données d’identification (qui est titulaire de tel numéro de gsm, quel est le numéro de gsm de telle personne, qui se trouve derrière telle adresse IP, …). Ces données sont les plus demandées et sont modérément attentatoires à la vie privée, par rapport notamment aux deuxième et troisième catégories.

La deuxième catégorie concerne les données de connexion et localisation (quel est notamment le lieu et la durée d’une communication).

La troisième catégorie concerne les données personnelles de communications (qui a appelé ou correspondu avec qui).

Les deuxième et troisième catégories sont plus attentatoires à la vie privée que la première. Les accès à ces données sont moins nombreux que ceux aux données d’identification, mais restent fréquents.

Après de nombreuses discussions au sein du gouvernement et avec les services et autorités concernées, et après avoir envisagé une différenciation entre les délais de conservation en fonction des catégories de données, la conclusion est que, vu les nécessités liées à la lutte contre les infractions terroristes, une période de 12 mois de conservation est nécessaire pour chacune des 3 catégories.

9. Le renforcement des garanties au niveau de l’accès des autorités aux données

La directive UE a été considérée comme particulièrement problématique parce qu’elle ne réglait que l’obligation de conservation sans réglementer et donc sans encadrer l’accès des autorités aux données concernées. La Cour constitutionnelle note que ‘ 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. ’

L’article 126 LCE annulé renvoyait pourtant explicitement, pour les deux régimes d’accès principaux, aux règles régissant cet accès, c’est-à-dire les articles 46*bis* et 88*bis* du Code d’instruction criminelle pour le cadre pénal et les articles 18/7 et 18/8 de la loi organique des services de renseignement et de sécurité pour les accès au niveau de l’activité de renseignement.

Le présent projet de loi donne suite à cette partie de l'arrêt de la Cour constitutionnelle en renforçant le lien entre l'article 126 LCE et le régime d'accès défini dans les autres lois précitées. Il clarifie aussi le fait que l'accès aux données conservées n'est possible que pour les finalités explicitement énumérées dans l'article 126 LCE.

Mais le présent projet de loi va plus loin en renforçant les garanties prévues par le Code d'instruction criminelle et la loi organique des services de renseignement et de sécurité. Il encadre aussi mieux l'accès pour les autres finalités. Celles-ci sont précisées et étendues à certaines situations très spécifiques.

a) Renforcement des garanties dans le Code d'instruction criminelle

Le projet de loi modifie en première instance les règles quant à l'accès aux données d'identification qui est réglé par l'article 46*bis* du Code d'instruction criminelle et qui concerne l'accès aux données des deux premières catégories. Cet article 46*bis* a déjà été modifié par les lois du 27 décembre 2004 et du 23 janvier 2007. Il n'est pas possible d'alourdir la procédure pour une mesure aussi fréquente et dont l'impact sur la vie privée reste limité. Les conditions restent bien entendu applicables, notamment l'autorisation préalable et motivée du parquet ou du juge d'instruction.

Le projet introduit néanmoins une différenciation de l'accès aux donnés à l'article 46*bis*, en ajoutant au § 1er que pour des infractions de moindre gravité, qui ne sont pas de nature à entraîner une peine d'emprisonnement correctionnel principal d'un an ou une peine plus lourde, les données peuvent uniquement être requises pour une période de six mois préalable à la décision du procureur du Roi.

Le Conseil d'Etat fait remarquer dans son avis que ce n'est pas la même différenciation sur la base de la gravité de l'infraction que celle prévue pour l'article 88*bis* C.I.Cr. (voy. *infra*) et que les raisons y afférentes doivent être indiquées plus clairement.

Tout d'abord, il serait déraisonnable de rendre la demande des données visées à l'article 46*bis*, § 1er, 1° et 2° possible seulement pour les infractions graves.

Comme il a déjà été indiqué, les données d'identification visées ne sont pas de nature à ce que leur communication implique une intrusion importante dans la vie privée.

Enfin, le raisonnement du Conseil d'Etat n'est que partiellement valide lorsqu'il indique que les données d'identification de l'article 46*bis* peuvent *de facto* être conservées pour une durée beaucoup plus longue que 12 mois. D'une part, il est vrai que ce délai de conservation ne commence à courir qu'à ' la date à partir de laquelle une communication est possible pour la dernière fois à l'aide du service utilisé ' (article 126, § 3, premier alinéa LCE) mais, d'autre part, cette règle ne va pas toujours mener dans la pratique à une durée de conservation plus longue que douze mois.

Il faut en particulier prendre en compte la situation des adresses IP dynamiques qui changent fréquemment et pour lesquelles le délai commencera à courir à partir de la fin de la communication concernée. Or, pouvoir identifier qui utilisait une adresse IP précise à un

moment X est de plus en plus important pour les enquêtes en raison de l'évolution des communications.

Le régime applicable pour ce qui concerne le repérage des communications et donc l'accès aux données des deux dernières catégories (données de connexion et de localisation et données personnelles de communication) est également considérablement renforcé sur le plan des garanties. Ce régime est défini à l'article 88*bis* du Code d'instruction criminelle. Le projet de loi apporte trois garanties principales.

Il introduit une exigence de subsidiarité : la mesure ne peut être autorisée que si le résultat ne peut pas être atteint par une autre mesure moins intrusive.

Le projet introduit aussi une différenciation sur la base de la gravité de l'infraction. La mesure ne sera plus disponible dans le cadre de la poursuite d'infractions punies de moins d'un an d'emprisonnement. Pour les infractions punies de un à cinq ans d'emprisonnement, la mesure pourra être autorisée, mais ne pourra porter que sur les données relatives aux six derniers mois. Pour les infractions punies d'au moins cinq ans d'emprisonnement et/ou reprises sur la liste prévue à l'article 90*ter* du Code d'instruction criminelle (c'est-à-dire les infractions pouvant donner lieu à écoute téléphonique), et/ou qui sont commises dans le cadre d'une organisation criminelle, la mesure pourra porter sur une période de neuf mois précédant la demande. Enfin, elle pourra porter sur l'entièreté de la période de conservation pour les enquêtes en matière de terrorisme.

