Cour constitutionnelle

Arrêt n° 97/2024
du 26 septembre 2024
Numéros du rôle : 7907, 7929, 7930, 7931 et 7932

En cause : les recours en annulation totale ou partielle de la loi du 20 juillet 2022 « relative à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités », introduits par l'Ordre des barreaux francophones et germanophone, par l'ASBL « Académie Fiscale » et Jean Pierre Riquet, par l'ASBL « Liga voor Mensenrechten », par l'ASBL « Ligue des droits humains » et par Jens Hermans et autres.

La Cour constitutionnelle,

composée des présidents Pierre Nihoul et Luc Lavrysen, et des juges Thierry Giet, Joséphine Moerman, Michel Pâques, Yasmine Kherbache, Danny Pieters, Sabine de Bethune, Emmanuelle Bribosia, Willem Verrijdt, Kattrin Jadin et Magali Plovie, assistée du greffier Nicolas Dupont, présidée par le président Pierre Nihoul,

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 2 janvier 2023 et parvenue au greffe le 4 janvier 2023, l'Ordre des barreaux francophones et germanophone, assisté et représenté par Me Alexandre Cassart, avocat au barreau de Charleroi, et par Me Jean-François Henrotte, Me Elisabeth Kiehl et Me Eric Lemmens, avocats au barreau de Liège-Huy, a introduit un recours en annulation de la loi du 20 juillet 2022 « relative à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités » (publiée au *Moniteur belge* du 8 août 2022).

b. Par requêtes adressées à la Cour par lettres recommandées à la poste les 3, 6 et 8 février 2023 et parvenues au greffe les 6, 7, 8 et 9 février 2023, des recours en annulation totale ou partielle (articles 2 à 17) de la même loi ont été introduits par l'ASBL « Académie Fiscale » et Jean Pierre Riquet, par l'ASBL « Liga voor Mensenrechten », assistée et représentée par Me Raf Jespers, avocat au barreau d'Anvers, par l'ASBL « Ligue des droits humains », assistée

et représentée par Me Catherine Forget, avocat au barreau de Bruxelles, et par Jens Hermans, la fondation privée « Ministry of Privacy » et Matthias Dobbelaere-Welvaert, assistés et représentés par Me Jan De Groote, avocat au barreau de Termonde.

Ces affaires, inscrites sous les numéros 7907, 7929, 7930, 7931 et 7932 du rôle de la Cour, ont été jointes.

Le Conseil des ministres, assisté et représenté par Me Evrard de Lophem, Me Sébastien Depré et Me Germain Haumont, avocats au barreau de Bruxelles, a introduit des mémoires (dans toutes les affaires), les parties requérantes dans les affaires n^{os} 7907, 7930 et 7931 ont introduit des mémoires en réponse et le Conseil des ministres a également introduit des mémoires en réplique (dans les affaires n^{os} 7907, 7930 et 7931).

Par ordonnance du 28 février 2024, la Cour, après avoir entendu les juges-rapporteurs Thierry Giet et Sabine de Bethune, 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 à l'expiration de ce délai et les affaires seraient mises en délibéré.

À la suite de la demande de la partie requérante dans l'affaire n° 7907 à être entendue, la Cour, par ordonnance du 13 mars 2024, a :

- fixé l'audience au 10 avril 2024;

- invité les parties à lui faire part, dans un mémoire complémentaire à introduire le 5 avril 2024 au plus tard, et dont elles échangeront une copie dans le même délai, leurs observations sur l'incidence de l'arrêt de la Cour européenne des droits de l'homme *Podchasov c. Russie* du 13 février 2024, sur le traitement des présents recours.

Des mémoires complémentaires ont été introduits par :

- la partie requérante dans l'affaire n° 7907;

- la partie requérante dans l'affaire n° 7930;

- les parties requérantes dans l'affaire n° 7932;

- le Conseil des ministres.

À l'audience publique du 10 avril 2024 :

- ont comparu :

. Me Jean-François Henrotte et Me Elisabeth Kiehl, également *loco* Me Eric Lemmens, pour la partie requérante dans l'affaire n° 7907;

. Jean Pierre Riquet, en personne et pour l'ASBL « Académie Fiscale » (parties requérantes dans l'affaire n° 7929);

. Me Raf Jespers, pour la partie requérante dans l'affaire n° 7930;

. Me Catherine Forget, pour la partie requérante dans l'affaire n° 7931;

. Me Jan De Groote, pour les parties requérantes dans l'affaire n° 7932;

. Me Evrard de Lophem, également *loco* Me Sébastien Depré, et Me Germain Haumont, pour le Conseil des ministres;

- les juges-rapporteurs Thierry Giet et Sabine de Bethune ont fait rapport;

- les parties précitées ont été entendues;

- les affaires ont été mises en délibéré.

Par ordonnance du 15 mai 2024, la Cour, après avoir entendu les juges-rapporteurs Thierry Giet et Sabine de Bethune, a décidé :

- de rouvrir les débats;

- d'inviter les parties à lui faire part, dans un mémoire complémentaire à introduire le 30 mai 2024 au plus tard, leurs observations sur l'incidence des arrêts de la Cour de justice de l'Union européenne *La Quadrature du Net e.a.* (Données personnelles et lutte contre la contrefaçon) (C-470/21) et *Procura della Repubblica presso il Tribunale di Bolzano* (C-178/22) du 30 avril 2024 sur le traitement des présents recours et à communiquer dans le même délai aux autres parties, ainsi qu'au greffe de la Cour par courriel envoyé à l'adresse « greffe@const-court.be »;

- de fixer le jour d'une nouvelle audience au 5 juin 2024.

Des mémoires complémentaires ont été introduits par :

- la partie requérante dans l'affaire n° 7907;

- le Conseil des ministres.

A l'audience publique du 5 juin 2024 :

- ont comparu :

. Me Alexandre Cassart, également *loco* Me Jean-François Henrotte, et Me Elisabeth Kiehl, également loco Me Eric Lemmens, pour la partie requérante dans l'affaire n° 7907;

. Me Raf Jespers, également *loco* Me Catherine Forget, pour les parties requérantes dans les affaires n^{os} 7930 et 7931;

. Me Jan De Groote, pour les parties requérantes dans l'affaire n° 7932;

. Me Evrard de Lophem, également *loco* Me Sébastien Depré, pour le Conseil des ministres;

- les juges-rapporteurs Thierry Giet et Sabine de Bethune 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 la recevabilité

En ce qui concerne la position des parties requérantes

Affaire n° 7907

A.1.1. La partie requérante, qui est l'Ordre des barreaux francophones et germanophone, soutient qu'elle dispose de l'intérêt à demander l'annulation des articles 5, 4° et 6°, 8 à 11, 13 à 15, 19, 21, 22, 24 à 42 et 44 de la loi du 20 juillet 2022 « relative à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités » (ci-après : la loi du 20 juillet 2022), au regard des missions qu'elle poursuit en vertu de l'article 495 du Code judiciaire. En effet, les dispositions attaquées portent atteinte au secret professionnel de l'avocat en ce qu'elles permettent notamment de déterminer si un client a consulté un avocat, ainsi que la date et l'heure de cette communication, mais aussi d'identifier l'avocat et ses clients. Or, ces informations sont confidentielles et couvertes par le secret professionnel. La partie requérante ajoute que la Cour, par l'arrêt n° 126/2005 du 13 juillet 2005 (ECLI:BE:GHCC:2005:ARR.126), a reconnu son intérêt à agir pour demander l'annulation de dispositions concernant la profession d'avocat et, par l'arrêt n° 84/2015 du 11 juin 2015 (ECLI:BE:GHCC:2015:ARR.084), confirmé son intérêt à agir en ce qui concerne des dispositions d'une portée analogue à celle des dispositions attaquées.

A.1.2. La partie requérante ajoute que les dispositions attaquées forment un tout indivisible au regard des griefs qu'elle soulève, de sorte que, contrairement à ce que soutient le Conseil des ministres, l'intérêt à agir n'est pas limité à l'article 27, 2°, de la loi du 20 juillet 2022, qui concerne uniquement l'accès aux données protégées et non leur conservation, laquelle est réglée par d'autres dispositions. Par ailleurs, l'article 27, 2°, précité, ne s'applique pas aux communications du client ni aux données détenues par celui-ci, alors que ces informations sont, le cas échéant, couvertes par le secret professionnel. Les autres dispositions de la loi du 20 juillet 2022 s'appliquent donc nécessairement et portent atteinte au secret professionnel, dès lors que cette loi ne fait aucune distinction selon que les données sont couvertes par ce secret ou non. Partant, la partie requérante estime disposer d'un intérêt en ce qui concerne les troisième et quatrième branches du moyen unique, contrairement à ce que soutient le Conseil des ministres. Du reste, par les arrêts n° 57/2021 du 22 avril 2021 (ECLI:BE:GHCC:2021:ARR.057) et n° 96/2018 du 19 juillet 2018 (ECLI:BE:GHCC:2018:ARR.096), la Cour a admis l'intérêt de l'Ordre des barreaux francophones et germanophone dans le cadre de recours en annulation dirigés contre des lois d'une portée très similaire à celle de la loi du 20 juillet 2022. Il n'y a pas lieu, en l'espèce, de se départir de cette jurisprudence.

Affaire n° 7929

A.2. La première partie requérante, l'ASBL « Académie Fiscale », estime disposer d'un intérêt à demander l'annulation des articles 2 à 17 de la loi du 20 juillet 2022, eu égard à son but statutaire, dès lors que ces dispositions sont susceptibles d'affecter directement et défavorablement la situation des comptables-fiscalistes, des experts-comptables et des conseillers fiscaux, ainsi que celle des contribuables défendus par les personnes précitées. En effet, la loi du 20 juillet 2022 porte atteinte au secret professionnel des professionnels comptables et fiscaux en ce que la consultation des métadonnées conservées permet de déterminer si un professionnel comptable et fiscal a été consulté, mais aussi d'identifier ce professionnel, ses clients, les dates et heures de leurs communications. Or, le secret professionnel constitue un principe général qui participe du respect des droits fondamentaux.

Par ailleurs, la seconde partie requérante, qui est une personne physique, est un professionnel qui travaille dans le domaine de la fiscalité et qui est soumis au secret professionnel en vertu de son inscription au registre public des conseillers fiscaux certifiés de l'Institut des conseillers fiscaux et des experts-comptables. À ce titre, elle est directement affectée par les dispositions attaquées qui prévoient des mesures de conservation des données soumises au secret professionnel. La partie requérante se présente également comme un citoyen et un contribuable, de sorte qu'à ce titre, elle estime être directement affectée par les mesures de conservation précitées, dans le cadre de sa relation privée éventuelle avec son avocat.

Affaire n° 7930

A.3. La partie requérante, la « Liga voor Mensenrechten », soutient qu'elle dispose d'un intérêt à demander l'annulation de l'ensemble de la loi du 20 juillet 2022 au regard de son but statutaire, qui consiste à combattre toute injustice et toute atteinte aux droits des personnes ou des communautés, ainsi qu'à défendre les principes d'égalité, de liberté et d'humanisme sur lesquels reposent les sociétés démocratiques, et ce, notamment à travers des actions en justice. À cet égard, elle affirme que la loi du 20 juillet 2022 affecte divers droits fondamentaux en ce qu'elle apporte des modifications à la loi du 13 juin 2005 « relative aux communications électroniques » (ci-après : la loi du 13 juin 2005). Elle relève en outre que la Cour a déjà admis, à plusieurs reprises, son intérêt à agir.

Affaire n° 7931

A.4. La partie requérante, à savoir la « Ligue des droits humains », estime disposer d'un intérêt à demander l'annulation de la loi du 20 juillet 2022 au regard de son but statutaire, qui consiste à combattre l'injustice et toute atteinte arbitraire aux droits d'un individu, ainsi qu'à soutenir toute initiative tendant à la formation et à la promotion des droits et libertés, dès lors que cette loi semble mettre à mal certains droits fondamentaux. Elle relève par ailleurs que la Cour a reconnu à maintes reprises son intérêt à agir, notamment en matière de conservation de données issues de communications électroniques. Par ailleurs, elle soutient poursuivre l'ambition d'éviter que la lutte contre le terrorisme devienne une excuse pour revoir certaines valeurs fondamentales de l'état de droit, tel le principe de la légalité des délits et des peines.

Affaire n° 7932

A.5.1. Les parties requérantes soutiennent que la loi du 20 juillet 2022 revêt une portée générale en ce que la conservation des données qu'elle vise concerne chaque utilisateur d'un service de communications électroniques. En outre, l'utilisation des moyens de communications électroniques est indispensable dans la société, de sorte que tout utilisateur potentiel de tels moyens dispose d'un intérêt à attaquer cette loi. En effet, la Cour a déjà jugé que, dans le cas d'une norme touchant à un aspect essentiel de la liberté du citoyen, il n'est pas nécessaire d'examiner si la situation personnelle des parties requérantes est affectée, l'intérêt étant en toute hypothèse établi.

A.5.2. Plus précisément, les première et troisième parties requérantes se présentent comme des utilisateurs finaux de services de communications électroniques directement concernés par les mesures prévues par la loi du

20 juillet 2022. Or, celles-ci portent atteinte à leur vie privée en raison du risque d'accès non autorisé aux données de communications électroniques conservées et du risque d'utilisation abusive de ces données. Partant, les parties requérantes précitées ont intérêt à demander l'annulation de la loi du 20 juillet 2022 pour mettre fin à la conservation de leurs données personnelles prévue en vertu de cette loi.

A.5.3. La deuxième partie requérante est une personne morale dont le but statutaire est de s'efforcer de sauvegarder la vie privée de chaque citoyen, et notamment de lutter contre le développement d'une société de surveillance par les pouvoirs publics. Dans ce cadre, elle est habilitée à prendre toute mesure pour défendre les droits et libertés fondamentaux consacrés par la Constitution et par la Convention européenne des droits de l'homme. Or, la loi du 20 juillet 2022 vise à autoriser les autorités publiques à s'immiscer dans la vie privée des citoyens, ce qui affecte en tout état de cause le droit garanti par l'article 22 de la Constitution et par l'article 8 de la Convention européenne des droits de l'homme. L'intérêt de la deuxième partie requérante est dès lors conforme à la jurisprudence de la Cour et ne s'apparente pas à une *actio popularis*.

En ce qui concerne la position du Conseil des ministres

A.6. Le Conseil des ministres soutient que le recours dans l'affaire n° 7907 n'est recevable qu'en ce qui concerne l'article 27, 2°, de la loi du 20 juillet 2022. Sous la réserve de certaines exceptions sur lesquelles le recours ne porte pas, cette disposition exclut du champ d'application de la loi du 20 juillet 2022 l'accès à toutes les métadonnées relatives aux moyens de communications détenus par un avocat, pour les communications tant entrantes que sortantes. En revanche, les troisième et quatrième branches du moyen unique portent sur la loi du 20 juillet 2022 dans son ensemble sans établir aucun lien avec le secret professionnel des avocats. Or, selon la jurisprudence de la Cour, l'intérêt de l'Ordre des barreaux francophones et germanophone est limité aux dispositions ayant une incidence sur le droit d'accès à un juge, sur l'administration de la justice et sur l'assistance que les avocats peuvent offrir à leurs clients. Seules les critiques que cette partie formule au sujet de la protection du secret professionnel de l'avocat sont donc recevables.

Quant au fond

En ce qui concerne la position des parties requérantes

Affaire n° 7907

A.7. La partie requérante prend un moyen unique de la violation des articles 10 et 11 de la Constitution, lus en combinaison ou non avec les articles 6 et 8 de la Convention européenne des droits de l'homme et avec les articles 7, 8 et 47 de la Charte des droits fondamentaux de l'Union européenne (ci-après : la Charte). Elle soutient que les dispositions citées au moyen garantissent la protection du secret professionnel de l'avocat, dès lors que celui-ci relève du droit au procès équitable et qu'il constitue une composante essentielle du droit au respect de la vie privée. Elle ajoute que, bien que le secret professionnel de l'avocat ne soit pas intangible, il constitue l'un des principes fondamentaux sur lesquels repose l'organisation de la justice dans une société démocratique. Ce secret porte notamment sur l'existence même de la consultation d'un avocat. Dans ce cadre, les dates et heures auxquelles l'avocat a été consulté sont des données qui revêtent un caractère confidentiel. Il en va de même pour l'agenda professionnel de l'avocat et pour l'identité des clients.

A.8.1. Dans la première branche du moyen unique, la partie requérante soutient que les dispositions attaquées ne différencient pas – ou, à tout le moins, pas suffisamment – les utilisateurs titulaires du secret professionnel par rapport aux autres utilisateurs. En effet, ces dispositions traitent de la même manière l'ensemble des utilisateurs émetteurs de communications électroniques, sans distinguer ceux dont les communications sont protégées par le secret professionnel, comme les clients des avocats. Elles ne tiennent donc pas compte du statut particulier des communications de l'avocat, ni du caractère fondamental du secret professionnel auquel l'avocat est soumis et de la nécessaire relation de confiance qui l'unit à ses clients.

La partie requérante constate que, par son arrêt n° 84/2015, la Cour a jugé que 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 » était disproportionné au regard des articles 7, 8 et 52, paragraphe 1, de la Charte en ce que cette loi s'appliquait sans aucune exception, notamment à

des personnes dont les communications sont soumises au secret professionnel. Par ailleurs, par l'arrêt n° 57/2021, la Cour a annulé l'article 9 de la loi du 29 mai 2016 « relative à la collecte et à la conservation des données dans le secteur des communications électroniques », en ce que cette disposition traitait de la même manière les communications soumises au secret professionnel et les autres communications.

Selon la partie requérante, la loi du 20 juillet 2022 ne permet pas de remédier à l'inconstitutionnalité constatée dans les arrêts précités. Le législateur ne vise en effet que les communications qui émanent de l'avocat et non celles qui émanent du client, alors qu'il s'agit de communications plus préjudiciables pour le secret professionnel dès lors qu'elles indiquent aux autorités le fait que le client a contacté l'avocat ainsi que la localisation et le moment de ce contact. Le législateur permet donc de déterminer concrètement si un avocat a été consulté, d'identifier cet avocat ainsi que ses interlocuteurs, mais aussi la date et les heures de la communication. Ce système porte une atteinte majeure à la confiance nécessaire du client envers son avocat et est de nature à dissuader une personne de faire appel à celui-ci au moyen d'outils de communications électroniques. Le législateur a donc porté atteinte au secret professionnel ainsi qu'aux droits fondamentaux garantis par les dispositions visées au moyen, et ce, en ne distinguant pas utilement les personnes dont les communications sont soumises au secret professionnel, d'une part, et les autres personnes, d'autre part.