Enfin, une protection explicite est prévue pour les avocats et les médecins.

b) Renforcement des garanties dans la loi organique des services de renseignement et de sécurité

L'accès aux données conservées est réglé par les articles 18/3, 18/7 et 18/8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité. Cet accès est déjà fortement encadré.

L'article 18/3 règle la procédure de mise en œuvre des méthodes spécifiques et leur contrôle par une Commission indépendante, composée de trois magistrats (la Commission BIM). Il prévoit aussi des garanties en vue de préserver le secret professionnel des avocats et médecins et le secret des sources des journalistes.

Conformément à l'art. 18/3, § 1er, de la loi organique, les méthodes spécifiques ne peuvent être mises en œuvre que si :

- les méthodes ordinaires s'avèrent insuffisantes pour récolter les informations nécessaires à une mission de renseignement (subsidiarité);

- il y a une menace potentielle;

- elles sont proportionnelles au degré de gravité de la menace;

- la décision du chef du service est écrite et motivée.

Ces conditions impliquent que les services de renseignement doivent, pour chaque méthode, justifier le lien entre la cible et la menace.

Aucune méthode spécifique ne peut être mise en œuvre avant la notification de la décision du chef du service à la commission. Le contrôle de légalité des méthodes spécifiques par les membres de la commission, en ce compris le respect de la subsidiarité et de la proportionnalité, peut s'effectuer à tout moment. Le Comité R, organe de contrôle parlementaire, remplit un rôle juridictionnel dans le cadre des méthodes BIM.

Il est interdit aux services de renseignement d'obtenir, d'analyser et d'exploiter des données protégées par le secret professionnel et le secret des sources, sauf si le service dispose au préalable d'indices sérieux selon lesquels l'avocat, le médecin ou le journaliste prend personnellement et activement part à une menace.

Dans ce cas, trois garanties sont prévues :

- la méthode ne peut être utilisée qu'après que la commission a émis un avis conforme;

- la méthode ne peut être appliquée sans que, selon le cas, le président de l'OVB, de l'OBFG, du Conseil National de l'Ordre des Médecins ou de l'Association Générale des Journalistes Professionnels en ait été informé au préalable.

- le président de la commission doit vérifier si les données obtenues via cette méthode ont un lien direct avec la menace.

Le renforcement des garanties prévues à l'article 18/3 vise principalement à rendre obligatoire différentes mentions et motivations dans la décision du chef du service, dont la motivation de la période de rétroactivité des données demandées aux opérateurs.

Il est également précisé, pour renforcer les garanties existantes, l'obligation pour le dirigeant du service de mettre fin à la méthode dès qu'il est constaté une illégalité, ou que la menace qui l'a justifiée n'existe plus, ou qu'elle n'est plus utile.

c) Pour les autres accès

Le projet de loi comme la loi annulée concerne principalement la conservation aux fins de l'enquête pénale ainsi que du renseignement, mais d'autres finalités secondaires sont prévues. Le projet de loi ajoute certaines finalités ciblées, mais prévoit des limitations importantes.

Ainsi, la cellule ' personnes disparues ' de la Police aura accès, par l'intermédiaire d'un service de police désigné par le Roi, aux données dans le cadre d'une disparition inquiétante, mais seulement pour une période de 48 heures, étant entendu qu'un accès plus large dans le cadre de l'enquête judiciaire est possible.

Les services d'urgence offrant de l'aide sur place pourront obtenir certaines données conservées dans certaines situations, mais pour autant que la demande envers l'opérateur intervienne au plus tard dans les 24 heures de l'appel.

Quant au Service de médiation pour les télécommunications, pour ce qui concerne une utilisation malveillante d'un réseau ou d'un service de communications électroniques, il pourra obtenir les données d'identification de la personne qui est à l'origine de cette utilisation malveillante.

10. Le renforcement de la sécurisation des données conservées par les opérateurs

Enfin, le projet de loi, faisant suite notamment aux préoccupations émises par la Cour de justice, renforce les mesures à prendre par les opérateurs et fournisseurs de manière à protéger et sécuriser les données et l'accès à celles-ci. Il s'agit notamment de prendre des mesures de protection technologiques à l'égard de ces données, d'assurer la traçabilité des accès, de détruire les données à l'expiration du délai, ou encore de désigner un préposé à la protection des données chargé de veiller au respect des différentes règles en la matière » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1567/001, pp. 10-18).

B.5. Après l'adoption de la loi attaquée, la Cour de justice de l'Union européenne a répondu à deux questions préjudicielles relatives à l'interprétation de l'article 15, paragraphe 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.

B.6.1. L'article 15 de la directive précitée dispose :

« 1. Les Etats membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale - c'est-à-dire la sûreté de l'Etat - la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive [95/46]. A cette fin, les Etats membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne.

[…] ».

B.6.2. La Cour de justice de l'Union européenne a répondu par un arrêt rendu en grande chambre le 21 décembre 2016, donc lorsque la loi attaquée avait déjà été adoptée (CJUE,

21 décembre 2016, C-203/15, *Tele2 Sverige AB c. Post-och telestyrelsen* et C-698/15, *Secretary of State for the Home Departement c. Tom Watson et a.*).

B.6.3. La Cour de justice conclut au point 78 de cet arrêt qu'« une mesure législative par laquelle un Etat membre impose, sur le fondement de l'article 15, paragraphe 1, de la directive 2002/58, aux fournisseurs de services de communications électroniques, aux fins mentionnées par cette disposition, d'accorder aux autorités nationales, dans les conditions prévues par une telle mesure, l'accès aux données conservées par lesdits fournisseurs, porte sur des traitements de données à caractère personnel par ces derniers, traitements qui relèvent du champ d'application de cette directive ».

B.6.4. La Cour de justice rappelle que l'article 5, paragraphe 1, de la directive prévoit que les Etats membres doivent garantir, par leur législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public ainsi que la confidentialité des données relatives au trafic y afférentes. Le principe de confidentialité implique une interdiction faite aux tiers de stocker, sans le consentement des utilisateurs, les données relatives au trafic afférentes à leurs communications électroniques (points 84 et 85).

B.6.5. La Cour de justice rappelle également que l'article 15, paragraphe 1, de la directive permet aux Etats membres d'introduire des exceptions à l'obligation de principe énoncée à l'article 5, paragraphe 1, précité, exceptions qui, conformément à la jurisprudence constante de la Cour, sont d'interprétation stricte. « [L'article 15] ne saurait donc justifier que la dérogation à cette obligation de principe et, en particulier, à l'interdiction de stocker ces données, prévue à l'article 5 de cette directive, devienne la règle, sauf à vider largement cette dernière disposition de sa portée » (points 88 et 89).

Il est relevé, à cet égard :

« L'article 15, paragraphe 1, première phrase, de la directive 2002/58 prévoit que les mesures législatives qu'il vise et qui dérogent au principe de confidentialité des communications et des données relatives au trafic y afférentes doivent avoir pour objectif de ' sauvegarder la sécurité nationale - c'est-à-dire la sûreté de l'Etat - la défense et la sécurité publique, ou [d']assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques ', ou doivent poursuivre un des autres objectifs visés à l'article 13, paragraphe 1, de la

directive 95/46, auquel renvoie l'article 15, paragraphe 1, première phrase, de la directive 2002/58 (voir, en ce sens, arrêt du 29 janvier 2008, *Promusicae*, C-275/06, EU:C:2008:54, point 53). Une telle énumération d'objectifs revêt un caractère exhaustif ainsi qu'il ressort de l'article 15, paragraphe 1, deuxième phrase, de cette dernière directive, aux termes duquel les mesures législatives doivent être justifiées par ' un des motifs énoncés ' à l'article 15, paragraphe 1, première phrase, de ladite directive. Partant, les Etats membres ne sauraient adopter de telles mesures à d'autres fins que celles énumérées à cette dernière disposition » (point 90).

La Cour de justice conclut, en ce qui concerne la portée de l'article 15, § 1, de la directive :

« Les Etats membres peuvent adopter une mesure dérogeant au principe de confidentialité des communications et des données relatives au trafic y afférentes lorsqu'elle est ' nécessaire, appropriée et proportionnée, au sein d'une société démocratique ', au regard des objectifs que cette disposition énonce. Quant au considérant 11 de cette directive, il précise qu'une mesure de cette nature doit être ' rigoureusement ' proportionnée au but poursuivi. En ce qui concerne, en particulier, la conservation de données, l'article 15, paragraphe 1, deuxième phrase, de ladite directive exige que celle-ci n'ait lieu que ' pendant une durée limitée ' et ' lorsque cela est justifié ' par un des objectifs visés à l'article 15, paragraphe 1, première phrase, de cette même directive » (point 95).

B.6.6. La Cour de justice examine ensuite si une réglementation nationale telle celle qui s'applique à la première affaire qui a donné lieu aux questions préjudicielles dont elle est saisie satisfait aux conditions prédécrites. Elle constate que la réglementation nationale en cause prévoit une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique, et qu'elle oblige les fournisseurs de services de communications électroniques à conserver ces données de manière systématique et continue, et ce sans aucune exception. Les données ainsi conservées permettent de retrouver et d'identifier la source d'une communication et sa destination, la date, l'heure et la durée de cette communication, le matériel de communication des utilisateurs, ainsi que de localiser le matériel de communication mobile (points 97 et 98).

Selon la Cour de justice, prises dans leur ensemble, ces données sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées. Ces données fournissent ainsi les moyens d'établir le profil des

personnes concernées, information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications.

La Cour de justice a jugé :

« 100. L'ingérence que comporte une telle réglementation dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte s'avère d'une vaste ampleur et doit être considérée comme particulièrement grave. La circonstance que la conservation des données est effectuée sans que les utilisateurs des services de communications électroniques en soient informés est susceptible de générer dans l'esprit des personnes concernées le sentiment que leur vie privée fait l'objet d'une surveillance constante (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 37).

101. Même si une telle réglementation n'autorise pas la conservation du contenu d'une communication et, partant, n'est pas de nature à porter atteinte au contenu essentiel desdits droits (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 39), la conservation des données relatives au trafic et des données de localisation pourrait toutefois avoir une incidence sur l'utilisation des moyens de communication électronique et, en conséquence, sur l'exercice par les utilisateurs de ces moyens de leur liberté d'expression, garantie à l'article 11 de la Charte (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 28).

102. Eu égard à la gravité de l'ingérence dans les droits fondamentaux en cause que constitue une réglementation nationale prévoyant, aux fins de la lutte contre la criminalité, la conservation de données relatives au trafic et de données de localisation, seule la lutte contre la criminalité grave est susceptible de justifier une telle mesure (voir, par analogie, à propos de la directive 2006/24, arrêt Digital Rights, point 60).

103. En outre, si l'efficacité de la lutte contre la criminalité grave, notamment contre la criminalité organisée et le terrorisme, peut dépendre dans une large mesure de l'utilisation des techniques modernes d'enquête, un tel objectif d'intérêt général, pour fondamental qu'il soit, ne saurait à lui seul justifier qu'une réglementation nationale prévoyant la conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation soit considérée comme nécessaire aux fins de ladite lutte (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 51).

104. A cet égard, il convient de relever, d'une part, qu'une telle réglementation a pour effet, eu égard à ses caractéristiques décrites au point 97 du présent arrêt, que la conservation des données relatives au trafic et des données de localisation est la règle, alors que le système mis en place par la directive 2002/58 exige que cette conservation des données soit l'exception.

105. D'autre part, une réglementation nationale telle que celle en cause au principal, qui couvre de manière généralisée tous les abonnés et utilisateurs inscrits et vise tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic, ne prévoit aucune différenciation, limitation ou exception en fonction de l'objectif poursuivi. Elle concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques, sans que ces personnes se trouvent, même indirectement, dans

une situation susceptible de donner lieu à des poursuites pénales. Elle s'applique donc même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions pénales graves. En outre, elle ne prévoit aucune exception, de telle sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, points 57 et 58).

106. Une telle réglementation ne requiert aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique. Notamment, elle n'est pas limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique et/ou sur un cercle de personnes 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 lutte contre la criminalité (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 59).

107. Une réglementation nationale telle que celle en cause au principal excède donc les limites du strict nécessaire et ne saurait être considérée comme étant justifiée, dans une société démocratique, ainsi que l'exige l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte.