A.8.2. Dans la deuxième branche du moyen unique, la partie requérante affirme que la loi du 20 juillet 2022 ne différencie pas – ou pas suffisamment – les données couvertes par le secret professionnel des autres données, alors que la première catégorie de données doit faire l'objet d'un traitement plus spécifique que la seconde.

A.8.3. Contrairement à ce que le Conseil des ministres soutient en ce qui concerne les première et deuxième branches du moyen unique, la partie requérante affirme que le renforcement des règles entourant l'accès aux données conservées ne suffit pas pour justifier la conservation généralisée de ces données. En l'espèce, l'absence de limites et de contrôle en matière de conservation des données, en particulier sous l'angle de la nécessité de préserver le secret professionnel, conduit à considérer que le moyen est fondé. En effet, le secret professionnel de l'avocat porte non seulement sur le contenu des échanges mais aussi sur l'existence même de ceux-ci. Partant, le simple fait de conserver les métadonnées des communications des avocats viole les droits de la défense si l'ingérence que la conservation implique n'est pas acceptable au regard des droits fondamentaux, ce qui est précisément le cas en l'espèce.

En outre, l'interprétation conciliante de l'article 27, 2°, de la loi du 20 juillet 2022, proposée par le Conseil des ministres, selon laquelle cette disposition couvre également les communications qui émanent du client, n'est pas admissible, dès lors que le libellé du texte vise le moyen de communications électroniques d'un avocat. Par ailleurs, dans l'hypothèse de l'interprétation conciliante précitée, les données détenues par un tiers sont conservées et demeurent accessibles sans qu'il soit tenu compte de leur confidentialité, ce qui n'est pas admissible au regard de la grande quantité et de la nature extrêmement large des données récoltées et conservées par des opérateurs tiers.

A.8.4. En ce qui concerne l'absence de proportionnalité de la mesure, la partie requérante ajoute que l'absence de concours actif de l'avocat, évoqué par le Conseil des ministres, tend à confirmer le caractère discriminatoire de la loi du 20 juillet 2022 ainsi que l'atteinte majeure portée au secret professionnel, dès lors qu'un concours actif permet précisément à l'avocat d'assister à la réalisation de la mesure et de faire valoir ses observations, ce qui n'est pas possible en l'espèce.

La partie requérante ajoute que le tri réalisé *a posteriori*, mis également en évidence par le Conseil des ministres, n'apporte pas de réponse satisfaisante, en raison de l'absence d'une procédure spécifique ou d'une norme prescrite à peine de nullité, dès lors que la Cour de cassation admet que toute preuve, même obtenue illégalement, est admissible en matière répressive et en matière civile, sauf dans le cas de la violation d'une règle prescrite à peine de nullité, d'un vice entachant la fiabilité de la preuve ou de la violation du droit à un procès équitable. En réalité, en l'absence de recours préalable et de concours effectif de l'avocat, aucun contrôle n'aura lieu. Dans les faits, même dans l'hypothèse où un élément de preuve couvert par le secret professionnel est écarté, les autorités auront en toute hypothèse pris connaissance au préalable de cet élément. Par ailleurs, la Cour européenne des droits de l'homme a confirmé que le respect du secret professionnel exclut que le juge saisi des poursuites examine et décide lui-même si des éléments sont protégés par ce secret, dès lors qu'une telle méthode mettrait systématiquement à mal le secret professionnel et lui ferait perdre toute substance. En outre, la loi du

20 juillet 2022 ne prévoit rien en matière de restitution ou de suppression des données qui auraient fait l'objet d'un accès irrégulier, contrairement, par exemple, à l'article 90*octies*, § 3, du Code d'instruction criminelle.

A.8.5. La partie requérante ajoute qu'un traitement particulier doit être réservé aux titulaires du secret professionnel, mais aussi aux métadonnées couvertes par celui-ci, dans tous les cas de figure. Il en va d'autant plus ainsi au regard de la nature des métadonnées concernées. Par ailleurs, les dispositions du Code d'instruction criminelle que le Conseil des ministres estime comparables à celles de la loi du 20 juillet 2022 ne sont pas pertinentes en l'espèce car cette loi ne prévoit pas de concours actif de l'avocat, contrairement aux dispositions précitées du Code d'instruction criminelle.

A.9.1. Dans la troisième branche du moyen unique, la partie requérante relève que le législateur a mis en place une obligation d'enregistrement et de conservation de certaines métadonnées consultables par les autorités, en se basant sur un système de taux d'infractions par arrondissement. Un large ensemble de données est donc susceptible d'être collecté, ce qui constitue en réalité une couverture généralisée du territoire et donc de l'ensemble des citoyens. En effet, les moyens de communications électroniques concernés sont tant les services de communications électroniques « classiques », comme la téléphonie, que des services plus récents, comme les services de messagerie en ligne. En outre, aucun élément ne justifie l'obligation généralisée de conservation des données, qui s'étend tant aux justiciables faisant l'objet d'une enquête ou de poursuites qu'aux justiciables ne faisant pas l'objet de telles mesures. Par ailleurs, la loi du 20 juillet 2022 ne précise pas non plus les métadonnées qui servent de manière effective les objectifs de défense de la sécurité publique et ceux de prévention, de recherche, de détection et de poursuite des infractions pénales. En réalité, la loi du 20 juillet 2022 ne modifie pas substantiellement le système antérieur, qui a pourtant été annulé par la Cour. La Cour de justice de l'Union européenne (ci-après : la Cour de justice) estime d'ailleurs qu'une mesure de conservation généralisée et indifférenciée des données constitue une ingérence telle dans les droits fondamentaux des personnes visées qu'elle n'est en principe pas admissible.

A.9.2. Dans la quatrième branche du moyen unique, la partie requérante considère que le système mis en place par la loi du 20 juillet 2022 n'est pas proportionné au but poursuivi par le législateur. En effet, l'accumulation des données conservées en vertu d'une obligation de conservation d'un large ensemble de métadonnées qui couvre *de facto* l'ensemble du territoire permet de réaliser une « carte digitale » très précise de chaque personne. Ce système constitue une ingérence à ce point grave dans les droits fondamentaux qu'elle n'est pas proportionnée au but poursuivi et qu'elle porte par ailleurs une atteinte dévastatrice au secret professionnel de l'avocat. Certes, la loi du 20 juillet 2022 ne prévoit pas l'enregistrement du contenu de la conversation entre l'avocat et son client, mais la prise de connaissance des métadonnées est suffisante pour identifier la consultation de l'avocat en tant que telle et pour tirer certaines conclusions en fonction des circonstances, comme un appel passé quelques minutes après les faits. Or, le secret professionnel de l'avocat a pour objectif de donner à ceux qui exercent cette profession les garanties nécessaires de crédibilité afin que ceux qui s'adressent à un avocat puissent avoir la certitude que les secrets qu'ils confieront à leur conseil ne seront pas dévoilés à des tiers. La mesure attaquée n'est donc aucunement proportionnée au regard du caractère essentiel du secret professionnel précité, dont la Cour a rappelé l'importance, par l'arrêt n° 127/2013 du 26 septembre 2013 (ECLI:BE:GHCC:2013:ARR.127). Le système attaqué a pour conséquence que les justiciables ne pourront jamais consulter un avocat en toute confiance ni avoir la certitude que l'existence et les circonstances de cette consultation ne seront pas révélées aux autorités publiques. Enfin, la partie requérante constate que les travaux préparatoires de la loi du 20 juillet 2022 ne justifient pas l'identité de traitement entre les personnes titulaires du secret professionnel et les autres personnes. Le législateur n'a pas envisagé la mise en place de mesures moins restrictives, comme un tri entre les métadonnées ordinaires et celles qui sont liées à un titulaire du secret professionnel par un mécanisme de filtre à l'entrée, ce qui est pourtant techniquement envisageable.

A.9.3. La partie requérante ajoute, en ce qui concerne les troisième et quatrième branches du moyen unique, que la jurisprudence de la Cour de justice exige la mise en place d'un filtre minimal à l'entrée, indépendamment du dispositif prévu en matière d'accès aux données. Contrairement à ce que soutient le Conseil des ministres, la conservation des données couvertes par le secret professionnel génère une ingérence distincte, indépendamment des limites prévues en ce qui concerne l'accès aux données.

L'établissement, précité, d'un filtre à l'entrée n'est qu'un exemple mettant en évidence le fait que d'autres solutions existent. Or, celles-ci n'ont pas été envisagées, alors que la loi du 20 juillet 2022 porte précisément une

atteinte discriminatoire aux droits fondamentaux garantis par les dispositions citées au moyen. Par ailleurs, les difficultés techniques qui découleraient de la mise en place du filtre précité, mises en évidence par le Conseil des ministres, ne sont pas insurmontables, de sorte que cette mesure est possible en pratique. S'il est vrai qu'il ne revient pas à la Cour de statuer sur l'opportunité d'un dispositif législatif, elle demeure néanmoins compétente pour décider qu'une loi est inconstitutionnelle en l'absence d'un tel dispositif. Or, le filtrage préalable apparaît comme la seule mesure capable d'assurer que la conservation des métadonnées par les opérateurs ne s'applique pas aux données couvertes par le secret professionnel. Si celui-ci est irréalisable, comme le prétend le Conseil des ministres, cela signifie que l'ingérence prévue par la loi du 20 juillet 2022 est en tout état de cause disproportionnée.

Par ailleurs, selon la partie requérante, les autres obstacles invoqués par le Conseil des ministres en ce qui concerne le mécanisme de filtrage ne sont pas convaincants. En particulier, ce système ne pourrait être considéré comme octroyant un privilège à l'avocat. En effet, le secret professionnel est une garantie fondamentale pour le justiciable dans un État démocratique. Les avocats sont tenus de respecter ce secret sous peine de sanctions pénales et déontologiques. La levée du secret ne se conçoit d'ailleurs qu'en vertu de l'état de nécessité ou d'un conflit avec une valeur supérieure. Cette dérogation ne s'opère que dans la mesure nécessaire à la défense des droits respectifs des parties à la cause. Le fait que certains avocats sont susceptibles de commettre eux-mêmes des infractions ne modifie en rien ces constats, dès lors que l'avocat ne peut se retrancher derrière sa profession pour bénéficier d'une impunité. En outre, le fait qu'une personne malintentionnée puisse détourner les moyens de communication d'un avocat, ce que soulève également le Conseil des ministres, renvoie à un cas de figure exceptionnel qui ne justifie aucunement la mesure attaquée.

Affaire n° 7929

A.10.1. Les parties requérantes prennent un moyen unique de la violation des articles 10 et 11 de la Constitution, lus en combinaison ou non avec les articles 6 et 8 de la Convention européenne des droits de l'homme et avec les articles 7, 8, 11 et 47 de la Charte. Selon elles, les dispositions attaquées traitent de la même manière les utilisateurs de services de télécommunications ou de communications électroniques qui sont soumis au secret professionnel, dont les professionnels comptables et fiscaux, et les autres utilisateurs de ces services, sans tenir compte du statut particulier des professionnels précités, du caractère fondamental du secret professionnel auquel ceux-ci sont soumis ni de la nécessaire relation de confiance avec leurs clients. Par ailleurs, les dispositions attaquées traitent également de la même manière, d'une part, les justiciables qui font l'objet de mesures d'enquête et de poursuite pour des faits susceptibles de relever des finalités définies pour la conservation des données électroniques litigieuses et, d'autre part, ceux qui ne font pas l'objet de telles mesures.

A.10.2. Les parties requérantes relèvent que les travaux préparatoires de la loi du 20 juillet 2022 indiquent que celle-ci a pour objet de transposer partiellement la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 « sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE » (ci-après : la directive 2006/24/CE) et 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 (directive vie privée et communications électroniques) » (ci-après : la directive 2002/58/CE). Cependant, selon les parties requérantes, les obligations de conservation prévues par la loi du 20 juillet 2022 sont excessives par rapport aux objectifs poursuivis par le législateur, dès lors qu'aucune garantie n'est prévue en ce qui concerne les données relatives aux experts-comptables et aux conseillers fiscaux alors que celles-ci sont confidentielles et couvertes par le secret professionnel. En effet, la loi du 20 juillet 2022 ne remplit pas les conditions admises par la Cour de justice quant aux exceptions à l'interdiction de la conservation généralisée des données. Les parties requérantes relèvent en outre que, bien que la loi du 20 juillet 2022 n'autorise pas, sauf exception, la conservation de données divulguant le contenu des communications, elle admet la prise de connaissance de métadonnées qui sont susceptibles de révéler la consultation d'un professionnel comptable et fiscal, et qui sont de nature à permettre de tirer certaines conclusions en fonction des circonstances.

Selon les parties requérantes, la raison d'être du secret professionnel des professionnels comptables est d'intérêt général et vise à donner à ceux qui exercent cette profession les garanties de crédibilité nécessaires pour que ceux qui s'adressent à eux aient la certitude que les secrets confiés ne seront pas dévoilés à des tiers. Or, la loi du 20 juillet 2022 porte atteinte à cette garantie alors que rien ne permet de justifier l'identité de traitement entre tous les utilisateurs des services de communications, parmi lesquels ceux qui sont soumis au secret professionnel. Les parties requérantes relèvent que des poursuites pénales pourraient être introduites par les autorités compétentes sur la base des données confidentielles récoltées en vertu de la loi du 20 juillet 2022 sans qu'un contrôle juridictionnel soit prévu aux divers stades de la procédure, ce qui n'est pas conforme à l'article 6 de la Convention européenne des droits de l'homme ni à l'article 47 de la Charte. Par ailleurs, en ce qui concerne l'identité de traitement précitée entre les justiciables, les parties requérantes soutiennent qu'il existe un risque non négligeable que les bases de données soient gérées avec légèreté par les opérateurs réticents face aux coûts engendrés par les obligations découlant de la loi du 20 juillet 2022.

A.10.3. Les parties requérantes relèvent que l'article 13 de la loi du 20 juillet 2022 est formulé en des termes généraux qui ne permettent pas d'identifier l'ensemble des autorités visées par cette disposition. Celles-ci seront vraisemblablement identifiées par une circulaire ministérielle. Par ailleurs, la loi du 20 juillet 2022 ne prévoit pas de garantie en ce qui concerne les données confidentielles couvertes par le secret professionnel des experts-comptables et fiscalistes, mais elle se limite à confier au Roi le soin de fixer les mesures techniques et administratives que les opérateurs concernés devront prendre pour garantir la protection des données conservées. En outre, d'un point de vue technique, il est possible de faire le tri, par un mécanisme de filtre à l'entrée, entre les métadonnées ordinaires et celles qui sont liées à un titulaire du secret professionnel.

Selon les parties requérantes, la Cour de justice estime que l'article 15 de la directive 2002/58/CE 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 à localisation de tous les abonnés et utilisateurs, pour tous les moyens de communications électroniques. Cette disposition impose par ailleurs un contrôle préalable par une juridiction ou par une autorité administrative indépendante, ainsi qu'une conservation des données sur le territoire de l'Union. Les parties requérantes constatent du reste que la Cour de justice a jugé que la directive 2006/24/CE était incompatible avec le principe de proportionnalité, de sorte qu'une réglementation nationale ne peut pas avoir le même contenu que celle-ci, ce qui démontre le caractère discriminatoire de la loi du 20 juillet 2022.

A.10.4. Les parties requérantes ajoutent que l'obligation de conservation des données prévue par la loi du 20 juillet 2022 relève du champ d'application du droit au respect de la vie privée et de la liberté d'expression, garantis par les articles 7, 8 et 11 de la Charte. À cet égard, la Cour de justice estime que l'article 15 de la directive 2002/58/CE, lu à la lumière des dispositions précitées de la Charte, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale permettant à une autorité étatique d'imposer, aux fins de la sauvegarde de la sécurité nationale, aux fournisseurs de services de communications électroniques la transmission généralisée et indifférenciée des données relatives au trafic et à la localisation vers les services de sécurité et de renseignement. Certes, la loi du 20 juillet 2022 prévoit une conservation d'une durée limitée à douze mois, mais rien ne justifie en l'espèce de viser l'ensemble des personnes sans opérer une distinction lorsque les données sont couvertes par le secret professionnel. La circonstance que les données conservées peuvent, le cas échéant, ne pas être utilisées par la suite est également sans pertinence, dès lors que l'accès aux données constitue une ingérence distincte dans les droits fondamentaux. Par ailleurs, les données relatives au trafic et à la localisation sont susceptibles de révéler des informations sur un nombre important d'aspects de la vie privée des personnes concernées, comme l'orientation sexuelle, les opinions politiques, les convictions religieuses ou encore l'état de santé. Prises dans leur ensemble, ces données donnent des indications très précises sur les personnes dont les données ont été conservées et permettent dès lors d'établir leur profil.

A.10.5. Les parties requérantes relèvent que la conservation des données relatives au trafic et à la localisation à des fins policières est susceptible, à elle seule, de porter atteinte au droit garanti par l'article 7 de la Charte et d'entraîner des effets dissuasifs sur les utilisateurs en ce qui concerne l'utilisation de leurs moyens de communications électroniques, ce qui constitue une ingérence dans la liberté d'expression garantie par l'article 11 de la Charte. Ces effets dissuasifs affectent en particulier les personnes dont les communications sont soumises au secret professionnel ainsi que les lanceurs d'alertes. Par ailleurs, la quantité importante de données relatives au trafic et à la localisation susceptibles de révéler des informations sensibles, collectée en vertu d'une mesure de

conservation généralisée et indifférenciée, comporte des risques d'abus et d'accès illicite. La Cour de justice impose dans ce cadre que la conservation des données relatives aux communications électroniques soit l'exception et non la règle. Elle doit en outre être soumise à des règles claires et précises, et respecter par ailleurs des exigences minimales. L'ingérence doit se limiter au strict nécessaire et respecter le principe de proportionnalité. En toute hypothèse, l'objectif de lutter contre la criminalité grave n'est pas de nature à justifier une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et à la localisation telle qu'elle est prévue par la loi du 20 juillet 2022. En effet, bien que cette loi prévoie la création de zones en fonction du taux de criminalité, elle ne précise pas comment le comptage des infractions est réalisé. Par ailleurs, cette loi ne se limite pas à viser des situations ponctuelles liées à une menace grave et effective pour la sécurité nationale. Elle ne prévoit pas non plus un régime spécifique pour les personnes soumises au secret professionnel ni pour celles qui font l'objet d'une enquête.

Affaire n° 7930

A.11.1. La partie requérante prend un premier moyen de la violation des articles 11, 12, 22 et 29 de la Constitution, et des articles 5, 6, 9 et 15, paragraphe 1, de la directive 2002/58/CE, lus à la lumière des articles 7, 8, 11, 47 et 52, paragraphe 1, de la Charte, de la violation des articles 6, 8, 10, 11 et 18 de la Convention européenne des droits de l'homme et des articles 13 et 54 de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 « relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil » (ci-après : la directive (UE) 2016/680). Elle soutient que les articles 5, 6, 8, 9, 10, 11, 12 et 13 de la loi du 20 juillet 2022 sont des mesures qui instaurent *de iure* et *de facto* une obligation généralisée de conservation des données de communications, ainsi qu'un accès très large aux données conservées.

Selon la partie requérante, les dispositions précitées de la loi du 20 juillet 2022 ne sont pas conformes à la jurisprudence de la Cour de justice qui est applicable en la matière. En effet, celles-ci visent une cinquantaine de types de données différentes qui constituent la majorité des données de trafic et de localisation. L'article 11 de cette loi détermine cinq zones géographiques dans lesquelles les données doivent être conservées par les opérateurs sous certaines conditions, ce qui aboutit *de facto* à ce que l'ensemble du territoire belge puisse tomber sous le coup de l'obligation de conservation, et ce, pendant des périodes longues ou indéterminées. L'article 13 de cette loi détermine quant à lui dix autorités qui, sous certaines conditions, peuvent obtenir un accès aux données conservées par les opérateurs. Il s'agit d'un nombre très important d'autorités, dont la plupart sortent du cadre des objectifs de l'article 15, paragraphe 1, de la directive 2002/58/CE. Parmi ces autorités, on retrouve certaines autorités compétentes pour la prévention, la recherche, la détection ou la poursuite de faits qui constituent une simple infraction pénale, sans que ces faits relèvent de la criminalité grave.

A.11.2. La partie requérante ajoute que la loi du 20 juillet 2022 doit être examinée dans son intégralité, dès lors que c'est l'ensemble de cette loi qui viole les principes dégagés par la jurisprudence de la Cour de justice, tant du point de vue de la conservation des données que de l'accès à celles-ci. En effet, le caractère général des mesures viole le principe de proportionnalité, dès lors que toutes les données de trafic et de localisation sont conservées, que pratiquement l'ensemble du territoire tombe sous l'obligation de conservation et qu'un large groupe d'autorités peut accéder aux données, ce qui va à l'encontre des objectifs poursuivis par l'article 15, paragraphe 1, de la directive 2002/58/CE. En réalité, la loi du 20 juillet 2022 instaure une conservation généralisée et indifférenciée des données.

Selon la partie requérante, les conditions exceptionnelles dans lesquelles la Cour de justice autorise une conservation généralisée et indifférenciée des données ne sont pas remplies par la loi du 20 juillet 2022. En effet, la conservation des données dans le cadre de la sécurité nationale sur la base du niveau de menace déterminé par l'Organe de coordination pour l'analyse de la menace (ci-après : l'OCAM) ne prévoit pas le moindre contrôle par une juridiction ou par une autorité administrative indépendante et établit des délais dont la durée n'apparaît pas, en l'espèce, comme étant nécessaire. En outre, les dispositions relatives à la conservation des données dans le cadre de la criminalité grave visent des infractions qui ne relèvent pas de ce type de criminalité. La notion même de criminalité grave est définie de manière trop large en ce qui concerne l'accès aux données par les autorités compétentes pour la prévention, la recherche, la détection ou la poursuite, par rapport à la définition de criminalité grave pour la conservation des données. En effet, alors que, pour la conservation des données, l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle est visé, l'accès aux données renvoie quant à lui l'article 88*bis*, § 1er, du

Code d'instruction criminelle ainsi qu'aux infractions relatives aux abus de marché, qui présentent un seuil de peine beaucoup plus faible que l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle.

A.11.3. La partie requérante ajoute, en ce qui concerne la proportionnalité de la conservation des données, que contrairement à ce que soutient le Conseil des ministres, la conservation d'un grand nombre de données est prévue non seulement par l'article 8 de la loi du 20 juillet 2022, mais également par les articles 5 et 12 de cette loi. Il ressort de ces dispositions qu'il est possible de conserver des données d'identification sans que cela s'avère nécessaire ou strictement limité. En outre, l'article 8 de la loi du 20 juillet 2022 n'est pas compatible avec la jurisprudence de la Cour de justice en ce qu'il porte sur d'autres données que l'adresse IP et les données civiles de l'utilisateur, comme la section de législation du Conseil d'État l'a mis en évidence. De surcroît, les données concernées ne présentent pas de lien avec les finalités de sauvegarde de la sécurité nationale, de lutte contre la criminalité grave et de prévention des menaces graves pour la sécurité publique. La partie requérante souligne par ailleurs que le nombre important de données visées ne saurait être justifié par une nécessité technique. Elle attire en outre l'attention sur le fait que la conservation des données, d'une part, et l'accès aux donnés, d'autre part, constituent des ingérences différentes, de sorte qu'une conservation généralisée de données ne peut être justifiée à l'aide des garanties relatives à l'accès à ces données. Enfin, l'ingérence dans le droit au respect de la vie privée doit être examinée à l'aune de l'identification concrète des personnes concernées et non du point de vue général et abstrait des technologies disponibles.

A.12.1. Un deuxième moyen est pris de la violation des articles 11, 12, 22 et 29 de la Constitution, de l'article 15, paragraphe 1, et des articles 5, 6 et 9 de la directive 2002/58/CE, lus à la lumière des articles 7, 8, 11, 47 et 52, paragraphe 1, de la Charte, de la violation des articles 6, 8, 10, 11 et 18 de la Convention européenne des droits de l'homme et des articles 13 et 54 de la directive (UE) 2016/680. La partie requérante soutient que les articles 5, 6, 8, 9, 10 et 12 de la loi du 20 juillet 2022, qui portent sur les données que les opérateurs sont tenus de conserver, violent les principes de proportionnalité et de nécessité en ce qui concerne le nombre et les catégories de données visées. La partie requérante précise que les dispositions précitées de la loi du 20 juillet 2022 permettent de tirer des conclusions très précises sur la vie privée des personnes visées, notamment sur les habitudes de la vie quotidienne, le lieu de résidence ou encore les relations sociales, ce qui permet d'établir le profil de ces personnes. La loi du 20 juillet 2022 entraîne la conservation d'un grand nombre de données de catégories diverses, ce qui entraîne en soi la violation de l'article 22 de la Constitution et des articles 7 et 8 de la Charte, dès lors que la vie privée des citoyens n'est plus protégée.

Par ailleurs, les articles 5, 6, 8, 9, 10 et 12 de la loi du 20 juillet 2022 visent un ensemble de données trop large au regard de la jurisprudence de la Cour de justice et prévoient des délais de conservation trop longs. De surcroît, aucune profession n'est exemptée de la conservation des données, pas même les médecins, les avocats ou les journalistes. En outre, l'obligation de conservation qui incombe aux opérateurs porte sur la quasi-totalité des données et permet d'identifier avec précision les communications concernées. La conservation de ces données concerne presque toute la population, sans que celle-ci se trouve nécessairement dans une situation donnant lieu à des poursuites pénales. Autrement dit, la loi du 20 juillet 2022 impose la conservation, sans motif, généralisée et indifférenciée d'un point de vue personnel, temporel et géographique, de l'essentiel des données de trafic et de localisation.

À cet égard, l'article 8 de la loi du 20 juillet 2022 n'impose pas de mentionner le fondement de la conservation, contrairement aux articles 5 et 6 de cette loi. La partie requérante ajoute que les données visées peuvent être demandées par les autorités sans que cet accès ait nécessairement un lien avec l'objectif mentionné. En ce qui concerne la conservation des données dans les zones géographiques, l'article 9 de la loi du 20 juillet 2022 mentionne comme objectifs la sauvegarde de la sécurité nationale, la lutte contre la criminalité grave, la prévention de menaces graves contre la sécurité publique ainsi que la sauvegarde des intérêts vitaux d'une personne physique. Cependant, ce même article 9 précise aussi que les zones géographiques ne peuvent être incluses que dans le but de sauvegarder la sécurité nationale ou en cas de risque élevé de criminalité grave, ce qui est contradictoire. L'article 11, quant à lui, prévoit une obligation de conservation susceptible de couvrir l'ensemble du territoire.

A.12.2. La partie requérante rappelle que l'Autorité de protection des données a souligné que la loi du 20 juillet 2022 revient dans les faits à une obligation de conservation généralisée et indifférenciée des données à des fins de lutte contre la criminalité. En outre, cette Autorité s'est interrogée sur la nécessité de l'obligation de conservation préventive et systématique des données prévue à l'article 5 de cette loi. Selon la partie requérante, les remarques de l'Autorité de protection des données sont aussi pertinentes en ce qui concerne l'obligation de

conserver systématiquement les données de trafic de tous les utilisateurs des moyens de communications électroniques et la possibilité de traiter des données de localisation autres que les données de trafic pour assurer la sécurité et le bon fonctionnement du réseau ou du service ou pour détecter ou analyser les fraudes ou l'utilisation malveillante du réseau. Les articles 6, 8 et 9 de la loi du 20 juillet 2022 précisent qu'ils s'appliquent sans préjudice 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) » (ci-après : le RGPD) et de la loi du 30 juillet 2018 « relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel » (ci-après : la loi du 30 juillet 2018). Selon la partie requérante, cette affirmation ne suffit pas à garantir le respect du RGPD.

A.12.3. Si l'obligation de conservation exclut formellement le contenu de la communication, la partie requérante observe que la Cour de justice a jugé que la conservation de catégories de données très précises permettant d'établir le profil des personnes visées, comme c'est le cas de celles qui sont visées par la loi du 20 juillet 2022, n'était pas admissible. En ce qui concerne, en particulier, la conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs ainsi que des adresses IP, la partie requérante affirme qu'une telle conservation est autorisée en vue de la sauvegarde de la sécurité nationale, et uniquement aux fins de lutter contre la criminalité grave et de prévenir les menaces graves contre la sécurité publique, pourvu que cette possibilité soit soumise au strict respect de conditions matérielles et procédurales, que la durée de conservation n'excède pas celle qui est strictement nécessaire au regard de l'objectif poursuivi et que la mesure prévoie des conditions et des garanties strictes quant à l'utilisation des données.

Dans ce cadre, la partie requérante observe que l'article 8 de la loi du 20 juillet 2022 prévoit de manière générale l'obligation de conserver le numéro de registre national, les données de l'identifiant ainsi que l'adresse IP ayant servi lors de la souscription ou de l'activation des services de communications électroniques. Il ne précise pas le cadre dans lequel ces données doivent être conservées, contrairement à ce qui est prévu à l'article 5 de cette loi. Ces données sont conservées jusqu'à douze mois après la fin du service. L'article 9 de la loi du 20 juillet 2022, lui, dispose que, pour les zones géographiques, les données visées à l'article 10, notamment les données d'identification et l'adresse IP, font l'objet d'une conservation. Ce n'est que dans l'article 9 qu'il est précisé que les finalités sont la sauvegarde de la sécurité nationale, la lutte contre la criminalité grave, la prévention de menaces graves contre la sécurité publique et la sauvegarde des intérêts vitaux d'une personne physique. Enfin, l'article 12 impose la conservation d'un large éventail de données d'identification. La partie requérante allègue que ce système n'est pas conforme aux exigences de la Cour de justice, dès lors que la finalité de la conservation dépasse largement les seules fins de sécurité nationale, de criminalité grave et de prévention de menaces graves contre la sécurité publique. En effet, les dispositions précitées de la loi du 20 juillet 2022 n'offrent aucun fondement à la conservation ni ne prévoient un fondement qui consiste en la sécurité du réseau ou en la sauvegarde des intérêts vitaux d'une personne physique. Seul l'article 9 de la loi définit un certain cadre. Par ailleurs, aucune disposition ne prévoit des conditions matérielles et procédurales régissant l'utilisation des données visées.

A.12.4. La partie requérante formule des observations complémentaires au sujet de la finalité de lutte contre la fraude et l'utilisation malveillante de réseaux, d'une part, et concernant la finalité de préservation de la sécurité et de bon fonctionnement du réseau, d'autre part. Elle soutient que l'article 5 de la loi du 20 juillet 2022 établit clairement une distinction entre ces finalités et que cette disposition instaure une conservation généralisée des données de trafic des utilisateurs. Par ailleurs, aucun contrôle de nécessité n'est prévu en ce qui concerne la conservation des données.

En ce qui concerne, plus précisément, la responsabilité déléguée aux opérateurs pour qu'ils conservent les données de trafic nécessaires pour assurer la sécurité et le bon fonctionnement des réseaux et des services, la partie requérante soutient que cette finalité n'est pas mentionnée à l'article 23 du RGPD, de sorte que la mesure n'est pas admissible. Dans ce cadre, l'article 6, paragraphe 1, *f)*, du RGPD ne peut pas être invoqué. Enfin, à supposer que cette mesure trouve une justification dans l'article 15, paragraphe 1, de la directive 2002/58/CE, l'article 5 de la loi du 20 juillet 2022 aboutirait à une conservation générale de données qui est incompatible avec l'article 6, paragraphes 1 et 2, du Traité sur l'Union européenne.

A.13.1. La partie requérante prend un troisième moyen de la violation des articles 11, 12, 22 et 29 de la Constitution, de l'article 15, paragraphe 1, et des articles 5, 6 et 9 de la directive 2002/58/CE, lus à la lumière des articles 7, 8, 11, 47 et 52, paragraphe 1, de la Charte, de la violation des articles 6, 8, 10, 11 et 18 de la Convention

européenne des droits de l'homme et des articles 13 et 54 de la directive (UE) 2016/680. Elle soutient que les articles 10 et 11 de la loi du 20 juillet 2022 imposent aux opérateurs de conserver certaines données dans cinq zones bien déterminées, ce qui aboutit dans les faits à une conservation généralisée indifférenciée de la majeure partie des données de trafic et de localisation, pour une période qui n'est pas systématiquement déterminée par la loi mais qui doit notamment être précisée par arrêté royal. L'article 10 de la loi du 20 juillet 2022, en particulier, aboutit à la conservation des données de localisation appartenant à des personnes qui ne se trouvent pas dans la zone géographique pour laquelle les données doivent être conservées.

A.13.2. La partie requérante précise que l'article 11 de la loi du 20 juillet 2022 prévoit que les données visées sont conservées soit pour une période de six à douze mois, soit pour une période non déterminée par la loi, soit pour une période à déterminer par arrêté royal. Selon elle, l'article 11 ne remplit dès lors pas la condition de période limitée au strict nécessaire imposée par la Cour de justice. Tout d'abord, les délais de conservation de six à douze mois sont d'une durée telle qu'ils permettent de fournir des informations précises sur la vie privée de l'utilisateur du moyen de communications électroniques. Ensuite, en ce qui concerne les zones déterminées par l'OCAM, l'obligation de conservation généralisée s'applique à l'ensemble du territoire dès que cet organe évalue le niveau de la menace au niveau 3 pour l'ensemble du territoire. Dans cette hypothèse, l'obligation de conservation doit être confirmée par arrêté royal, étant entendu qu'en l'absence de confirmation, il est mis fin à la conservation des données. Le délai de conservation n'est donc pas très clair. Enfin, aucun délai n'est prévu pour les zones visées à l'article 126/3, §§ 3 à 5, de la loi du 13 juin 2005, tel qu'il a été inséré par l'article 11 de la loi du 20 juillet 2022. En ce qui concerne ces dernières, le législateur a uniquement prévu que le délai de conservation est fixé par arrêté royal, sans fixer de délai minimum ou maximum. Partant, l'article 11 de la loi du 20 juillet 2022 ne répond pas à la condition dégagée par la Cour de justice selon laquelle la conservation des données est subordonnée au respect de conditions matérielles et procédurales énoncées par des règles claires et précises.

A.13.3. En ce qui concerne les zones géographiques organisées autour du taux de criminalité prévu à l'article 11 de la loi du 20 juillet 2022, la partie requérante soutient que la nécessité de la mesure n'est pas démontrée. En effet, les travaux préparatoires de cette loi attestent du fait qu'il n'existe aucune donnée précise quant aux répercussions de la conservation des données sur la lutte contre la criminalité grave. En outre, la mesure prévue à l'article 11 de la loi du 20 juillet 2022 n'est pas liée à des lieux stratégiques ou à des lieux fréquentés par un nombre élevé de personnes, mais uniquement aux chiffres de la criminalité. Une situation permanente est créée, dès lors que la liste des zones est établie annuellement. Par ailleurs, le taux de criminalité lié aux infractions de la zone est faible, de sorte que le critère retenu est trop large. La mesure en elle-même affecte la grande majorité des citoyens qui ne sont pas concernés par des infractions pénales. Selon la partie requérante, le faible taux de criminalité retenu à l'article 11 de la loi du 20 juillet 2022 ne permet pas de déduire un risque d'infractions élevé, même compte tenu de la nature des infractions visées. Partant, la mesure n'est pas proportionnée et elle s'avère incompatible avec les droits fondamentaux des citoyens, comme cela ressort d'ailleurs des travaux préparatoires de la loi du 20 juillet 2022, qui attestent en outre du fait que le législateur est dans l'impossibilité de préciser les pourcentages du territoire et de la population qui sont effectivement visés.