108. En revanche, l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, ne s'oppose pas à ce qu'un Etat membre adopte une réglementation permettant, à titre préventif, la conservation ciblée des données relatives au trafic et des données de localisation, à des fins de lutte contre la criminalité grave, à condition que la conservation des données soit, en ce qui concerne les catégories de données à conserver, les moyens de communication visés, les personnes concernées ainsi que la durée de conservation retenue, limitée au strict nécessaire.

109. Pour satisfaire aux exigences énoncées au point précédent du présent arrêt, cette réglementation nationale doit, en premier lieu, prévoir des règles claires et précises régissant la portée et l'application d'une telle mesure de conservation des données et imposant un minimum d'exigences, de telle 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. Elle doit en particulier indiquer en quelles circonstances et sous quelles conditions une mesure de conservation des données peut, à titre préventif, être prise, garantissant ainsi qu'une telle mesure soit limitée au strict nécessaire (voir, par analogie, à propos de la directive 2006/24, arrêt Digital Rights, point 54 et jurisprudence citée).

110. En second lieu, s'agissant des conditions matérielles auxquelles doit satisfaire une réglementation nationale permettant, dans le cadre de la lutte contre la criminalité, la conservation, à titre préventif, des données relatives au trafic et des données de localisation, afin de garantir qu'elle soit limitée au strict nécessaire, il convient de relever que, si ces conditions peuvent varier en fonction des mesures prises aux fins de la prévention, de la recherche, de la détection et de la poursuite de la criminalité grave, la conservation des données n'en doit pas moins toujours répondre à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi. En particulier, de telles conditions

doivent s'avérer, en pratique, de nature à délimiter effectivement l'ampleur de la mesure et, par suite, le public concerné.

111. S'agissant de la délimitation d'une telle mesure quant au public et aux situations potentiellement concernés, la réglementation nationale doit être fondée sur des éléments objectifs permettant de viser un public dont les données sont susceptibles de révéler un lien, au moins indirect, avec des actes de criminalité grave, de contribuer d'une manière ou d'une autre à la lutte contre la criminalité grave ou de prévenir un risque grave pour la sécurité publique. Une telle délimitation peut être assurée au moyen d'un critère géographique lorsque les autorités nationales compétentes considèrent, sur la base d'éléments objectifs, qu'il existe, dans une ou plusieurs zones géographiques, un risque élevé de préparation ou de commission de tels actes.

112. Eu égard à l'ensemble des considérations qui précèdent, il convient de répondre à la première question dans l'affaire C-203/15 que l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique ».

B.6.7. A la seconde question préjudicielle dans l'affaire C-203/15 et à la première question préjudicielle dans l'affaire C-698/15, la Cour de justice répond que l'article 15, paragraphe 1, de la directive 2002/58/CE, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale régissant la protection et la sécurité des données relatives au trafic et des données de localisation, en particulier l'accès des autorités nationales compétentes aux données conservées, sans limiter, dans le cadre de la lutte contre la criminalité, cet accès aux seules fins de lutte contre la criminalité grave, sans soumettre ledit accès à un contrôle préalable par une juridiction ou une autorité administrative indépendante, et sans exiger que les données en cause soient conservées sur le territoire de l'Union (point 125).

B.6.8. De son côté, la Cour européenne des droits de l'homme a entre-temps jugé la législation suédoise relative à l'interception massive de communications électroniques conforme à l'article 8 de la Convention européenne des droits de l'homme, dans son arrêt *Centrum för Rättvisa* c. Suède, du 19 juin 2018. Pour conclure à l'absence de violation, elle se base sur les critères qu'elle a développés dans sa jurisprudence antérieure (*cf.* notamment CEDH, grande chambre, 4 décembre 2015, *Roman Zakharov* c. Russie). Elle observe, en particulier, ce qui suit :

« La Cour a expressément reconnu que les autorités nationales disposent d'une ample marge d'appréciation pour choisir les moyens de sauvegarder la sécurité nationale (*cf. Weber et Saravia*, précité, § 106). Dans les affaires *Weber et Saravia* et *Liberty e.a.*, la Cour a admis que les règles d'interception de masse n'excédaient pas, en soi, cette marge. Compte tenu du raisonnement de la Cour dans ces arrêts et compte tenu des menaces qui pèsent actuellement sur de nombreux Etats contractants (notamment le terrorisme mondial et d'autres formes graves de criminalité telles que le trafic de drogue, la traite des êtres humains, l'exploitation sexuelle des enfants et la cybercriminalité), des évolutions technologiques qui ont permis aux terroristes et aux criminels d'échapper plus facilement à la détection sur Internet et de l'imprévisibilité des voies par lesquelles les communications électroniques sont transmises, la Cour considère que la décision de recourir à un système d'interception de masse pour identifier des menaces pour la sécurité nationale jusqu'ici inconnues est une décision qui relève toujours de la marge d'appréciation des Etats » (CEDH, 19 juin 2018, *Centrum för Rättvisa* c. Suède, § 112).

Quant au mémoire de la « Fondation pour enfants disparus et sexuellement exploités, en abrégé ' Child Focus ' »

B.7.1. Dans un mémoire du 23 avril 2018, reçu au greffe le 25 avril 2018, Child Focus communique ses observations à propos des recours en annulation.

B.7.2. L'article 87, § 2, de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle prévoit que lorsque la Cour constitutionnelle statue sur des recours en annulation, toute personne justifiant d'un intérêt peut adresser ses observations dans un mémoire à la Cour dans les trente jours de la publication prescrite par l'article 74 de cette loi spéciale. Elle est de ce fait, réputée partie au litige.

B.7.3. La publication précitée s'est faite au *Moniteur belge* du 15 février 2017. Le mémoire est donc irrecevable.

Quant au fond

B.8. Un moyen unique dans les affaires n^{os} 6590 et 6597 est pris de la violation, par la loi attaquée, des articles 10 et 11 de la Constitution lus isolément 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.9.1. L'Ordre des barreaux francophones et germanophone, partie requérante dans l'affaire n° 6590, reproche à la loi 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. Cette partie requérante constate que la loi implique encore une obligation généralisée d'enregistrement et de conservation de certaines métadonnées, lesquelles permettent de déterminer si un avocat a été consulté par une personne physique ou morale, d'identifier cet avocat, d'identifier ses interlocuteurs et en particulier ses clients, ainsi que les date et heure de la communication. Cette obligation généralisée s'impose à l'ensemble des fournisseurs au public de services de téléphonie fixe, de téléphonie mobile, d'accès à internet, de courrier électronique par internet, de téléphonie par internet et de réseaux publics de communications électroniques.

B.9.2. La partie requérante dans l'affaire n° 6590 fait également grief à la loi attaquée de prévoir une obligation généralisée de conservation des données sans opérer de distinction entre les justiciables selon qu'ils font, ou non, l'objet d'une mesure d'enquête ou de poursuite pour des faits susceptibles de donner lieu à des condamnations pénales.

Elle soutient encore que les catégories de données visées par la loi sont extrêmement larges et variées, en ce qu'elles concernent celles qui visent à identifier l'utilisateur ou l'abonné et les moyens de communication, les données relatives à l'accès et la connexion de l'équipement terminal au réseau et au service et à la localisation de cet équipement, y compris le point de terminaison du réseau, ainsi que les données de communication même si leur contenu est en revanche exclu.

B.10.1. Les parties requérantes dans l'affaire n° 6597 reprochent à la loi attaquée de traiter de manière identique les utilisateurs de services de télécommunications ou de communications électroniques soumis au secret professionnel, dont notamment les professionnels comptables et fiscaux, et les autres utilisateurs de ces services sans tenir compte du statut particulier des professionnels comptables et fiscaux, du caractère

fondamental du secret professionnel auquel ils sont soumis et de la nécessaire relation de confiance qui doit les unir à leurs clients.

B.10.2. Elles reprochent également à la loi attaquée de traiter 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.

B.11.1. Un premier moyen dans l'affaire n° 6599 est pris de la violation des articles 10, 11, 12, 15, 22 et 29 de la Constitution, lus isolément ou combinés 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, avec l'article 17 du Pacte international relatif aux droits civils et politiques, avec le principe général de sécurité juridique, de proportionnalité, de droit à l'autodétermination en matière d'information ainsi qu'avec l'article 5, § 4, du Traité de l'Union européenne.

B.11.2. L'ASBL « Liga voor Mensenrechten » et l'ASBL « Ligue des Droits de l'Homme », parties requérantes dans l'affaire n° 6599, reprochent à la loi attaquée de prévoir une obligation générale de conservation des données, ce qui oblige les opérateurs et les fournisseurs de services téléphoniques publics (y compris la téléphonie par internet), d'accès à internet et de courrier électronique par internet ainsi que les fournisseurs de réseaux publics de communications électroniques, à conserver durant douze mois, *de facto* pour tous les Belges, suspects ou non, les données relatives au trafic concernant la téléphonie fixe, la téléphonie mobile et la téléphonie par internet, et les données relatives à l'accès à internet, et à les mettre à la disposition de la police et de la justice, des services de renseignement et de sécurité, des services d'urgence, de la Cellule des personnes disparues ainsi que du Service de médiation pour les télécommunications.

B.12.1. Un premier moyen dans l'affaire n° 6601 est pris de la violation, par la loi attaquée, de l'article 8 de la Convention européenne des droits de l'homme, des articles 7, 8, 11.4 et 52 de la Charte des droits fondamentaux de l'Union européenne, des articles 10, 11, 19 et 22 de la Constitution, de l'article 2, a), de la directive 95/46/CE du Parlement européen et

du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ainsi que des articles 1, 2, 3, 5, 6, 9 et 15 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.

B.12.2. Les parties requérantes dans l'affaire n° 6601 sont des personnes physiques qui habitent en Belgique et utilisent différents services de communications électroniques dans le cadre d'un contrat conclu avec un opérateur. Dans la première branche du premier moyen, elles font grief à la loi attaquée d'imposer une obligation générale et indifférenciée de conservation des données d'identification, de connexion et de localisation ainsi que des données de communication personnelles à charge des fournisseurs de services de téléphonie, en ce compris par internet, d'accès à internet, de courrier électronique par internet, aux opérateurs qui fournissent des réseaux publics de communications électroniques ainsi qu'aux opérateurs qui fournissent un de ces services.

B.13. Compte tenu de leur connexité, les moyens exposés dans les diverses affaires doivent être examinés ensemble.

B.14.1. L'article 22 de la Constitution dispose :

« Chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi.

La loi, le décret ou la règle visée à l'article 134 garantissent la protection de ce droit ».

L'article 8 de la Convention européenne des droits de l'homme dispose :

« 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au

bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui ».

B.14.2. Les articles 7, 8, 11 et 52 de la Charte des droits fondamentaux de l'Union européenne disposent :

« Article 7

Respect de la vie privée et familiale

Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications.

Article 8

Protection des données à caractère personnel

1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante ».

« Article 11

Liberté d'expression et d'information

1. Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontières.

2. La liberté des médias et leur pluralisme sont respectés ».

« *Article 52*

Portée et interprétation des droits et des principes

1. Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.

2. Les droits reconnus par la présente Charte qui font l'objet de dispositions dans les traités s'exercent dans les conditions et limites définies par ceux-ci.

3. Dans la mesure où la présente Charte contient des droits correspondant à des droits garantis par la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention. Cette disposition ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue.

4. Dans la mesure où la présente Charte reconnaît des droits fondamentaux tels qu'ils résultent des traditions constitutionnelles communes aux Etats membres, ces droits doivent être interprétés en harmonie avec lesdites traditions.

5. Les dispositions de la présente Charte qui contiennent des principes peuvent être mises en œuvre par des actes législatifs et exécutifs pris par les institutions, organes et organismes de l'Union, et par des actes des Etats membres lorsqu'ils mettent en œuvre le droit de l'Union, dans l'exercice de leurs compétences respectives. Leur invocation devant le juge n'est admise que pour l'interprétation et le contrôle de la légalité de tels actes.

6. Les législations et pratiques nationales doivent être pleinement prises en compte comme précisé dans la présente Charte.

7. Les explications élaborées en vue de guider l'interprétation de la présente Charte sont dûment prises en considération par les juridictions de l'Union et des Etats membres ».