La partie requérante relève que le critère retenu par le législateur est celui des infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle. En raison du grand nombre d'infractions visés dans cette disposition, le critère précité apparaît comme étant trop large pour déterminer les infractions à retenir dans le cadre de la conservation des données. Selon la partie requérante, la compétence du juge d'instruction dans le cadre de l'article 90*ter* du Code d'instruction criminelle ne permet pas de justifier la mesure de conservation des données qui est attaquée, laquelle apparaît comme une mesure de conservation généralisée incompatible avec le caractère exceptionnel et subsidiaire d'une méthode d'ingérence dans les droits fondamentaux garantis par les articles 7 et 8 de la Charte ainsi que par l'article 22 de la Constitution dans le cadre de la lutte contre la criminalité grave. La partie requérante précise que l'ensemble des infractions visées par l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle ne relèvent pas toutes de la notion de criminalité grave, dès lors que certaines de ces infractions sont punies d'un emprisonnement de trois mois à deux ans. Par ailleurs, la liste figurant à l'article 90*ter* du Code d'instruction criminelle a été conçue pour délimiter la compétence spécifique du juge d'instruction et non pour définir la criminalité grave dans le cadre de la protection des données, ce qui n'est pas compatible avec la jurisprudence de la Cour de justice. En outre, la notion de criminalité grave en soi n'est pas précisée en droit pénal. Le critère retenu ne fait par ailleurs aucune distinction entre les poursuites, la condamnation, l'absence de poursuite et le classement sans suite. Du reste, il y a lieu de relever que la notion d'infraction grave ne peut être interprétée de manière excessivement large par les États membres de l'Union européenne.

A.13.4. La partie requérante conteste l'affirmation selon laquelle les constatations prévues du nombre d'infractions peuvent se faire de manière scientifique et objective sur la base des données statistiques visées par la loi du 20 juillet 2022, dès lors que la banque de donnée désignée par le législateur n'a pas été créée à cette fin. Cette banque de données contient un grand nombre d'informations qui sont simplement en lien avec des infractions, notamment les données des victimes, les signalements d'infractions justifiés ou non, ainsi que des faits ayant mené à une déclaration de culpabilité. Autrement dit, le législateur ne vise pas uniquement les faits portés devant le juge et ayant abouti à une condamnation, alors que c'est pourtant le nombre d'infractions effectivement commises qui détermine s'il peut être procédé à la conservation des données dans un arrondissement déterminé. Du reste, l'Autorité de protection des données a mis en doute, dans le cadre de son avis sur la loi du 20 juillet 2022, la pertinence du recours à cette banque de données.

Contrairement à ce que soutient le Conseil des ministres, la partie requérante affirme qu'il n'est pas nécessaire de mettre en évidence une solution de remplacement en ce qui concerne la banque de données retenue par le législateur pour démontrer l'absence de pertinence de cette dernière. En toute hypothèse, il serait souhaitable que la loi du 20 juillet 2022 vise une banque de données spécifique, compte tenu de l'incidence considérable qu'elle exerce sur le droit au respect de la vie privée, et que cette banque de données repose sur des affaires dont le parquet ou les tribunaux ont été effectivement saisis à des fins de poursuites.

A.13.5. En ce qui concerne la conservation des données dans le cadre d'une menace de niveau 3, également prévue à l'article 11 de la loi du 20 juillet 2022, la partie requérante soutient que les exigences dégagées par la Cour de justice sont violées. En effet, aucun contrôle juridictionnel et effectif pour vérifier l'établissement d'un tel niveau n'est prévu. Par ailleurs, si le niveau 4 de la menace correspond à une menace sérieuse et imminente, il y a lieu de constater que le niveau 3 n'atteint pas ce seuil de gravité, de sorte que ce dernier niveau ne répond pas à la notion de « menace pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible » consacrée par la jurisprudence de la Cour de justice. En outre, l'article 11 de la loi du 20 juillet 2022 ne répond pas à la condition selon laquelle la mesure de conservation des données ne peut être imposée que pour une période limitée au strict nécessaire. Du reste, l'article 11 ne précise pas la manière dont il est mis fin à cette mesure, excepté en ce qui concerne la fin automatique d'une mesure couvrant l'ensemble du territoire en l'absence d'arrêté royal de confirmation.

A.13.6. L'article 11 de la loi du 20 juillet 2022 vise par ailleurs trois zones, insérées à l'article 126/3, § 3 à 5, de la loi du 13 juin 2005, qu'il distingue sur la base de la nature de la menace à laquelle elles sont susceptibles d'être exposées. Selon la partie requérante, le nombre de lieux et d'infrastructures pour lesquels des données doivent être conservées dans le cadre de ces zones est élevé au point qu'est visée la quasi-totalité du territoire belge, ce qui aboutit à une conservation généralisée et indifférenciée des données de l'ensemble de la population. En outre, le périmètre des zones n'est pas déterminé par la loi mais par un arrêté royal, le législateur n'ayant pas prévu de périmètre maximum ni minimum. Du reste, l'Autorité de protection des données a mis en évidence que l'article 11 de la loi du 20 juillet 2022 vise des lieux qui ne sont pas uniquement caractérisés par un risque élevé de préparation ou de commission d'actes de criminalité grave, comme l'exige la jurisprudence de la Cour de justice.

En ce qui concerne la conservation *de facto* généralisée de données, visée à l'article 11 de la loi du 20 juillet 2022, la partie requérante précise que cette disposition prévoit la conservation de données dans les communes comportant des infrastructures critiques. Dans les faits, cette mesure vise les données de toute personne qui se connecte aux serveurs internet de ces infrastructures, notamment les serveurs d'un hôpital mais aussi les serveurs loués dans un centre de données commercial ou auprès de fournisseurs de services dans le *cloud*. L'incidence d'une telle conservation des données est énorme et équivaut en réalité à une obligation de conservation généralisée. De même, les personnes qui disposent d'une connexion internet fixe et qui habitent dans le voisinage de certains bâtiments ou de certaines zones, par exemple à proximité d'une gare, sont aussi affectées par la conservation des données. En effet, l'article 10 de la loi du 20 juillet 2022 ne porte pas uniquement sur les réseaux mobiles mais également sur certaines connexions internet fixes. Cette mesure n'est absolument pas pertinente en matière de criminalité grave ou de sécurité nationale.

A.13.7. L'article 11 de la loi du 20 juillet 2022 dispose que l'étendue du périmètre de certaines zones est déterminée par arrêté royal, le législateur n'ayant pas déterminé lui-même les périmètres minimum et maximum à respecter. Une telle mesure s'avère contraire à l'interdiction de conservation généralisée et indifférenciée des données, dès lors qu'elle ne remplit pas à la condition de clarté et de précision. Par ailleurs, il appartient au législateur de fixer lui-même la liste des zones ainsi que le périmètre de celles-ci. Le principe de la légalité formelle contenu dans l'article 22 de la Constitution est violé.

A.13.8. La partie requérante observe que l'article 45 de la loi du 20 juillet 2022 prévoit que la conservation ciblée des données sur la base des critères prévus à l'article 126/3, §§ 3 à 5, de la loi du 13 juin 2005 entre en vigueur à une date fixée par arrêté royal, au plus tard le 1er janvier 2027. Cette date butoir confirme que la mesure de conservation des données n'est pas réalisable, puisqu'il faudra beaucoup de temps pour rendre le système opérationnel dans les zones visées. Par ailleurs, il est incohérent que cette mesure transitoire concerne certaines zones et non d'autres, alors que les intérêts légitimes et les difficultés techniques sont les mêmes pour les différentes zones.

A.13.9. En ce qui concerne l'utilisation de variables, à l'article 11 de la loi du 20 juillet 2022, pour organiser un système souple correspondant à la réalité du terrain, la partie requérante soutient que le législateur a créé des critères quantitatifs purement arbitraires et contestables au regard des principes de nécessité, de proportionnalité et de subsidiarité. Les seuils retenus dans la loi du 20 juillet 2022 font référence à de faibles pourcentages de criminalité, qui ne sont pas sérieux. Contrairement à ce que soutient le Conseil des ministres, il appartient effectivement à la Cour d'examiner ces seuils dans le cadre de son contrôle de proportionnalité. En ce qui concerne les variables relatives au délai de conservation, la partie requérante relève que ce mécanisme est en contradiction flagrante avec, d'une part, la disposition de la loi du 20 juillet 2022 qui fixe l'importance des infractions sur la base des statistiques relatives au nombre d'infractions commises sur une moyenne de trois ans et, d'autre part, la disposition qui fixe chaque année la liste des arrondissements et des zones de police. L'article 11 de la loi du 20 juillet 2022 est incompatible avec la nécessité de lutter contre le risque élevé d'actes de criminalité grave, dès lors que, dans les faits, les zones sont fixées *a posteriori*, chaque année, pour une période de conservation variable, puisqu'elles sont issues de statistiques criminelles antérieures. En réalité, la liste établie annuellement ne tient tout simplement pas compte de la réalité actuelle du terrain. Pour le surplus, la partie requérante considère que l'applicabilité du mécanisme de révision périodique est contestable et que ce mécanisme ne démontre pas que la mesure prévue à l'article 11 de la loi du 20 juillet 2022 est nécessaire.

A.13.10. La partie requérante insiste sur le fait que l'article 11 de la loi du 20 juillet 2022 équivaut à une obligation de conservation généralisée et indifférenciée des données. Dans son avis sur l'avant-projet de loi à l'origine de cette loi, la section de législation du Conseil d'État s'est d'ailleurs interrogée sur le choix des zones géographiques et sur la nécessité d'établir les différents types de zones. La mesure s'avère donc disproportionnée et incompatible avec la jurisprudence de la Cour de justice. La partie requérante soutient par ailleurs que l'argument du Conseil des ministres, selon lequel les caractéristiques propres à l'État belge le distingueraient d'autres États et justifieraient la nécessité et la proportionnalité de la mesure, n'est pas défendable. Dans les faits, cet argument justifierait que chaque État membre dont la superficie est réduite puisse se soustraire au champ d'application de l'article 15, paragraphe 1, de la directive 2002/58/CE. Partant, il ne peut être soutenu que des facteurs objectifs justifient une conservation généralisée de données sur l'ensemble du territoire.

A.14.1. Un quatrième moyen est pris de la violation des articles 11, 12, 22 et 29 de la Constitution, de l'article 15, paragraphe 1, et des articles 5, 6 et 9 de la directive 2002/58/CE, lus à la lumière des articles 7, 8, 11, 47 et 52, paragraphe 1, de la Charte, des articles 6, 8, 10, 11 et 18 de la Convention européenne des droits de l'homme et des articles 13 et 54 de la directive (UE) 2016/680. La partie requérante soutient que l'article 13 de la loi du 20 juillet 2022, qui vise les autorités pouvant accéder aux données conservées par les opérateurs en vertu des articles 5 et 6 de cette loi, n'est pas compatible avec la jurisprudence de la Cour de justice. Selon celle-ci, l'accès aux données doit être justifié afin de préserver la sécurité nationale ou de lutter contre la criminalité grave, étant entendu que, lorsque des données ont été conservées sur le fondement de la sécurité nationale, le fondement de la criminalité grave ne peut être invoqué. Or, l'article 13 de la loi du 20 juillet 2022 a une portée trop large, dès lors que les autorités visées ne sont pas compétentes pour préserver la sécurité nationale ni pour lutter contre la criminalité grave. Partant, la mesure n'est pas conforme à l'article 15, paragraphe 1, de la directive 2002/58/CE.

L'article 13 de la loi du 20 juillet 2022 autorise dix autorités distinctes à accéder aux données visées. Ces autorités sont, pour la plupart, nouvelles par rapport aux régimes antérieurs qui avaient déjà été censurés par la Cour. La circonstance que l'accès aux données est dans une certaine mesure limité n'est pas de nature à démontrer le caractère justifié de l'ingérence dans les droits fondamentaux, dès lors que les données visées sont très étendues. En outre, la notion de « criminalité grave » visée audit article 13 n'est pas la même que celle qui est visée à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle, dont il est question à l'article 11 de la loi du 20 juillet 2022. Ce même article 13 a une portée beaucoup plus large dans cette perspective, ce qui entraîne une contradiction sur la notion de « criminalité grave » dans le cadre de la conservation de données, d'une part, et dans le cadre de

l'accès aux données, d'autre part. Pour cette raison, l'article 15, paragraphe 1, de la directive 2002/58/CE est violé. La partie requérante soutient par ailleurs que les autorités administratives visées à l'article 13 de la loi du 20 juillet 2022 ne peuvent pas accéder aux données dans le cadre de la criminalité grave et que les différentes finalités mentionnées dans cette disposition ne constituent pas des fondements de traitement de données admissibles au regard de la jurisprudence de la Cour de justice, de la directive 2002/58/CE et du RGPD.

A.14.2. La partie requérante soutient qu'en ce qu'il vise les « autorités administratives ou judiciaires compétentes pour la prévention, la recherche, la détection ou la poursuite d'une infraction commise en ligne ou par le biais d'un réseau ou service de communications électroniques », l'article 13 de la loi du 20 juillet 2022 pose problème dès lors qu'il ne se limite pas aux infractions relevant de la criminalité grave mais qu'il s'étend à l'ensemble des infractions pénales. En outre, l'article 13 mentionne que les autorités visées dans cette disposition ne peuvent accéder aux données qu'en vertu d'une norme législative formelle, sans identifier celle-ci. Par ailleurs, le législateur a prévu que la liste des autorités habilitées à obtenir les données conservées de la part d'un opérateur est fixée par une circulaire ministérielle. La partie requérante observe à cet égard que le ministre compétent à cette fin n'est pas précisé et ce n'est en toute hypothèse pas une circulaire qui doit modifier le contenu de la loi. Cette mesure s'avère également contraire au fait que l'article 13 de la loi du 20 juillet 2022 dispose aussi que seules les autorités visées par la loi peuvent obtenir un accès aux données auprès des opérateurs.

A.14.3. La partie requérante prend un cinquième moyen de la violation des articles 10, 11, 22 et 29 de la Constitution, lus en combinaison ou non avec l'article 15, paragraphe 1, et les articles 5, 6 et 9 de la directive 2002/58/CE, lus à la lumière des articles 7, 8, 11, 47 et 52, paragraphe 1, de la Charte, des articles 6, 8, 10, 11 et 18 de la Convention européenne des droits de l'homme et des articles 13 et 54 de la directive (UE) 2016/680. La partie requérante observe que la loi du 20 juillet 2022 vise notamment la conservation de données de communication de personnes soumises au secret professionnel, à savoir les médecins, les avocats et les journalistes, et ce, de la même manière que pour la conservation des données de communication des autres personnes, qui ne sont pas soumises au secret professionnel. Or, le législateur n'a prévu aucun mécanisme de contrôle pertinent pour permettre aux personnes soumises au secret professionnel de s'opposer à la collecte, à la conservation ou à la prise de connaissance de leurs données, alors qu'elles se trouvent dans une situation objectivement différente de la situation des autres personnes.

La partie requérante observe en outre que l'article 88*bis* du Code d'instruction criminelle, tel qu'il a été modifié par l'article 27 de la loi du 20 juillet 2022, autorise le juge d'instruction à viser un avocat ou un médecin qui est lui-même soupçonné d'une infraction. Il est certes prévu que le bâtonnier ou le représentant provincial de l'Ordre des médecins est averti lors de la mise en œuvre de la mesure et que les éléments relevant du secret professionnel ne sont pas consignés dans le procès-verbal. Cependant, ces garanties sont insuffisantes pour garantir la constitutionnalité du procédé. Par ailleurs, aucune garantie n'est prévue en ce qui concerne les autorités autres que le juge d'instruction, alors que celles-ci peuvent aussi demander accès aux données d'avocats, de médecins ou de journalistes.

Affaire n° 7931

A.15. La partie requérante prend un moyen unique de la violation des articles 11, 12, 22 et 29 de la Constitution, lus en combinaison ou non avec les articles 7, 8, 11, 47 et 52, paragraphe 1, de la Charte , avec l'article 8 de la Convention européenne des droits de l'homme, avec les articles 5, 6 et 15 de la directive 2002/58/CE et avec les articles 13 et 54 de la directive (UE) 2016/680.

A.16.1. Tout d'abord, en ce qui concerne la collecte systématique et indifférenciée de certaines données, la partie requérante observe que la loi du 20 juillet 2022 impose aux opérateurs la conservation de certaines données d'identification, qui s'ajoutent à celles qui doivent déjà être collectées pour identifier les abonnées, comme le numéro de registre national. Les données doivent être conservées pendant toute la durée d'activation du service et jusqu'à douze mois après la date de la dernière communication à l'aide du service, sans toutefois que le législateur indique en quoi cette durée de conservation s'avère nécessaire par rapport à l'objectif poursuivi. Par ailleurs, si la Cour de justice admet en principe que les données collectées relatives à l'identité civile des utilisateurs soient conservées sans délai particulier, il y a lieu de constater qu'en l'espèce, la loi du 20 juillet 2022 porte sur d'autres données, notamment l'identifiant créé pour chaque communication, la date du début de l'abonnement ou encore les données relatives au paiement. En toute hypothèse, ces informations permettent de localiser des personnes. Or,

le législateur n'indique pas en quoi la collecte de ces données est nécessaire au regard à l'objectif poursuivi, de sorte que l'article 8 de la loi du 20 juillet 2022 est disproportionné et qu'il viole les dispositions citées dans le moyen.

En cas de doute au sujet de l'article 8 de la loi du 20 juillet 2022, il y a lieu, selon la partie requérante dans l'affaire n° 7931, de poser une question préjudicielle à la Cour de justice, afin de déterminer si 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, s'oppose à une mesure législative imposant, sans délai particulier, la conservation de plusieurs donnés d'identification de l'ensemble des utilisateurs de moyens de communications électronique afin de lutter contre les infractions pénales et de sauvegarder la sécurité publique, ou si cette disposition doit être limitée à la collecte de données relatives à l'identité civile de l'utilisateur.

A.16.2. La partie requérante relève que la Cour de justice admet la collecte systématique et indifférenciée des adresses IP dans le cadre de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique. Néanmoins, la loi du 20 juillet 2022 autorise l'accès aux adresses IP dans des hypothèses plus larges. Par ailleurs, l'article 13 de cette loi admet que des autorités qui ne sont pas chargées de lutter contre la criminalité grave accèdent aux adresses IP, ce qui n'est pas admissible. En outre, la Cour de justice impose que la durée de conservation soit limitée à ce qui est strictement nécessaire au regard de l'objectif poursuivi, ce que le législateur n'explique pas, et que des conditions et des garanties strictes en ce qui concerne l'exploitation des données soient établies, ce ne prévoit pas la loi du 20 juillet 2022.

A.16.3. La partie requérante relève par ailleurs que l'article 5 de la loi du 20 juillet 2022 oblige les opérateurs à conserver, et à traiter le cas échéant, les données de localisation et les autres données de trafic nécessaires pour détecter et analyser une fraude présumée ou une utilisation malveillante présumée du réseau de communications électroniques. Les notions de « fraude » et d'« utilisation malveillante du réseau » sont définies par la loi et par les travaux préparatoires de celle-ci en donnent plusieurs exemples concrets. De la sorte, le législateur instaure en réalité une obligation de collecte ainsi qu'une conservation systématique et indifférenciée de certaines données à des fins de lutte contre la criminalité en général. Or, la Cour de justice précise que seule la lutte contre la criminalité grave est susceptible de justifier des ingérences dans les droits fondamentaux garantis par les articles 7 et 8 de la Charte, ce qui n'est pas le cas pour la fraude présumée ni pour l'utilisation malveillante de réseau. Dans ce cadre, la circonstance que la collecte est limitée à certaines catégories de données n'est pas pertinente. Selon le législateur, il n'est pas possible de prévoir un système moins intrusif. Néanmoins, l'Autorité de protection des données a souligné que des mesures moins attentatoires étaient possibles, par exemple en prévoyant une obligation de conservation des données lorsqu'il existe des indices de fraude ou d'utilisation malveillante du réseau. Par ailleurs, la durée de conservation des données apparaît manifestement disproportionnée. En toute hypothèse, le Conseil des ministres tente de démontrer le caractère nécessaire de la mesure alors que c'est la proportionnalité de celle-ci qui est mise en cause.

Du reste, selon la partie requérante, en cas de doute en ce qui concerne l'article 5 de la loi du 20 juillet 2022, il conviendrait de poser une question préjudicielle à la Cour de justice pour déterminer si l'article 15, paragraphe 1, de la directive 2002/58/CE, lu en combinaison avec les articles 7, 8 et 52, paragraphe 1, de la Charte, s'oppose à une obligation générale, pour les opérateurs et les fournisseurs de services de communications électroniques, applicable à d'autres faits que les actes de criminalité grave, en vue de détecter et d'analyser une fraude présumée ou une utilisation malveillante présumée d'un réseau de communications électroniques, de conserver les données de trafic et de localisation au sens de cette directive, générées ou traitées dans le cadre de la fourniture de ces services.

A.16.4. L'article 5 de la loi du 20 juillet 2022 laisse la possibilité aux opérateurs de conserver et de traiter les données de trafic nécessaires pour assurer la sécurité et le bon fonctionnement des réseaux et services de communications électroniques, en particulier pour détecter et analyser une atteinte potentielle ou réelle à cette sécurité, y compris pour identifier l'origine de cette atteinte. La partie requérante constate que les opérateurs sont par ailleurs déjà tenus par une obligation de prendre les mesures d'ordre technique et organisationnel nécessaires pour gérer les risques en matière de sécurité des réseaux et des services de manière appropriée, le cas échéant conjointement pour assurer la sécurité du réseau. Ils peuvent aussi identifier les personnes concernées par une transmission d'informations et prendre connaissance de données en matière de communications électroniques si le bon fonctionnement du réseau et la bonne exécution d'un service de communications électroniques l'exigent. Partant, la partie requérante n'aperçoit pas en quoi l'article 5 de la loi du 20 juillet 2022 s'avère nécessaire en sus des obligations déjà prévues. Par ailleurs, cette disposition autorise le responsable de traitement à ne plus effectuer

une mise en balance des intérêts en présence pour s'assurer qu'il n'existe pas, pour atteindre l'objectif visé, d'autres moyens qui soient moins intrusifs pour la personne concernée. La mesure est donc disproportionnée.

A.17.1. En ce qui concerne la conservation ciblée des données prévue par la loi du 20 juillet 2022, la partie requérante indique que le législateur a prévu un critère statistique et a visé certaines zones sujettes à un taux important de criminalité grave. Les données qui doivent être conservées sont listées à l'article 10 de la loi du 20 juillet 2022. Celles-ci sont conservées de manière systématique et indifférenciée en vertu de l'article 9 de cette loi, sur la base d'un critère géographique détaillé à l'article 11. Selon ce système, le législateur impose la collecte des données de trafic et de localisation sur certaines zones sujettes à un taux important de criminalité grave, calculé sur la base de la moyenne annuelle des infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle constatées par zone de police ou par arrondissement judiciaire, par mille habitants, sur une moyenne de trois ans. La durée de conservation des données varie, entre six et douze mois, en fonction du nombre d'infractions constatées. Or, selon la partie requérante, le législateur ne justifie pas les raisons pour lesquelles ces données doivent être conservées durant ce délai ni en quoi cette conservation est nécessaire. Par ailleurs, si la Cour de justice autorise la collecte systématique et indifférenciée des données à des fins de lutte contre la criminalité grave, force est de constater que la loi du 20 juillet 2022 vise la criminalité en général, dès lors que les infractions visées à l'article 90*ter* du Code d'instruction criminelle sont notamment des infractions de droit commun comme le faux informatique, la fraude informatique ou le vol avec violence. En réalité, le législateur aurait pu cibler certaines infractions en fonction de la peine qui y est attachée. Il y a donc lieu d'annuler les dispositions précitées de la loi du 20 juillet 2022.

Contrairement à ce qu'indique le Conseil des ministres, la notion d'infraction grave ne peut être entièrement laissée à l'appréciation des États membres, sous peine d'entraîner des divergences d'interprétation quant aux objectifs visés par l'article 15, paragraphe 1, de la directive 2002/58/CE. En cas de doute à ce sujet, il y a lieu de poser une question préjudicielle à la Cour de justice, afin de déterminer si l'article 15, paragraphe 1, de la directive 2002/58/CE, lu en combinaison avec les articles 7, 8 et 52, paragraphe 1, de la Charte, s'oppose à une conservation ciblée des données relatives au trafic et à la localisation, limitée au moyen d'un critère géographique à des fins autres que la criminalité grave, à savoir la lutte contre le faux informatique, la fraude informatique ou encore le vol avec violence, indépendamment du seuil de la peine. Dans son mémoire en réponse, la partie requérante propose d'interroger également la Cour de justice pour déterminer si les notions d'infractions pénales graves et de criminalité grave au sens de la jurisprudence de la Cour de justice sont des notions autonomes du droit de l'Union ou s'il appartient aux autorités compétentes des États membres d'en préciser elles-mêmes le contenu et, dans l'hypothèse où il s'agirait de notions autonomes du droit de l'Union, les modalités selon lesquelles il convient de déterminer s'il est question d'infractions pénales graves ou de criminalité grave.

A.17.2. La partie requérante ajoute que les dispositions précitées de la loi du 20 juillet 2022 n'établissent pas un indicateur relatif au nombre de faits commis, contrairement à ce qui est mentionné dans les travaux préparatoires, dès lors qu'elles prévoient un critère basé sur des données relatives à la qualification des faits au début de l'enquête, de sorte que des erreurs existent, notamment lorsque la qualification des faits est modifiée en cours d'enquête ou lorsque les faits sont classés sans suite. Un critère plus précis aurait pu être retenu, comme le nombre d'infractions ayant abouti à une condamnation par les cours et tribunaux. Contrairement à ce qu'indique le Conseil des ministres, dans l'hypothèse où l'ensemble du territoire devrait être visé par l'obligation de conservation des métadonnées, ce ne serait pas en raison d'un taux de criminalité élevé dans les différentes zones, mais en raison d'un critère géographique particulièrement large incluant la criminalité en général et fondé sur des données erronées, dès lors que les statistiques retenues par la loi du 20 juillet 2022 ne sont pas fiables. Par ailleurs, l'application du critère géographique entraîne certaines difficultés pour les services comme « WhatsApp », « Skype » ou « Facebook », soumis aux mêmes obligations que les autres opérateurs alors que ces services ne sont pas toujours en mesure de déterminer la localisation de l'utilisateur. Dans cette hypothèse, il ressort de la loi du 20 juillet 2022, notamment de son article 9, qu'il convient de stocker *a minima* l'ensemble des données pour couvrir la zone concernée, ce qui suppose donc une collecte des données traitées sur l'ensemble du territoire belge, ce qui n'est pas admis par la Cour de justice.

Par ailleurs, si l'opérateur n'est pas en mesure de limiter la conservation des données aux seules zones visées par la loi du 20 juillet 2022, il est tenu de conserver ces données en limitant au strict nécessaire leur conservation en dehors de cette zone, au regard des possibilités techniques. Ce faisant, le législateur a décidé d'appliquer le principe de minimisation des données de manière souple, afin d'éviter une discrimination entre les victimes de

faits graves de criminalité en fonction des moyens des opérateurs. En réalité, il porte de la sorte atteinte à un principe fondamental du droit à la protection des données à caractère personnel auquel il ne peut pas être dérogé. Afin de limiter l'ingérence au strict nécessaire, le législateur aurait dû prévoir qu'en cas de doute, l'opérateur ne peut conserver que les données relatives à la zone concernée.

A.17.3. L'article 11 de la loi du 20 juillet 2022 prévoit que le périmètre des zones sujettes à un taux important de criminalité grave est déterminé par le Roi, alors que le principe de légalité contenu dans l'article 22 de la Constitution et dans les articles 7, 8 et 52, paragraphe 1, de la Charte impose que cet élément soit fixé dans une loi formelle. Du reste, le législateur impose la conservation des données sur un nombre très important de zones qu'il estime sujettes à un taux de criminalité grave, sans justifier concrètement en quoi ces zones sont effectivement caractérisées par un tel taux ni, partant, les raisons pour lesquelles la collecte des données est nécessaire eu égard à l'objectif poursuivi.

A.17.4. L'article 11 établit en outre la conservation ciblée de métadonnées à des fins de sécurité nationale, ce qui n'est pas admissible pour les mêmes raisons que celles qui concernent la conservation des données à des fins pénales. De plus, les missions de l'OCAM, qui détermine sur la base du niveau de la menace les zones géographiques concernées dans ce cadre, sont plus larges que celles qui sont relatives à la sécurité nationale. Or, la Cour de justice précise que la criminalité, même grave, n'est pas assimilable à une menace pour la sécurité nationale. Par ailleurs, les zones concernées par la conservation des données à des fins de sécurité nationale sont celles dont le niveau de la menace est au moins de 3, et ce, aussi longtemps que ce niveau perdure. Ce critère ne s'avère pas non plus conforme à la jurisprudence de la Cour de justice, qui semble imposer le recours au niveau 4, plus élevé, ainsi qu'une période dans laquelle le degré de menace doit être réévalué.

Il ressort aussi de l'article 11 de la loi du 20 juillet 2022 que le législateur impose la conservation des données sur un nombre très important de zones qu'il estime sujettes à une menace pour la sécurité nationale, sans justifier concrètement cette mesure ni la nécessité de la collecte des données. Par ailleurs, cette collecte est également prévue pour des zones potentiellement soumises à des menaces pour la sécurité nationale, ce qui n'est pas conforme à la jurisprudence de la Cour de justice, qui exige une menace réelle et actuelle, ou prévisible, pour la sécurité nationale. L'article 11 vise aussi la menace potentielle pour les intérêts des institutions internationales sans que cela ne soit raisonnablement justifié. La partie requérante constate qu'il est également prévu que le Roi puisse compléter la liste des zones énumérées à l'article 11, ainsi qu'adapter le périmètre des zones couvertes par l'obligation de conservation des données, ce qui est contraire au principe de légalité de l'article 22 de la Constitution. La Cour de justice impose par ailleurs que la conservation de données fasse l'objet d'un contrôle effectif par une juridiction ou par une autorité administrative indépendante, dont la décision est dotée d'un effet contraignant, afin de vérifier le respect des conditions et garanties qui doivent être prévues.

A.18. En ce qui concerne les règles relatives au gel rapide des données, la partie requérante allègue que les hypothèses visées à l'article 25 de la loi du 20 juillet 2022 sont plus larges que celles qu'autorise la Cour de justice, qui se limitent aux cas de criminalité grave et ne s'étendent pas à la lutte contre la criminalité en général. Par ailleurs, la durée de conservation des données est manifestement disproportionnée à l'objectif poursuivi.

A.19.1. En ce qui concerne l'accès aux données, l'article 13 de la loi du 20 juillet 2022 précise les autorités compétentes, notamment les autorités financières, de sorte que le législateur a estimé que les infractions à la réglementation relative aux abus de marchés relevaient de la criminalité grave. Cependant, la Cour de justice considère qu'il s'agit d'infractions qui relèvent de la criminalité en général. L'article 9 de la loi du 20 juillet 2022 précise en outre que le Roi peut compléter la liste des autorités compétentes, ce qui est contraire au principe de légalité contenu dans l'article 22 de la Constitution et dans les articles 7, 8 et 52, paragraphe 1, de la Charte, qui exigent le recours à une loi formelle. Par ailleurs, selon l'article 13 de cette loi, une circulaire ministérielle énumère les autorités habilitées à obtenir les données visées par la loi, ce qui est également contraire au principe de la légalité formelle précité. La partie requérante relève encore que les finalités visées à l'article 13 de la loi sont plus larges que celles qui sont fixées à l'article 15, paragraphe 1, de la directive 2002/58/CE.

A.19.2. Les conditions d'accès aux données collectées sont précisées à l'article 13 de la loi du 20 juillet 2022 et elles n'exigent pas que la demande d'accès soit motivée par rapport à l'objectif poursuivi, alors qu'un lien avec

l'objectif de lutte contre la criminalité est exigé. En outre, l'article 26 de la loi du 20 juillet 2022, qui encadre les conditions d'accès des autorités compétentes aux données collectées à des fins pénales, autorise le procureur du Roi ou l'officier de police judiciaire en cas d'urgence à accéder aux données d'identification, alors que la Cour de justice impose un contrôle préalable de la part d'une juridiction ou d'une autorité administrative indépendante. Or, le procureur du Roi ne saurait être considéré comme un tiers dans le cadre de la procédure d'accès aux données concernées.

En cas de doute sur ce point, il convient de poser des questions préjudicielles à la Cour de justice afin de déterminer, d'une part, si l'article 15, paragraphe 1, de la directive 2002/58/CE, lu en combinaison avec les articles 7, 8 et 52, paragraphe 1, de la Charte, s'oppose à ce que le procureur du Roi, voire en cas d'urgence un officier de police judiciaire, accède aux données d'identification collectées de manière systématique et indifférenciée à des fins de lutte contre la criminalité en général et, d'autre part, si l'article 15, paragraphe 1, précité, lu en combinaison avec les mêmes dispositions de la Charte, s'oppose à ce que le procureur du Roi accède en cas d'urgence aux données de trafic et de localisation à des fins de lutte contre la criminalité en général.

A.19.3. Par ailleurs, l'article 26 de la loi du 20 juillet 2022 permet au procureur du Roi d'imposer la collaboration des centres fermés et des lieux d'hébergement au sens de la loi du 15 décembre 1980 « sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers » (ci-après : la loi du 15 décembre 1980), sans expliquer en quoi cette collaboration est nécessaire par rapport à l'objectif poursuivi, à savoir la lutte contre la criminalité.

A.19.4. L'article 25 de la loi du 20 juillet 2022, quant à lui, autorise un accès aux données lorsqu'existent des indices sérieux d'infraction de nature à entraîner un emprisonnement correctionnel principal d'un an ou d'une peine plus lourde, ce qui vise en réalité la grande majorité des infractions prévues dans le Code pénal, qui ne peuvent donc être qualifiées de criminalité grave.

En cas de doute sur ce point, il convient de poser une question préjudicielle à la Cour de justice afin de déterminer si l'article 15, paragraphe 1, de la directive 2002/58/CE, lu en combinaison avec les articles 7, 8 et 52, paragraphe 1, de la Charte, s'oppose à ce que le juge d'instruction, ou le procureur du Roi en cas d'urgence, accède aux données de trafic et de localisation à des fins de lutte contre la criminalité en général, dès lors que les infractions visées sont punissables d'un an d'emprisonnement au minimum.

L'article 24 de la loi du 20 juillet 2022 permet l'accès aux données par un officier de police judiciaire, qui n'est pas un tiers à la procédure et ne peut donc être qualifié d'autorité indépendante comme l'exige la Cour de justice. De surcroît, en cas d'urgence, cet officier de police judiciaire peut exiger que l'opérateur lui fournisse les métadonnées, moyennant le contrôle ultérieur du juge d'instruction. Or, la Cour de justice impose un contrôle judiciaire préalable dans cette hypothèse.

A.19.5. La partie requérante ajoute que la loi du 20 juillet 2022 ne prévoit pas qu'une personne soit informée du traitement des données une fois que la limitation du traitement n'est plus justifiée au regard de l'objectif poursuivi, ce qui est le cas lorsque cette information n'est pas susceptible de compromettre l'enquête menée par les autorités, contrairement à ce qui est exigé par la Cour de justice. En cas de doute sur ce point, il convient de poser une question préjudicielle à cette juridiction afin de déterminer si l'article 15, paragraphe 1, de la directive 2002/58/CE, lu en combinaison avec les articles 7, 8, 47 et 52, paragraphe 1, de la Charte et les articles 13 et 54 de la directive (UE) 2016/680, impose une telle information.

Par ailleurs, la partie requérante constate que la loi du 20 juillet 2022 ne prévoit pas non plus une protection effective contre les risques d'abus et d'accès illicite aux données pour les personnes concernées. En effet, dans le cas où les autorités accèdent aux données mais estiment qu'il n'est pas nécessaire d'entamer des poursuites, la personne ne peut pas contester la légalité de la mesure d'enquête, sauf à introduire une action en responsabilité civile devant le tribunal de première instance, ce qui constitue une hypothèse assez peu probable et ne permet pas d'offrir un recours effectif. Ensuite, dans le cas où la personne concernée conteste la légalité de la mesure d'enquête dans le cadre d'une procédure pénale au cours de laquelle cette personne est amenée à comparaître devant un juge, la mesure concernée ne peut pas nécessairement être écartée des débats et il ne peut pas en être tenu compte dans l'appréciation de la peine, compte tenu de l'article 32 du titre préliminaire du Code de procédure pénale. Par ailleurs, les organes et autorités cités par le Conseil des ministres n'offrent pas non plus de voie de recours juridictionnelle aux personnes concernées, dès lors qu'il s'agit d'autorités administratives indépendantes.