B.15. Comme il ressort du texte de la loi attaquée et des travaux préparatoires cités en B.4.2, le législateur a entendu établir trois catégories de métadonnées devant être conservées - les données d'identification, les données d'accès et de connexion ainsi que les données de communication -, renforcer les conditions d'accès aux données par les autorités compétentes et renforcer la sécurisation des données conservées par les opérateurs, dans l'interprétation des arrêts de la Cour de justice de l'Union européenne et de la Cour selon laquelle une obligation généralisée de conservation des données pourrait être admise si cette obligation s'accompagne de telles garanties.

B.16. L'article 95 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 « relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) », entré en vigueur le

25 mai 2018, dispose que ce règlement n'impose pas d'obligations supplémentaires aux personnes physiques ou morales quant au traitement dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communication dans l'Union en ce qui concerne les aspects pour lesquels elles sont soumises à des obligations spécifiques ayant le même objectif énoncées dans la directive 2002/58/CE.

L'article 15, paragraphe 1, de la directive 2002/58/CE, cité en B.6.1, dispose que les Etats membres peuvent notamment adopter des mesures législatives afin de conserver des données durant une période limitée pour des raisons citées dans ce paragraphe, entre autres sauvegarder la sécurité nationale, la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, aux conditions précisées dans cette disposition.

B.17.1. L'article 126 de la loi du 13 juin 2005 relative aux communications électroniques, inséré par l'article 4 de la loi attaquée, fixe en son paragraphe 2, 2°, les conditions auxquelles les services de renseignement et de sécurité peuvent obtenir des données des fournisseurs et opérateurs visés au paragraphe 1er, alinéa 1er.

A cet égard, il convient de constater que, le 31 octobre 2017, le *Investigatory Powers Tribunal – London* a posé à la Cour de justice de l'Union européenne les questions préjudicielles suivantes (affaire C-623/17 *Privacy International* / *Secretary of State for Foreign and Commonwealth Affairs e.a.*) :

« Dans des circonstances où :

a. les capacités des SSR pour utiliser les DCM qui leur sont fournies sont essentielles pour la protection de la sécurité nationale du Royaume-Uni, notamment dans les domaines du contre-terrorisme, du contre-espionnage et de la lutte contre la prolifération;

b. une caractéristique fondamentale de l'utilisation des DCM par les SSR est la découverte de menaces pour la sécurité nationale inconnues jusque-là par le biais de techniques de masse non-ciblées qui exigent le regroupement des DCM en un endroit unique. Son utilité principale repose dans l'identification et l'établissement du profil rapide des cibles ainsi que la fourniture d'une base d'action au vu d'une menace imminente;

c. le fournisseur d'un réseau de communications électroniques n'est pas tenu de conserver par la suite les DCM (au-delà de la période requise par l'activité commerciale ordinaire) qui sont conservées par l'Etat seul (les SSR);

d. la juridiction nationale a jugé (sous réserve de certaines questions réservées) que les garanties entourant l'utilisation des DCM par les SSR sont conformes aux exigences de la CEDH; et

e. la juridiction nationale a jugé que l'imposition des exigences spécifiées aux points 119 à 125 de l'arrêt de la grande chambre dans les affaires jointes C 203/15 et C 698/15 *Tele2 Sverige AB/Post-och telestyrelsen* et *Secretary of State for the Home Department/Watson e.a* (' les exigences Watson '), si ces dernières étaient applicables, ferait échec aux mesures prises par les SSR pour protéger la sécurité nationale et mettrait par là même en péril la sécurité nationale du Royaume-Uni;

1. Vus l'article 4 TUE et l'article 1er, paragraphe 3, de la directive 2002/58/CE (directive vie privée et communications électroniques), une exigence dans des instructions données par le Secretary of State à un fournisseur d'un réseau de communications électroniques qu'il doit fournir les données de communications en masse aux services de sécurité et de renseignement (' SSR ') d'un Etat membre, relève-t-elle du champ d'application du droit de l'Union et de la directive vie privée et communications électroniques ?

2. En cas de réponse affirmative à la première question, les exigences Watson ou toute autre exigence en plus de celles imposées par la CEDH s'imposent-elles à de telles instructions du Secretary of State ? Si tel est le cas, comment et dans quelle mesure ces exigences s'appliquent-elles, eu égard à la nécessité essentielle pour les SSR d'utiliser l'acquisition de masse et les techniques de traitement automatisé pour protéger la sécurité nationale et eu égard à la mesure dans laquelle de telles capacités, si elles sont conformes à la CEDH, pourraient être fondamentalement frustrées par l'imposition de telles exigences ? ».

La Cour devra faire intervenir la réponse à ces questions préjudicielles dans son examen. Pour cette raison, l'examen de la loi attaquée doit, sur ce point, être suspendu jusqu'à ce que la Cour de justice ait rendu un arrêt dans l'affaire précitée.

B.17.2. L'article 126, § 2, 1°, de la loi du 13 juin 2005 relative aux communications électroniques, inséré par l'article 4 de la loi attaquée, fixe les conditions auxquelles les autorités judiciaires peuvent obtenir des données en vue de la recherche, de l'instruction et de la poursuite d'infractions. Par conséquent, il convient également d'attendre la réponse de la Cour de justice de l'Union européenne à la question préjudicielle suivante, qui a été posée par la *Audiencia provincial de Tarragona, Sección cuarta* le 14 avril 2016 (affaire C-207/16, *Ministerio Fiscal*) :

« Est-il possible de déterminer la gravité suffisante des infractions, en tant que critère justifiant l'atteinte aux droits fondamentaux reconnus aux articles 7 et 8 de la Charte, uniquement en prenant en considération la peine dont peut être punie l'infraction faisant l'objet d'une enquête ou est-il nécessaire, en outre, d'identifier dans le comportement délictueux un caractère préjudiciable particulier pour des intérêts juridiques individuels ou collectifs ?

Le cas échéant, s'il était conforme aux principes fondamentaux de l'Union appliqués par la Cour dans son arrêt Digital Rights en tant que normes de contrôle strict de la directive déclarée invalide par cet arrêt, de déterminer la gravité de l'infraction uniquement en fonction de la peine susceptible d'être infligée, quel devrait être le niveau minimal de cette peine ? Un niveau fixé de manière générale à un minimum de trois ans de prison serait-il conforme ? ».