Partant, la loi du 20 juillet 2022 viole les dispositions citées au moyen en ce qu'elle ne prévoit pas que les personnes soient informées que les autorités nationales compétentes ont accédé à leurs données ni que ces personnes disposent d'une voie de recours à contre un accès illégal aux données.

A.20. En ce qui concerne le chiffrement des communications, la partie requérante relève que l'article 3 de la loi du 20 juillet 2022 dispose que les opérateurs ne peuvent, en faisant usage d'un système de cryptographie, empêcher l'exécution d'une demande ciblée d'accès aux données, d'une part, et que l'utilisation de la cryptographie par un opérateur étranger ne peut avoir pour conséquence d'empêcher les opérateurs de conserver les données dans le cas où une personne utilise une carte SIM étrangère sur le territoire belge. Selon la partie requérante, cette mesure est manifestement disproportionnée. En effet, les mesures de cryptage permettent d'assurer la protection des données à caractère personnel et donc de contribuer à protéger le droit au respect de la vie privée. Différents instruments de droit international préconisent d'ailleurs le chiffrement des données afin d'assurer la sécurité des flux et la protection des données à caractère personnel.

A.21. Enfin, en ce qui concerne les conséquences de l'annulation de la loi du 20 juillet 2022, la partie requérante soutient que l'utilisation, dans le cadre d'une enquête pénale, de données collectées en violation de la directive 2002/58/CE et des articles 7 et 8 de la Charte constitue un dommage qui doit pouvoir être réparé de manière effective par une appréciation et une pondération des informations et des éléments de preuve, voire par une prise en compte de leur caractère illégal dans le cadre de la détermination de la peine, comme l'exige la jurisprudence de la Cour de justice. Or, la loi du 20 juillet 2022 ne prévoit pas de telles garanties.

À tout le moins, la Cour devrait préciser qu'il appartient au juge pénal de constater que les éléments de preuve collectés en violation de la directive 2002/58/CE et des articles 7 et 8 de la Charte qui ne peuvent pas être écartés des débats doivent en tous cas être pris en considération, au regard de leur caractère illégal, dans le cadre de la détermination de la peine. La partie requérante soutient que la Cour est bien compétente dans ce cadre, de manière similaire à ce que fait la Cour de justice dans plusieurs de ses arrêts.

En cas de doute à cet égard, il convient de poser une question préjudicielle à la Cour de justice afin de déterminer, d'une part, s'il est admis que des violations du droit de l'Union européenne, en particulier de la directive 2002/58/CE ainsi que des articles 7 et 8 de la Charte, entachant la collecte de preuves dans une procédure pénale nationale, puissent rester sans conséquence, même en cas d'infraction grave, et, d'autre part, si les violations précitées doivent être prises en compte en faveur de la personne poursuivie au moins au stade de l'appréciation des preuves ou de la fixation de la peine.

Affaire n° 7932

A.22. Les parties requérantes prennent un premier moyen de la violation articles 10, 11, 13, 15, 22, 23 et 29 de la Constitution, lus en combinaison ou non avec les articles 5, 6, 8, 9, 10, 11, 14 et 18 de la Convention européenne des droits de l'homme, avec les articles 7, 8, 11, 47 et 52 de la Charte, avec l'article 5, paragraphe 4, du Traité sur l'Union européenne ainsi qu'avec l'article 6 de la directive 2002/58/CE, avec la directive (UE) 2016/680 et avec le RGPD. Ce moyen porte sur la collecte et la conservation des données de trafic et de localisation.

A.23.1. Dans une première branche, les parties requérantes soutiennent que les articles 4 et 5 de la loi du 20 juillet 2022 prévoient une conservation de données généralisée qui ne répond pas aux exigences du droit de l'Union européenne.

A.23.2. En particulier, l'article 5 de la loi du 20 juillet 2022 prévoit notamment l'obligation pour un opérateur de conserver des données de trafic et de localisation pendant quatre mois pour pouvoir constater d'éventuelles fraudes ou utilisations malveillantes du réseau ou du service. Un tel traitement constitue une conservation de données de trafic généralisée et indifférenciée et ne respecte pas les exigences de l'article 6 de la directive 2002/58/CE. Il ressort également de la jurisprudence constante de la Cour de Justice qu'une telle conservation de données généralisée et indifférenciée n'est admissible que dans le cadre de la protection de la sécurité nationale. La fraude ou l'utilisation malveillante du réseau sont des phénomènes qui ne répondent

absolument pas à cette exigence. L'obligation de conservation prévue ne relève donc manifestement pas de l'exception visée à l'article 15, paragraphe 1, de la directive 2002/58/CE.

Les parties requérantes relèvent que l'article 5 de la loi du 20 juillet 2022 prévoit par ailleurs l'obligation pour un opérateur de conserver pendant douze mois le numéro de téléphone ou l'adresse IP attribuée à l'origine de la communication entrante, l'horodatage et le port utilisé, ainsi que les dates et heures précises de début et de fin de la communication, afin de pouvoir constater des fraudes ou des utilisations malveillantes du réseau ou du service. Il s'agit d'une obligation de conservation qui est contraire à l'article 6 de la directive 2002/58/CE et qui entraîne une violation des droits fondamentaux.

En outre, l'article 5 de la loi du 20 juillet 2022 prévoit la possibilité pour les opérateurs de conserver les données de trafic qui sont nécessaires pour garantir la sécurité et le bon fonctionnement de leur réseau ou service, mais aussi pour détecter et analyser une atteinte potentielle ou réelle au réseau. La durée de conservation maximale est de douze mois, mais en cas d'atteinte spécifique à la sécurité, les données peuvent même être conservées plus longtemps. Selon les parties requérantes, il s'agit d'un véritable droit de conservation qui ne respecte pas l'article 6 de la directive 2002/58/CE, lequel exige que les données de trafic soient effacées ou rendues anonymes dès qu'elles ne sont plus nécessaires à la transmission. L'exception prévue à l'article 15, paragraphe 1, de cette directive n'est pas non plus applicable, sauf s'il devait s'agir de criminalité grave ou d'une question de sécurité nationale. La loi applique toutefois une définition bien plus large, qui ne correspond pas au champ d'application européen.

A.23.3. Selon les parties requérantes, la conservation indifférenciée des données précitées, en violation du droit de l'Union européenne, entraîne une violation du principe d'égalité. En effet, les données des parties requérantes sont traitées de la même manière que les données qui font l'objet d'une enquête pénale relative à des infractions criminelles graves, alors que rien n'indique que les parties requérantes se trouvent dans une même situation. Il ressort de la jurisprudence de la Cour de justice que le droit au respect de la vie privée est également compromis.

A.24. Dans une deuxième branche, les parties requérantes allèguent que la conservation prévue à l'article 6 de la loi du 20 juillet 2022, en ce qui concerne les données de localisation pour la lutte contre la fraude et l'utilisation malveillante du réseau, n'est pas conforme au droit de l'Union européenne ni aux droits fondamentaux. Les parties requérantes relèvent que l'article 6 de la loi du 20 juillet 2022 permet la conservation des données de localisation autres que les données relatives au trafic. La durée de conservation est de douze mois pour le bon fonctionnement et la sécurité du réseau et de quatre mois pour détecter une fraude ou une utilisation malveillante du réseau. Cependant, l'article 9 de la directive 2002/58/CE exclut explicitement un tel traitement.

A.25.1. La troisième branche porte sur la conservation dans des zones géographiques spécifiques, prévue aux articles 9, 10 et 11 de la loi du 20 juillet 2022. Les parties requérantes relèvent tout d'abord que la conservation dans les zones autres que les zones géographiques spécifiques n'est pas nécessaire. À cet égard, elles affirment que, bien qu'il soit indiqué explicitement que les données sont conservées aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave, de la prévention de menaces graves contre la sécurité publique et de la sauvegarde des intérêts vitaux d'une personne physique, de sorte que les exigences de la Cour de justice paraissent formellement respectées, il découle toutefois de la mise en œuvre concrète du système que celui-ci entraîne *de facto* une conservation de données indifférenciée. Les parties requérantes soutiennent par ailleurs que la loi du 20 juillet 2022 ne permet pas de faire la distinction entre les différents objectifs et ne respecte pas la hiérarchie entre eux lorsqu'elle règle l'accès aux données, contrairement à ce qu'exige la Cour de justice. Les données qui, par exemple, sont conservées en vertu d'un objectif de sécurité nationale ne peuvent pas être utilisées pour la recherche d'infractions graves et la lutte contre celles-ci. Les autorités compétentes en matière d'enquêtes pénales ne peuvent donc pas accéder aux données s'il s'agit d'une conservation généralisée et indifférenciée. Partant, la loi du 20 juillet 2022 est insuffisamment prévisible et viole les directives citées au moyen.

En outre, le délai de conservation est en principe fixé à douze mois, à moins qu'un délai plus court soit fixé. Ce délai standard est disproportionné et dépasse le délai strictement nécessaire. Du reste, au lieu de recourir par défaut à un délai court, en limitant les délais plus longs à des circonstances exceptionnelles et moyennant une motivation sérieuse, il est choisi de faire usage du délai le plus long par défaut, de sorte que le principe de proportionnalité est violé. Les données doivent être conservées, tant en ce qui concerne la communication en provenance de la zone géographique déterminée que vers cette zone. Partant, les données de localisation d'un utilisateur final qui communique avec un utilisateur final dans une zone géographique concernée sont conservées, même si le premier utilisateur final ne se trouve pas dans une zone géographique soumise à une obligation de

conservation. Une telle obligation en dehors de la zone géographique concernée n'est pas strictement nécessaire. Enfin, la description des différentes zones géographiques à l'article 11 de la loi du 20 juillet 2022 est extrêmement large et comprend des zones qu'il n'est pas nécessaire de soumettre à une obligation de conservation, de sorte que celle-ci est *de facto* indifférenciée, ce qui n'est pas conforme aux exigences de la Cour de justice ni au principe de proportionnalité.

A.25.2. En ce qui concerne la conservation des données dans les arrondissements judiciaires et dans les zones de police, prévue à l'article 11 de la loi du 20 juillet 2022, les parties requérantes relèvent qu'une obligation de conservation est imposée dès qu'un certain nombre d'infractions est dépassé. Cependant, les statistiques utilisées dans ce cadre ne reflètent pas de manière fiable la criminalité, dès lors qu'elles concernent non seulement des condamnations ou des faits établis, mais aussi tout enregistrement d'un fait unilatéralement catalogué par la police comme constituant potentiellement une infraction. Selon les parties requérantes, ces statistiques risquent de fournir systématiquement une surestimation du nombre réel d'infractions, en raison de doubles enregistrements ou de faits enregistrés qui ne sont pas des infractions mais qui sont pourtant catalogués comme tels. Par ailleurs, le seuil d'infractions retenu a pour effet que la quasi-totalité du territoire est soumise à l'obligation de conservation, comme il ressort d'une analyse réalisée sur la base des statistiques de criminalité pour l'année civile 2021. Partant, la loi du 20 juillet 2022 aboutit à introduire une obligation de conservation généralisée et indifférenciée de données. En réalité, ce n'est que dans des cas exceptionnels que le critère combiné des statistiques au niveau de l'arrondissement judiciaire et de la zone de police n'entraîne pas une obligation de conservation. En outre, la mesure est en vigueur de manière permanente. Les conditions fixées par la Cour de justice pour une telle obligation de conservation, qui n'est admissible que dans un but de sécurité nationale, pour une durée limitée et dans des circonstances concrètes, ne sont donc pas respectées.

Du reste, selon les parties requérantes, le choix de désigner les arrondissements judiciaires comme zones géographiques est disproportionné, dès lors qu'il s'agit d'une zone de taille importante et que les chiffres en matière de criminalité pour tout l'arrondissement ne sont pas nécessairement représentatifs des différentes parties de la zone. L'utilisation des arrondissements judiciaires entraîne dès lors une obligation de conservation disproportionnée, qui n'est pas strictement nécessaire. De même, le délai de conservation prévu est particulièrement long et donne lieu à la conservation d'une énorme quantité de données, de nature extrêmement sensibles et relatives à de nombreuses personnes. Ce délai est donc disproportionné et n'est pas strictement nécessaire, de sorte qu'il viole les articles 10, 11 et 22 de la Constitution ainsi que les droits fondamentaux garantis par des dispositions analogues.

A.26.1. Les parties requérantes affirment que la détermination des zones géographiques dont le niveau de la menace est au moins de niveau 3, visées à l'article 11 de la loi du 20 juillet 2022, est dépourvue de fondement légal dès lors que les niveaux de menace sont définis uniquement par arrêté royal et non dans une loi formelle. Partant, il n'est pas satisfait à l'exigence de l'article 22 de la Constitution. En outre, le principe de prévisibilité exige que le citoyen puisse déterminer, sur la base du libellé légal, la signification des niveaux de menace, en raison des répercussions de ceux-ci sur la conservation obligatoire de ses données à caractère personnel. Par ailleurs, la Cour de justice autorise une obligation de conservation généralisée et indifférenciée en ce qui concerne la sécurité nationale lorsqu'existe une menace grave qui s'avère réelle, actuelle ou prévisible. Le niveau 3 ne répond pas à cette exigence, dès lors que la menace qu'il vise ne doit être que possible et vraisemblable, et non sérieuse et réelle.

A.26.2. Selon les parties requérantes, la loi du 20 juillet 2022 ne prévoit aucun effacement des données en cas de baisse du niveau de la menace dans une zone spécifique ou sur la totalité du territoire, ni de modalités de notification au citoyen concerné par la conservation des données, ni encore la possibilité d'introduire un recours contre cette conservation, comme l'exige pourtant la Cour de justice. Partant, la loi du 20 juillet 2022 viole les articles 10, 11 et 13 de la Constitution, lus en combinaison ou non avec les articles 5, 6, 8, 9, 10, 11, 14, 15, 17 et 18 de la Convention européenne des droits de l'homme.

A.26.3. En ce qui concerne les zones géographiques spécifiques visées à l'article 11 de la loi du 20 juillet 2022, les parties requérantes relèvent que le périmètre de celles-ci n'est pas précisé mais qu'il appartient au Roi d'en établir l'étendue. Dès lors, l'obligation de conservation n'est pas strictement nécessaire et ne respecte pas le principe de légalité contenu dans l'article 22 de la Constitution. À cet égard, il y a lieu de préciser que l'article 9 de la loi du 20 juillet 2022 permet déjà une extension de la zone concernée. Selon les parties requérantes, un périmètre de zone est superflu en ce qui concerne les connexions internet fixes, dont la localisation est connue avec précision, de sorte que la mesure est disproportionnée à leur égard. En outre, la durée de la conservation des données est indéterminée pour la plupart des zones concernées, ce qui n'est pas conforme à la jurisprudence de la

Cour de justice, laquelle exige que les mesures ne durent pas plus longtemps que ce qui est absolument nécessaire à la lumière de l'objectif poursuivi et des circonstances justifiant les mesures. À cet égard, la loi du 20 juillet 2022 ne prévoit pas d'évaluation du caractère nécessaire du système. Les mesures de conservation permanente que cette loi crée sont disproportionnées.

Les parties requérantes affirment par ailleurs qu'une obligation de conservation généralisée et indifférenciée ressort de la définition des zones géographiques spécifiques, qui a pour effet que des territoires entiers de communes sont soumis à une obligation de conservation permanente. L'article 11 de la loi du 20 juillet 2022 vise également les centres de données et services dans le *cloud*, ce qui a une incidence non seulement sur les visiteurs de ces infrastructures mais aussi sur leurs utilisateurs en ligne et sur les tiers auquel celles-ci fournissent des services. Partant, l'obligation de conservation touche l'ensemble des utilisateurs à distance de ces services numériques, de sorte que quiconque utilise un service se trouvant par hasard sur ces serveurs est soumis à une conservation de données généralisée. Celle-ci n'est pas proportionnée à l'objectif de protection de l'infrastructure, dès lors qu'elle s'applique par voie détournée à tous les services proposés à distance depuis cette infrastructure. D'ailleurs, une protection et une obligation plus ciblées sont possibles. Les parties requérantes énumèrent d'autres zones géographiques ne remplissant pas le critère de stricte nécessité en raison de leur étendue. La présence d'un centre de données entraîne automatiquement une obligation de conservation qui s'étend à l'ensemble du bâtiment. Selon les parties requérantes, la protection des bâtiments affectés aux personnes morales dont le potentiel économique ou scientifique doit être protégé, constitue toutefois un critère vague. En outre, la liste précise des lieux concernés n'est pas soumise à publication. Les autoroutes, qui entraînent une très large conservation des données de toute personne qui s'y déplace avec des appareils mobiles ou qui se trouve dans les environs, sont aussi concernées. En réalité, la conservation des données de localisation sur les autoroutes constitue un enregistrement permanent des déplacements de tous les véhicules avec carte SIM intégrée et permet d'enregistrer les déplacements des citoyens.

A.26.4. En ce qui concerne l'application de la loi du 22 juillet 2022 aux fournisseurs de service de communication tels que « Skype » ou « Whatsapp », qui doivent aussi procéder à la conservation obligatoire des données de trafic et de localisation, les parties requérantes relèvent que ceux-ci ne disposent pas de la localisation de l'utilisateur et qu'ils sont dans l'impossibilité de déterminer si celui-ci se trouve ou non dans la zone géographique concernée. L'article 9 de la loi du 20 juillet 2022 impose dans cette situation la localisation satellite de l'équipement terminal. Or, l'opérateur « classique » du réseau de communication avec lequel l'utilisateur final se connecte est déjà tenu de conserver des données. Une obligation complémentaire pour les services de communications électroniques tels que « Skype » ou « Whatsapp » n'est donc ni nécessaire ni proportionnée.

A.26.5. Les parties requérantes relèvent que les données à conserver, visées par l'article 10 de la loi du 20 juillet 2022, permettent une identification de l'origine et de la destination, ainsi que de la date et de l'heure de la communication, de la nature et de la quantité des données qui sont transmises. Les données concernent en outre la localisation dans le cas d'une communication mobile, ainsi que la localisation au moment d'une communication, mais aussi à chaque moment où l'équipement terminal est démarré ou éteint ou lorsque l'opérateur cherche à connaître quels équipements terminaux sont connectés à son réseau. Autrement dit, cette disposition crée un « droit de suivi » de l'utilisateur final sans qu'une telle mesure soit nécessaire ni proportionnée. En outre, la conservation de plusieurs éléments des données est disproportionnée en soi, dès lors que ces éléments ne contribuent pas à la lutte contre la criminalité grave ou à la protection de la sécurité nationale et dès lors que les critères sont si larges que les données sont collectées de manière indifférenciée. Étant donné que les données concernant l'origine et la destination de la communication sont déjà conservées, le volume des données envoyées n'a aucune valeur ajoutée. Celui-ci permet même de révéler partiellement le contenu de la communication, de sorte que l'article 29 de la Constitution est violé. Enfin, la conservation de la taille des données transférées, qui ne peut être considérée comme une simple donnée de trafic, n'est pas strictement nécessaire, pas plus que la conservation des données d'identification de l'équipement terminal prévue à l'article 10 de la loi du 20 juillet 2022, étant donné que d'autres données permettent déjà d'identifier l'utilisateur final.

A.27. Dans une quatrième branche, les parties requérantes soutiennent que l'obligation de conservation ciblée prévue à l'article 33 de la loi du 20 juillet 2022 viole la prévisibilité exigée par l'article 22 de la Constitution, en ce que le législateur n'a pas décrit avec précision les données de trafic et de localisation. Il est précisé que la conservation s'inscrit dans l'intérêt de l'exercice des missions des services de renseignement et de sécurité. Cependant, la Cour de justice exige que la conservation soit strictement nécessaire. Par ailleurs, l'article 33 n'impose pas que l'objet de la conservation présente un lien quelconque avec un comportement suspect ou dangereux. Le fait de soumettre l'ensemble des utilisateurs potentiels de certains moyens de communications, dans de grandes zones géographiques à la mesure visée par l'article 33 constitue une obligation de conservation

généralisée et indifférenciée. En outre, aucune voie de recours ni notification de la conservation des données ne sont prévues, contrairement à ce qu'exige la Cour de justice. Le législateur n'a pas non plus prévu l'intervention préalable d'un juge, ni une mesure d'effacement des données collectées en cas d'illégalité. Il en résulte qu'une autorité est autorisée à collecter des éléments illicites sans être sanctionnée, ce qui n'est pas dissuasif.

A.28. Dans une cinquième branche, les parties requérantes critiquent l'obligation de conservation généralisée et indifférenciée contenue dans l'article 34 de la loi du 20 juillet 2022. Elles relèvent à cet égard que ni cette disposition ni d'ailleurs l'article 33 de la loi du 20 juillet 2022 ne définissent la notion de « données de trafic et de localisation », ce qui ne satisfait pas au critère de prévisibilité imposé par l'article 22 de la Constitution et par la jurisprudence de la Cour de justice. De plus, en l'absence de confirmation par arrêté royal, aucune forme de publicité n'est prévue afin d'informer les personnes qui ont fait l'objet de la mesure prévue par l'article 34 de la loi du 20 juillet 2022, ce qui ne leur permet pas d'introduire valablement un recours. Partant, l'accès à la justice est entravé alors qu'il s'agit d'un élément essentiel dans le cas d'une mesure constituant une telle ingérence dans le droit au respect de la vie privée. Le législateur n'a pas non plus précisé ce qui devait advenir des données collectées illégalement, alors que celles-ci doivent être effacées selon les exigences de la jurisprudence de la Cour de justice.

A.29. Dans une sixième branche, les parties requérantes affirment que l'article 37 de la loi du 20 juillet 2022 ne définit pas la notion de « données de trafic et de localisation », ce qui est contraire à l'article 22 de la Constitution et à la jurisprudence de la Cour de justice. L'absence de contrôle quant à la stricte nécessité de la communication des données et l'absence du caractère nécessaire de la consultation des données sont également dénoncées. Partant, l'article 37 viole les articles 10, 11 et 22 de la Constitution.

A.30. Dans une septième branche, il est relevé que la loi du 20 juillet 2022 ne prévoit aucune disposition particulière en ce qui concerne la conservation des données de trafic et de localisation des avocats, des médecins et des journalistes, alors qu'il s'agit de données sensibles relevant du secret professionnel ou du secret des sources. Selon les parties requérantes, il est requis, au regard de la protection particulière dont ces groupes professionnels bénéficient mais aussi du droit à un procès équitable, du droit au respect de la vie privée, de la liberté d'expression et de la liberté de presse, que des garanties adéquates soient prévues dès le niveau de la conservation des données pour garantir le caractère strictement nécessaire de la mesure, ce qui n'a pas été fait par le législateur. Le principe d'égalité et de non-discrimination est donc violé. En ce qui concerne le client ou le patient des groupes professionnels précités, la loi du 20 juillet 2022 constitue un recul du degré de protection du droit à l'assistance au sens de l'article 23 de la Constitution et, partant, une violation de l'obligation de *standstill* que cette disposition constitutionnelle contient. Le législateur a par ailleurs violé la présomption d'innocence et les droits de la défense, dès lors que les avocats doivent pouvoir assister leurs clients sans surveillance, et du droit à la liberté d'expression, dès lors que les données des contacts des journalistes sont visées, ce qui empêche le travail de la presse.

A.31. Un deuxième moyen est pris de la violation des articles 10, 11, 15, 22 et 29 de la Constitution, lus en combinaison ou non avec les articles 5, 6, 8, 9, 10, 11, 14 et 18 de la Convention européenne des droits de l'homme, avec les articles 7, 8, 11, 47 et 52 de la Charte, avec l'article 5, paragraphe 4, du Traité sur l'Union européenne ainsi qu'avec la directive 2002/58/CE, avec la directive (UE) 2016/680 et avec le RGPD.

A.32.1. Dans une première branche, les parties requérantes soutiennent qu'il n'est pas nécessaire de conserver certaines données visées à l'article 8 de la loi du 20 juillet 2022 jusqu'à douze mois après la fin du service, dès lors qu'il s'agit de données superflues pour déterminer l'identité de l'utilisateur si d'autres données sont déjà conservées. La conservation devrait au moins être limitée aux situations dans lesquelles aucune autre donnée n'est disponible. Les parties requérantes doutent par ailleurs de l'adéquation de la conservation de l'adresse IP, dès lors qu'il existe des méthodes empêchant de remonter à l'utilisateur final via cette adresse. Enfin, l'article 8 de la loi du 20 juillet 2022 n'impose aucune hiérarchie entre les données qu'il vise, alors que certaines données ne sont pas nécessaires lorsque d'autres sont déjà connues. Il se peut aussi que certaines données ne soient plus exactes, par exemple en cas de changement d'adresse. Au regard de ce qui précède, l'article 8 de la loi du 20 juillet 2022 viole le droit au respect de la vie privée et l'article 5, paragraphe 1, *c)* et *d)*, du RGPD.

A.32.2. Dans une deuxième branche, les parties requérantes affirment que l'article 8 impose aux services de communication électronique gratuits tels que « Whatsapp » et « Skype », en l'absence de paiement ou

d'utilisation d'un numéro de téléphone, de conserver l'adresse IP, non seulement lors de la souscription ou de l'activation, mais aussi l'adresse IP à la source de la connexion. Cette obligation implique une collecte et une conservation permanente des adresses IP de l'utilisateur, ce qui entraîne l'identification de celui-ci, alors que rien ne démontre la nécessité d'une telle mesure, puisque les autorités disposent déjà, via les opérateurs de réseau, des adresses IP attribuées à la source et peuvent, dans les cas où la conservation des données de trafic est autorisée, relier ces adresses IP au service de communications électroniques gratuit utilisé. Par ailleurs, les parties requérantes n'aperçoivent pas pourquoi ces services sont ajoutés à la définition d'« opérateurs » alors que de nombreux autres services en ligne n'y sont pas inclus. Elles soutiennent que le critère permettant de déterminer qui est un opérateur n'est pas clair, de sorte que le principe d'égalité, lu en combinaison avec le principe de légalité, est violé.

A.32.3. Dans une troisième branche, les parties requérantes allèguent que l'article 12 de la loi du 20 juillet 2022 autorise l'utilisation d'une technologie de reconnaissance faciale, ce qui constitue une mesure extrêmement intrusive présentant des risques particuliers compte tenu de la sensibilité des données concernées. Or, il existe d'autres solutions, autorisées par la loi du 20 juillet 2022, comme l'utilisation de la carte d'identité électronique avec le code PIN. En outre, il n'est pas réaliste de parler de consentement explicite et informé de l'utilisateur dans le contexte d'un point de vente, tel qu'il est exigé par le RGPD. La loi du 20 juillet 2022 ne prévoit pas non plus de consentement écrit. Or, un consentement oral ne suffit pas en l'espèce. Partant, selon les parties requérantes, la loi du 20 juillet 2022 viole l'article 22 de la Constitution et les dispositions du droit de l'Union européenne citées au moyen.

A.32.4. La quatrième branche porte sur les cartes SIM intégrées dans les véhicules. Selon les parties requérantes, l'article 12 de la loi du 20 juillet 2022, en ce qu'il prévoit la conservation obligatoire du numéro de châssis si une carte SIM est intégrée dans un véhicule, en guise d'alternative aux autres méthodes d'identification, entraîne le traçage permanent d'un véhicule via la connexion internet, dès lors que l'utilisateur final du véhicule n'a que peu de contrôle sur la carte SIM et sur cette connexion internet. Or, rien ne démontre que cette identification du véhicule soit nécessaire. Combinée avec la conservation obligatoire des données de localisation sur les autoroutes, la mesure est disproportionnée.

A.32.5. Dans une cinquième branche, les parties requérantes soutiennent que l'article 8 de la loi du 20 juillet 2022, en ce qu'il prévoit la conservation de l'adresse IP attribuée à la source et des données d'identification des équipements terminaux pour un délai de douze ou six mois, est disproportionné. Par ailleurs, l'utilisation des données n'est pas limitée aux objectifs fixés par la Cour de justice, à savoir la protection de la sécurité nationale, la prévention de menaces graves pour la sécurité publique et la lutte contre la criminalité grave, alors qu'il s'agit d'une condition essentielle. En outre, la conservation des données précitées n'est pas strictement nécessaire, dès lors que d'autres données permettent déjà d'identifier l'utilisateur final.

A.32.6. La sixième branche porte sur la présomption d'innocence. Les parties requérantes affirment que l'article 12 de la loi du 20 juillet 2022 instaure la présomption qu'un service de communications électroniques est utilisé par la personne identifiée, applicable de manière générale, y compris dans le cadre de l'enquête pénale et du droit pénal. Selon elles, cette présomption est particulièrement problématique dans une situation dans laquelle il existe déjà un doute raisonnable quant à l'utilisateur réel d'un service de communications électroniques, ce qui est courant. En réalité, cette mesure a pour effet que l'utilisateur final présumé doit fournir une preuve négative, à savoir la preuve qu'il n'est pas la personne ayant effectué la transmission de données, ce qui n'est absolument pas réaliste. Partant, l'utilisateur final est en réalité confronté à l'impossibilité de fournir une preuve contraire, en violation du droit à la présomption d'innocence et à un procès équitable.

Les parties requérantes ajoutent que, contrairement à ce que soutient le Conseil des ministres, le fait que le législateur veuille faciliter l'identification de l'abonné par la réception d'un sms de l'opérateur lors de l'utilisation d'un service fixe d'accès à internet n'est pas pertinent lorsque l'opérateur n'intervient pas lui-même dans la fourniture du service internet, par exemple dans un café ou un restaurant.

A.33. Les parties requérantes prennent un troisième moyen de la violation des articles 10, 11, 15, 22 et 29 de la Constitution, lus en combinaison ou non ou non avec les articles 5, 6, 8, 9, 10, 11, 14 et 18 de la Convention européenne des droits de l'homme, avec les articles 7, 8, 11, 47 et 52 de la Charte, avec l'article 5, paragraphe 4, du Traité sur l'Union européenne, ainsi qu'avec la directive 2002/58/CE, avec la directive (UE) 2016/680 et avec le RGPD.

A.34.1. Dans une première branche, les parties requérantes soutiennent que l'article 13 de la loi du 20 juillet 2022 ne respecte pas la jurisprudence de la Cour de justice selon laquelle il existe une stricte hiérarchie des

finalités, étant entendu que les données collectées pour la protection de la sécurité nationale ne peuvent pas être utilisées pour la lutte contre la criminalité grave. En effet, la loi du 20 juillet 2022 ne prévoit pas, lors de la conservation, un compartimentage des données fondé sur le but poursuivi et elle n'effectue pas non plus une telle distinction au moment l'accès, de sorte que l'article 13 est manifestement contraire aux dispositions citées au moyen.

A.34.2. Les parties requérantes ajoutent que la définition de la « criminalité grave » retenue à l'article 13 de la loi du 20 juillet 2022 est trop étendue et va au-delà de ce qui est strictement nécessaire, alors que cette définition a une incidence sur la possibilité d'avoir accès aux données de trafic et de localisation conservées.

A.34.3. Par ailleurs, les parties requérantes relèvent que les articles 5 et 6 de la loi du 20 juillet 2022 instaurent une obligation de conservation généralisée et indifférenciée dans le cadre de laquelle certaines autorités se voient octroyer un accès « dans le cadre de leurs missions ». Cette obligation est délimitée dans des termes trop vagues et trop larges. À cet égard, l'article 13 de la loi autorise un accès pour d'autres finalités que celles qu'a acceptées la Cour de justice, à savoir la détection et la lutte contre la fraude et les utilisations malveillantes du réseau ou du service. Le principe de prévisibilité est violé, dès lors qu'un accès est possible, notamment, pour la prévention de menaces graves contre la sécurité publique, la sauvegarde des intérêts vitaux de personnes physiques et pour la prévention, la recherche, la détection ou la poursuite d'un fait qui relève de la criminalité grave. Dans ce cadre, les compétences des autorités visées ne sont pas délimitées, de sorte que leurs pouvoirs apparaissent comme étant relativement larges.

Les parties requérantes affirment que la liste des autorités qui peuvent avoir accès aux données conservées en vertu des articles 8 et 12 de la loi du 20 juillet 2022, établie à l'article 13 de cette loi, est particulièrement longue et comprend des entités compétentes pour la détection d'infractions pénales qui ne relèvent pas de la criminalité grave, contrairement à ce qui est exigé par la Cour de justice. Partant, les dispositions citées au moyen sont violées.

A.34.4. En ce qui concerne les autorités ayant accès aux données de trafic et de localisation conservées en vertu des articles 9 et 11 de la loi du 20 juillet 2022, fixées à l'article 13 de cette loi, les parties requérantes relèvent qu'il n'est pas tenu compte de la hiérarchie exigée par la Cour de justice en ce qui concerne les finalités, de sorte que les données peuvent être utilisées à des fins de moindre importance que celle pour laquelle la conservation est autorisée, ce qui apparaît contraire aux dispositions du droit de l'Union européenne visées au moyen ainsi qu'au droit au respect de la vie privée.

A.35. Dans une deuxième branche, les parties requérantes soutiennent que les griefs dirigés contre l'article 13 de la loi du 20 juillet 2022 valent aussi pour les modalités spécifiques d'accès aux données prévues sur la base de cette disposition, énumérées aux chapitres 3 à 10 de cette loi. En effet, ces modalités sont trop larges et ne prévoient pas les garanties procédurales nécessaires, comme un contrôle indépendant au moment de l'accès aux données sensibles telles que les adresses IP attribuées à la source. Ce n'est que dans certains cas que l'intervention d'un juge d'instruction ou d'un organe administratif indépendant est prévue en ce qui concerne l'accès aux données de trafic et de localisation. Partant, ces modalités spécifiques d'accès, prévues aux articles 21, 24, 26, 27, 28, 33, 34, 35, 37, 40, 41, 42 et 44 de la loi du 20 juillet 2022, sont contraires aux dispositions du droit de l'Union européenne citées au moyen, au droit au respect de la vie privée et au droit d'accès au juge en ce qu'elles ne répondent pas à la condition de prévisibilité et de légalité.

A.36. La troisième branche est consacrée en particulier à l'accès aux données des avocats, des médecins et des journalistes. Les parties requérantes soutiennent que, hormis dans le cadre de l'article 27 de la loi du 20 juillet 2022, il n'existe pas de protection particulière pour ces professions, et ce, même dans le cas pour lequel cette loi prévoit l'intervention d'un juge d'instruction. En découle une violation du principe d'égalité au regard de la nature particulière de ces groupes professionnels. En effet, les données couvertes par le secret professionnel ou par le secret des sources journalistiques sont traitées exactement de la même manière que celles des autres personnes. Compte tenu de la protection particulière dont bénéficient ces groupes professionnels eu égard au droit à un procès équitable, au droit au respect de la vie privée, à la liberté d'expression et à la liberté de presse, il y a lieu de prévoir des garanties adéquates pour ne permettre que l'accès strictement nécessaire. Par ailleurs, les données de ces groupes professionnels sont traitées différemment selon que l'accès s'effectue sur le fondement de l'article 27 de la loi du 20 juillet 2022 ou non, ce qui constitue également une violation du principe d'égalité. Pour le surplus, les parties requérantes précisent que les développements relatifs aux données des avocats, des médecins et des journalistes, exposés dans la septième branche du premier moyen, valent *mutatis mutandis* dans le cadre de la troisième branche du troisième moyen, cette fois en ce qui concerne l'accès aux données.

A.37. Le quatrième moyen est pris de la violation des articles 10, 11, 13 et 22 de la Constitution, lus en combinaison ou non avec les articles 5, 6, 8, 9, 10, 11, 14 et 18 de la Convention européenne des droits de l'homme, avec les articles 7, 8, 11, 47 et 52 de la Charte, avec l'article 5, paragraphe 4, du Traité sur l'Union européenne ainsi qu'avec la directive 2002/58/CE, avec la directive (UE) 2016/680 et avec le RGPD. Selon les parties requérantes, en application de la directive (UE) 2016/680 et de la jurisprudence de la Cour de justice, le droit interne doit prévoir une notification à l'utilisateur dont les données de trafic et de localisation ont été consultées par les autorités chargées d'enquêtes pénales. La loi du 20 juillet 2022 ne prévoit pas une telle notification et, partant, rend l'introduction d'un recours effectif illusoire. L'article 13 de la Constitution et les articles 6 et 13 de la Convention européenne des droits de l'homme sont donc violés.