Il ressort des conclusions de l'avocat général Henrik Saugmandsgaard Øe du 3 mai 2018 dans cette affaire que les dispositions pertinentes sont susceptibles de plusieurs interprétations.

B.18. Pour le surplus, les points de vue des parties devant la Cour divergent quant à l'interprétation à donner à plusieurs dispositions, notamment l'article 15, paragraphe 1, de la directive précitée 2002/58/CE et les articles 7, 8, 11 et 52 de la Charte des droits fondamentaux de l'Union européenne, que la Cour doit associer à son contrôle de la loi attaquée.

B.19.1. Comme l'indiquent les parties requérantes, la Cour de justice a toutefois jugé dans son arrêt du 21 décembre 2016 (C-203/15 et C-698/15 *Tele2 Sverige AB*) que l'article 5, paragraphe 1, de la directive 2002/58/CE énonce une obligation de principe d'assurer la confidentialité des communications et des données relatives au trafic y afférentes, et que l'article 15, paragraphe 1, de la même directive, contenant des exceptions à ce principe, doit être interprété de manière stricte pour éviter que la dérogation à l'obligation de principe prévue à l'article 5 de la directive devienne la règle, sauf à vider largement cette dernière disposition de sa portée.

La Cour de justice a également souligné que seuls les objectifs énoncés par l'article 15 peuvent justifier une mesure dérogeant au principe de confidentialité des communications et données relatives au trafic y afférentes, l'article 15 exigeant à cet égard que la conservation des données n'ait lieu que pendant une durée limitée et lorsque cela est justifié par un des motifs qu'il énumère.

B.19.2. Dès lors, comme le soulignent les parties requérantes, d'après la Cour de justice, une réglementation nationale qui énonce une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique, sans que les utilisateurs en soient informés, constitue une ingérence dans les droits fondamentaux consacrés par les articles 7 et 8 de la Charte particulièrement grave, de sorte que seule la lutte contre la criminalité grave est susceptible de justifier une telle mesure. La Cour de justice ajoute que si cet objectif est d'intérêt général, il ne saurait à lui seul justifier qu'une réglementation nationale prévoyant la conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation soit considérée comme nécessaire aux fins de ladite lutte.

La Cour de justice en conclut qu'une réglementation nationale qui ne prévoit aucune différenciation, limitation ou exception selon l'objectif poursuivi, et qui concerne de manière globale l'ensemble des personnes qui font usage de services de communications électroniques, sans distinction géographique ou dans le temps, sans que l'on ait égard au fait que ces personnes se trouvent même indirectement dans une situation pouvant donner lieu à des poursuites pénales ou que la communication des données concerne des personnes dont les communications sont soumises au secret professionnel ou sans requérir aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique, excède les limites du strict nécessaire et ne peut être considérée comme étant justifiée dans une société démocratique, comme l'exige l'article 15 de la directive, lu à la lumière des articles 7, 8, 11 et 52, paragraphe 1, de la Charte.

B.19.3. Selon les parties requérantes, la Cour de justice indique certes que l'article 15, paragraphe 1, de la directive 2002/58/CE ne s'oppose pas à une réglementation nationale qui permet une conservation ciblée des données relatives au trafic et des données de localisation, à des fins de lutte contre la criminalité grave, à condition que la conservation des données soit, en ce qui concerne les catégories de données à conserver, les moyens de communication visés, les personnes concernées ainsi que la durée de conservation retenue, limitée au strict nécessaire. Ceci implique que la réglementation nationale prévoie des règles claires et précises et que les personnes concernées par la conservation des données jouissent de

garanties suffisantes qui permettent de protéger efficacement leurs données à caractère personnel contre les risques d'abus. La Cour de justice ajoute que la réglementation nationale doit en particulier indiquer en quelles circonstances et sous quelles conditions une mesure de conservation des données peut être prise à titre préventif. Une telle réglementation doit être fondée sur des éléments objectifs qui permettent de viser un public dont les données sont susceptibles de révéler un lien avec la criminalité grave ou qui présente un risque grave pour la sécurité publique, cette délimitation pouvant être assurée au moyen d'un critère géographique lorsque les autorités nationales compétentes considèrent, sur la base d'éléments objectifs, qu'il existe, dans une ou plusieurs zones géographiques, un risque élevé de préparation ou de commission de tels actes.

B.19.4. Comme il ressort des B.3 et B.4, par l'adoption de la loi attaquée, le législateur poursuit des objectifs plus larges que la lutte contre la criminalité grave ou le risque d'atteinte grave à la sécurité publique.

Le législateur a également indiqué à plusieurs reprises dans les travaux préparatoires cités en B.4.2 qu'en ce qui concerne le principe même de l'obligation de conservation des données, il visait toutes les personnes, même si elles ne sont pas encore impliquées dans une enquête; il n'a par ailleurs pas opéré de distinction selon la période temporelle, la zone géographique ou un cercle de personnes, et n'a pas non plus prévu une exception à l'égard des personnes dont les communications sont soumises au secret professionnel.

B.19.5. Selon les parties requérantes, bien que les conditions d'accès aux données conservées aient été considérablement renforcées dans la loi attaquée, l'obligation générale de conservation des données qu'elle prévoit ne répond pas aux exigences prescrites par l'article 15, paragraphe 1, de la directive 2002/58/CE, lu à la lumière des articles 7, 8, 11 et 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, selon l'interprétation qu'en a donnée la Cour de justice par son arrêt du 21 décembre 2016. Une telle obligation excède en effet les limites du strict nécessaire et ne saurait être considérée comme étant justifiée dans une société démocratique, ainsi que l'exigent les dispositions européennes précitées.

B.20.1. Le Conseil des ministres souligne quant à lui que l'objectif poursuivi par la réglementation attaquée est multiple. Le législateur cherche d'abord à renforcer la situation

qui existe de longue date, dans laquelle l'accès à des données dans le secteur des télécommunications est obtenu dans le cadre d'enquêtes pénales, en créant un cadre législatif offrant les garanties nécessaires sur le plan de la protection de la vie privée. L'obligation de conservation est également introduite en vue de la recherche de la vérité dans de nombreuses formes de criminalité et vise ainsi à garantir l'intégrité du système pénal. Cette recherche de la vérité est dans l'intérêt tant de la victime et de l'accusé (qui pourra par exemple démontrer qu'il se trouvait ailleurs au moment des faits) que de toutes les autres personnes concernées. L'obligation de conservation est également dictée par les finalités qui consistent à intervenir en vue de faire suite à un appel aux services d'urgence ou à rechercher une personne disparue dont l'intégrité physique est en danger imminent. Cet élément constituerait une différence importante par rapport aux situations qui étaient évoquées dans les arrêts précités de la Cour de justice. Il existerait donc un lien de proportionnalité entre l'obligation générale de conservation et le but que le législateur s'est fixé.

B.20.2. Le Conseil des ministres souligne encore que le législateur n'a pas considéré qu'il était possible, à la lumière de l'objectif poursuivi, de mettre en place une obligation de conservation ciblée et différenciée, et qu'il a choisi d'entourer l'obligation de conservation générale et indifférenciée de garanties strictes, tant sur le plan de la protection de la conservation que sur le plan de l'accès, afin de limiter au minimum l'ingérence dans le droit à la protection de la vie privée. A cet égard, le Conseil des ministres souligne qu'il est tout simplement impossible d'opérer une différenciation *a priori* en fonction des personnes, des périodes temporelles et des zones géographiques. Il se réfère à cet égard également aux conclusions de l'avocat général Henrik Saugmandsgaard Øe dans les affaires jointes C-203/15 et C-698/15.

Il ressort des éléments dont dispose la Cour que la majorité des Etats membres connaissent par ailleurs de grandes difficultés pour mettre en conformité leur législation en matière de conservation des données avec les exigences émises par la Cour de justice dans sa jurisprudence (voy. : *Data retention across the EU*, http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention; lettre du ministre de la Justice et de la Sécurité des Pays-Bas du 26 mars 2018 au président de la « Tweede Kamer der Staten-Generaal », deuxième chambre, session 2017-2018, 34 537, n° 7).

B.21. Par conséquent, il y a lieu de poser à la Cour de justice de l'Union européenne la question préjudicielle proposée en ordre subsidiaire par le Conseil des ministres, telle qu'elle a été modifiée par la Cour.

B.22. La loi attaquée vise à permettre également une instruction pénale effective et une sanction effective des abus sexuels à l'égard de mineurs et à permettre effectivement l'identification de l'auteur d'un tel délit, même lorsqu'il est fait usage de moyens de communications électroniques. A l'audience, l'attention a été attirée à cet égard sur les obligations positives qui découlent des articles 3 et 8 de la Convention européenne des droits de l'homme en ce qui concerne la protection de l'intégrité physique et morale des mineurs et d'autres personnes vulnérables, tels qu'ils sont interprétés par la Cour européenne des droits de l'homme (CEDH, 2 décembre 2008, *K.U.* c. Finlande, §§ 46-49). Ces obligations pourraient également découler des dispositions correspondantes de la Charte des droits fondamentaux de l'Union européenne, ce qui pourrait avoir des conséquences pour l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58/CE.

B.23. Il convient dès lors de poser la deuxième question préjudicielle mentionnée dans le dispositif.

B.24. Enfin, il y a lieu de poser la troisième question préjudicielle mentionnée dans le dispositif.

Par ces motifs,

la Cour

a) avant de statuer quant au fond, pose à la Cour de justice de l'Union européenne les questions préjudicielles suivantes :

1. L'article 15, paragraphe 1, de la directive 2002/58/CE, lu en combinaison avec le droit à la sécurité, garanti par l'article 6 de la Charte des droits fondamentaux de l'Union européenne, et le droit au respect des données personnelles, tel que garanti par les articles 7, 8 et 52, § 1er, de la Charte des droits fondamentaux de l'Union européenne, doit-il être interprété en ce sens qu'il s'oppose à une réglementation nationale telle que celle en cause, qui prévoit une obligation générale pour les opérateurs et fournisseurs de services de communications électroniques de conserver les données de trafic et de localisation au sens de la directive 2002/58/CE, générées ou traitées par eux dans le cadre de la fourniture de ces services, réglementation nationale qui n'a pas seulement pour objectif la recherche, la détection et la poursuite de faits de criminalité grave, mais également la garantie de la sécurité nationale, de la défense du territoire et de la sécurité publique, la recherche, la détection et la poursuite d'autres faits que ceux de criminalité grave ou la prévention d'un usage interdit des systèmes de communication électronique, ou la réalisation d'un autre objectif identifié par l'article 23, paragraphe 1, du règlement (UE) 2016/679 et qui est en outre sujette à des garanties précisées dans cette réglementation sur le plan de la conservation des données et de l'accès à celles-ci ?

2. L'article 15, paragraphe 1, de la directive 2002/58/CE, combiné avec les articles 4, 7, 8, 11 et 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, doit-il être interprété en ce sens qu'il s'oppose à une réglementation nationale telle celle en cause, qui prévoit une obligation générale pour les opérateurs et fournisseurs de services de communications électroniques de conserver les données de trafic et de localisation au sens de la directive 2002/58/CE, générées ou traitées par eux dans le cadre de la fourniture de ces services, si cette réglementation a notamment pour objet de réaliser les obligations positives incombant à l'autorité en vertu des articles 4 et 8 de la Charte, consistant à prévoir un cadre légal qui permette une enquête pénale effective et une répression effective de l'abus sexuel des mineurs et qui permette effectivement d'identifier l'auteur du délit, même lorsqu'il est fait usage de moyens de communications électroniques ?

3. Si, sur la base des réponses données à la première ou à la deuxième question préjudicielle, la Cour constitutionnelle devait arriver à la conclusion que la loi attaquée méconnaît une ou plusieurs des obligations découlant des dispositions mentionnées dans ces questions, pourrait-elle maintenir provisoirement les effets de la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques afin d'éviter une insécurité juridique et de permettre que les données collectées et conservées précédemment puissent encore être utilisées pour les objectifs visés par la loi ?;

b) suspend en outre l'examen des affaires jusqu'à ce que la Cour de justice ait statué dans les affaires C-207/16 *Ministerio Fiscal* et C-623/17 *Privacy International / Secretary of State for Foreign and Commonwealth Affairs e.a.*

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 19 juillet 2018.

Le greffier, Le président,

P.-Y. Dutilleux J. Spreutels