Par ailleurs, le principe d'égalité et de non-discrimination est également violé dès lors qu'une personne qui fait l'objet d'autres mesures violant les droits fondamentaux sait qu'elle en fait l'objet et peut donc s'y opposer.

Pour le surplus, les parties requérantes relèvent que la loi du 20 juillet 2022 ne prévoit pas non plus de notification en dehors d'une enquête pénale, d'une part, et qu'en ce qui concerne de nombreuses modalités de consultation organisées par cette loi, il n'est pas prévu que la consultation fasse l'objet d'un contrôle indépendant, d'autre part. La loi du 20 juillet 2022 viole donc le droit d'accès à la justice et la faculté de faire usage d'un recours effectif.

A.38. Les parties requérantes prennent un cinquième moyen de la violation des articles 10, 11, 15, 22 et 29 de la Constitution, lus en combinaison ou non 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, avec l'article 5, paragraphe 4, du Traité sur l'Union européenne, ainsi qu'avec la directive 2002/58/CE, avec la directive (UE) 2016/680 et avec le RGPD. Elles soutiennent que l'interdiction, prévue à l'article 3 de la loi du 20 juillet 2022, pour les opérateurs d'avoir recours à la cryptographie si celle-ci empêche l'identification de l'utilisateur final ou la détection ou la localisation d'une communication constitue une ingérence disproportionnée dans le droit au respect de la vie privée des intéressés et va au-delà de ce qui est nécessaire dans une société démocratique. Une telle interdiction n'est pas nécessaire et les autorités compétentes disposent en outre de nombreuses autres possibilités pour repérer une communication et identifier des utilisateurs, qui sont moins drastiques qu'une interdiction générale pour l'opérateur. L'interdiction de la cryptographie rend les données accessibles, alors qu'une donnée cryptée n'est pas une donnée illégale par définition. Ainsi, des données qui ne concernent pas les pouvoirs publics deviennent également accessibles. Une telle interdiction a également des conséquences pour tous les utilisateurs de l'opérateur, étant donné que celui-ci devra opter pour une technologie de sécurisation plus faible afin de pouvoir satisfaire aux demandes des autorités compétentes.

A.39. Enfin, les parties requérantes prennent un sixième moyen de la violation des articles 10, 11, 22 et 29 de la Constitution, lus en combinaison ou non 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 et avec la directive 2002/58/CE. Elles allèguent que les mesures prévues à l'article 4, § 2, de la loi du 20 juillet 2022 peuvent être mises en œuvre pour des finalités qui dépassent le simple bon fonctionnement des services de communications électroniques, notamment à des fins de censure. Or, le législateur n'a prévu aucune évaluation par un organe indépendant, ni aucun critère d'évaluation clair. En réalité, l'opérateur se voit confier tout le soin d'évaluer s'il est satisfait à la définition de « fraude » ou d'« utilisateur malveillant du réseau ou du service » et de jauger l'adéquation et la proportionnalité d'une mesure. La définition d'« utilisation malveillante du réseau ou du service » est en outre bien trop large, dès lors qu'elle comprend toute utilisation d'un réseau ou service de communications électroniques aux fins de « provoquer des dommages ». Une telle définition ouvre la porte à la censure et permet de bloquer, sans contrôle judiciaire, des opinions jugées nuisibles. Partant, l'article 4 de la loi du 20 juillet 2022 viole la liberté d'expression et d'information.

En ce qui concerne la position du Conseil des ministres

Affaire n° 7907

A.40.1. En ce qui concerne les première et deuxième branches du moyen unique, le Conseil des ministres soutient que l'article 27, 2°, de la loi du 20 juillet 2022 limite drastiquement l'ingérence dans le secret

professionnel de l'avocat. Il précise que la mesure visée par cette disposition consiste en l'accès, ordonné par le juge d'instruction, aux métadonnées relatives au moyen de communication électronique détenu par un avocat ou par un médecin. Cette mesure ne peut être exécutée que si l'avocat ou le médecin est lui-même soupçonné d'avoir commis ou participé à une infraction grave visée à l'article 88*bis*, § 1er, du Code d'instruction criminelle, ou si des faits précis laissent présumer que des tiers soupçonnés d'avoir commis une telle infraction utilisent le moyen de communication concerné. En ce qui concerne les avocats, le bâtonnier est systématiquement averti de la mesure. Le Conseil des ministres ajoute que l'article 27, 2°, de la loi du 20 juillet 2022 ne suppose aucun concours actif de l'avocat et ne porte pas sur le contenu des communications, mais uniquement sur les métadonnées relatives au moyen de communication concerné.

En outre, le Conseil des ministres considère que l'ingérence dans le secret professionnel de l'avocat est justifiée au regard d'objectifs d'intérêt général précis et documentés dans les travaux préparatoires de la loi du 20 juillet 2022. En effet, celle-ci poursuit un objectif de protection des citoyens, en ce compris des avocats, eu égard au tournant numérique que prend la société, qui rejaillit sur les formes les plus graves de criminalité et d'atteintes à la sécurité nationale. Il s'agit d'objectifs légitimes. Dans ce cadre, l'article 27, 2°, de la loi du 20 juillet 2022 n'autorise l'accès aux métadonnées que dans des hypothèses d'infractions considérées comme relevant de la criminalité grave.

A.40.2. Selon le Conseil des ministres, l'interprétation de l'article 27, 2°, de la loi du 20 juillet 2022 par la partie requérante dans l'affaire n° 7907 est erronée, dès lors que cette disposition vise les moyens de communications des avocats dans leur globalité, c'est-à-dire à la fois comme émetteurs et comme récepteurs des communications électroniques, ainsi qu'il est précisé dans les travaux préparatoires. Partant, les deux premières branches du moyen unique reposent sur une interprétation erronée de la disposition attaquée et ne sont pas fondées. Dans l'hypothèse où il existerait un doute quant à l'interprétation correcte à conférer à l'article 27, 2°, de la loi du 20 juillet 2022, il revient à la Cour d'acter une interprétation de cette disposition qui soit conforme aux dispositions citées au moyen.

A.40.3. Le Conseil des ministres ajoute que l'article 27, 2°, de la loi du 20 juillet 2022 est une forme classique, adéquate et proportionnée de disposition protectrice du secret professionnel des avocats. Elle emprunte d'ailleurs une formulation comparable à d'autres dispositions du Code d'instruction criminelle visant à protéger le secret professionnel de l'avocat, lesquelles ont d'ailleurs été validées par la Cour constitutionnelle, à savoir les articles 39*bis*, § 9, 56*bis*, § 3, et 90*octies* de ce Code, qui se focalisent sur les outils professionnels de l'avocat, comme les moyens de communication, les systèmes informatiques, les locaux ou les résidences, plutôt que sur les interactions des clients avec ces outils. De manière similaire au système prévu par ces dispositions, la protection spécifique prévue à l'article 27, 2°, de la loi du 20 juillet 2022 ne remet pas en cause le secret professionnel qui attaché aux métadonnées relatives à d'autres outils de communication, par exemple ceux qui sont détenus par le client lui-même. Dans le cadre de l'instruction, il appartient au juge d'instruction de trier les métadonnées récoltées relativement à d'autres outils de communication, pour écarter les données protégées par le secret professionnel de l'avocat.

Le Conseil des ministres rappelle que la protection procédurale spécifique mise en place *a priori* par l'article 27, 2°, de la loi du 20 juillet 2022 ne vise que les moyens de communication détenus par les avocats, précisément parce que ceux-ci sont dépositaires du secret professionnel en vertu de l'article 458 du Code pénal, qu'ils entretiennent une relation de confiance avec leurs clients et qu'ils relèvent d'instances organisées par la loi chargées de veiller au respect de la déontologie professionnelle. À cet égard, l'intervention obligatoire du bâtonnier, prévue par la disposition attaquée, constitue une garantie importante du secret professionnel de l'avocat.

A.40.4. Le Conseil des ministres ajoute que les éléments protégés par le secret professionnel ne sont pas consignés au procès-verbal. Ces éléments ne sont pas détruits immédiatement, mais conservés dès lors que la mise en balance entre les intérêts protégés par le secret professionnel et ceux qui pourraient lui être supérieurs est une analyse essentiellement casuistique, comme il ressort de la jurisprudence de la Cour et de celle de la Cour de cassation. La suppression définitive des données conservées ne survient qu'à la fin des différentes durées de conservation établies dans la loi du 20 juillet 2022. Par ailleurs, la disposition attaquée prévoit l'intervention systématique du juge d'instruction, ce qui est conforme à la jurisprudence de la Cour de justice.

A.41.1. En ce qui concerne les troisième et quatrième branches, le Conseil des ministres estime tout d'abord que la conservation des métadonnées relatives au moyen de communication des avocats n'implique pas

d'ingérence dans le secret professionnel. En réalité, l'Ordre des barreaux francophones et germanophone confond la conservation des métadonnées et l'accès à ces données. Selon le Conseil des ministres, il faut distinguer la protection accordée au secret professionnel de l'avocat et la protection de la vie privée des individus. En ce qui concerne le secret professionnel, seul l'accès aux métadonnées est susceptible d'engendrer une ingérence concrète, contrairement à la conservation des données, qui apparaît comme étant neutre vis-à-vis du secret professionnel, dès lors que les données sont stockées par les opérateurs qui ignorent l'activité professionnelle de leurs abonnés. Par ailleurs, la loi du 20 juillet 2022 érige en infraction pénale tout accès non autorisé aux métadonnées conservées par les opérateurs en vertu de cette loi.

A.41.2. Selon le Conseil des ministres, la mise en place d'un filtre préventif, tel qu'il est évoqué par l'Ordre des barreaux francophones et germanophone, serait impraticable, contre-productive et potentiellement discriminatoire, outre qu'il n'appartient pas à la Cour de se substituer au législateur sur l'opportunité d'une mesure législative, qui relève du choix politique du législateur. En effet, un tel système entraînerait des difficultés techniques de mise en œuvre, qui ressortent des travaux préparatoires de la loi du 20 juillet 2022. Les bases de données des opérateurs devraient être obligatoirement liées à la qualité professionnelle des avocats, ce qui obligerait tous les avocats à disposer d'une ligne téléphonique professionnelle. Les opérateurs seraient par ailleurs obligés d'interroger leurs clients professionnels afin de déterminer leurs activités et de vérifier cette information auprès de l'ordre professionnel concerné. En outre, la liste des avocats change constamment au gré des nouvelles arrivées au barreau, des radiations et des départs en retraite, ce qui exigerait une mise à jour continue qui engendrerait une charge de travail impraticable pour les opérateurs et pour les ordres professionnels concernés. Pour les adresses IP, le filtrage à l'entrée serait inopérant, dès lors que la plupart de celles-ci sont des adresses dynamiques dont l'attribution varie constamment. D'autres difficultés émergeraient lorsque les personnes en communication sont abonnées auprès d'opérateurs différents, qui devraient s'échanger en permanence des données pour identifier quelles données conserver. Les avocats inscrits aux barreaux étrangers mais séjournant à Bruxelles ne seraient quant à eux pas couverts par le filtre à l'entrée, ce qui créerait une discrimination entre les avocats inscrits à un barreau belge et les autres avocats, alors que tous sont pourtant tenus au secret professionnel.

Le Conseil des ministres ajoute que ce filtre serait contre-productif, dès lors qu'il impliquerait d'identifier d'entrée de jeu les avocats dans les bases de données constituées en application de la loi, ce qui permettrait de tirer systématiquement des conclusions à partir des métadonnées des clients. Enfin, d'un point de vue juridique, ce système aurait pour effet de transformer le devoir attaché au secret professionnel en un privilège pour l'avocat, ainsi que pour les personnes qui parviendraient à détourner les moyens de communication détenus par un avocat. En effet, les métadonnées seraient de toute façon immunisées, même si le moyen de communication était utilisé à des fins criminelles. En réalité, la conservation des métadonnées de l'avocat est également susceptible de protéger celui-ci, puisqu'une procédure spécifique d'accès aux métadonnées conservées est prévue en cas de disparition inquiétante d'une personne dont il existe des indices sérieux portant à croire que son intégrité physique se trouve en danger imminent, ce qui peut être le cas d'un avocat.

A.41.3. Le Conseil des ministres ajoute par ailleurs que la loi du 20 juillet 2022 met en place une conservation ciblée des métadonnées, justifiée par les objectifs poursuivis et conforme à la jurisprudence de la Cour. En effet, si la conservation des données est ciblée sur la base de critères géographiques, l'accès aux métadonnées est strictement encadré par l'article 13 de la loi du 20 juillet 2022. L'exposé des motifs de cette loi précise par ailleurs de manière transparente pourquoi la conservation ne peut être ciblée que sur la base de critères géographiques. Le Conseil des ministres précise en outre que, par l'adoption de la loi du 20 juillet 2022, le législateur exerce la marge d'appréciation que lui reconnaît la jurisprudence européenne en matière de protection des données, en prenant soin de se conformer aux indications fournies par cette jurisprudence. C'est notamment le cas de l'utilisation des critères géographiques précités, qui renvoient à cinq catégories de lieux, correspondant à des catégories mises en évidence par la Cour de justice elle-même. Il s'agit des zones caractérisées par un taux important de criminalité grave, par un niveau de menace grave, par une exposition particulière à la criminalité grave, par une menace grave potentielle pour les intérêts vitaux du pays ou pour les besoins essentiels de la population, et par une menace potentielle grave pour les intérêts des institutions internationales établies sur le territoire national. Le délai de conservation des données est par ailleurs adapté au degré d'intensité de la criminalité dans chaque zone. Ces choix sont justifiés dans les travaux préparatoires au moyen d'exemples concrets et prenant comme référence la jurisprudence de la Cour et celle de la Cour de justice. En toute hypothèse, la partie requérante ne démontre pas en quoi la marge d'appréciation reconnue par la jurisprudence de la Cour de

justice aurait été mise en œuvre de manière disproportionnée ni en quoi la justification minutieuse de la mesure serait entachée d'erreurs ou de lacunes.

Le Conseil des ministres souligne que la loi du 20 juillet 2022 procède d'un équilibre complexe réalisé par le législateur, notamment sur le plan technique. Cette complexité est confirmée par l'entrée en vigueur différée prévue par l'article 45, alinéa 1er, de cette loi, qui témoigne de l'équilibre trouvé par le législateur entre différents intérêts légitimes, à savoir la protection de l'État et de ses citoyens, le respect de la vie privée et les capacités techniques des opérateurs. Le Conseil des ministres rappelle par ailleurs que la Cour n'exerce pas de contrôle juridictionnel sur le contenu des travaux préparatoires ni sur le processus d'élaboration de la loi. En outre, l'appréciation des dispositifs techniques envisageables relève de la marge d'appréciation du pouvoir législatif, en particulier dans les domaines techniquement complexes.

Affaires n^os^ 7929, 7930, 7931 et 7932

La conservation des données

A.42.1. En ce qui concerne les critiques des parties requérantes à propos de la conservation des données, le Conseil des ministres soutient que les articles 8 et 12 de la loi du 20 juillet 2022, qui imposent aux opérateurs de conserver les données d'identification des utilisateurs finaux pendant une période de douze mois, d'identifier les abonnés et de conserver certaines données permettant d'identifier ceux-ci, sont proportionnés. Selon lui, il n'est pas toujours facile, en pratique, d'identifier un utilisateur final, un équipement ou un service, de sorte qu'il est parfois nécessaire de conserver des données complémentaires ou de croiser des données pour obtenir une identification exacte au sens de l'article 5, paragraphe 1, *d)*, du RGPD, comme le précisent les travaux préparatoires de la loi du 20 juillet 2022. Par ailleurs, il est essentiel que les opérateurs conservent suffisamment de données d'identification pour permettre aux autorités d'identifier rapidement, précisément et sans erreur les personnes, équipements ou services qui présentent un intérêt pour l'enquête. À cet égard, chaque type de donnée d'identification a fait l'objet d'une justification minutieuse dans les travaux préparatoires. Par ailleurs, la liste des données visées est issue d'une consultation publique et des apports techniques des opérateurs. En outre, les bases de données sont réalisées de manière automatisée en application de l'article 8 de la loi du 20 juillet 2022, ce qui ne permet de tenir compte de chaque cas individuel qu'au seul stade de l'accès à une donnée conservée. Pour le surplus, il revient au Roi de préciser les données visées, dans le respect du RGPD et de la loi du 30 juillet 2018, afin d'adapter les bases de données aux évolutions techniques à venir.

Au sujet de la période de douze mois de conservation des données, le Conseil des ministres soutient que cette durée est justifiée dans les travaux préparatoires et que ce délai générique est assorti de nuances afin de correspondre aux réalités techniques auxquelles sont confrontés les opérateurs. Partant, le législateur a pris soin de fixer des délais correspondant à ses besoins en ce qui concerne les finalités poursuivies.

A.42.2. À propos de la critique relative à la nécessité d'étendre l'obligation de conservation des données aux opérateurs tels que « WhatsApp » ou « Skype », le Conseil des ministres relève qu'en vertu de la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 « établissant le code des communications électroniques européen (refonte) », certains services fournis par ces opérateurs sont désormais inclus dans la définition de « services de communications électroniques », de sorte que ceux-ci ont la qualité d'opérateur au même titre que les opérateurs traditionnels. En réalité, les parties requérantes critiquent la définition même et non la loi du 20 juillet 2022. En toute hypothèse, dès lors que les entreprises précitées fournissent des services de communications électroniques, il est justifié, dans le respect des principes d'égalité de traitement, de non-discrimination et de neutralité technologique, de traiter celles-ci de la même manière que les fournisseurs de services de communications traditionnels en ce qui concerne la conservation des données d'identification, d'autant que les personnes faisant l'objet d'enquêtes utilisent de plus en plus les services des « nouveaux » opérateurs.

A.42.3. Le Conseil des ministres observe, au sujet de la critique relative à l'article 12 de la loi du 20 juillet 2022, qui permet à un opérateur d'identifier un de ses abonnés via la carte SIM embarquée dans un véhicule, que cette disposition n'autorise aucunement le traçage des personnes. Il ne s'agit que d'une manière de retrouver l'identité du conducteur principal du véhicule, qui est minutieusement justifiée dans les travaux préparatoires, ce qui atteste d'une mise en balance effective des intérêts opérée sur ce point précis. Le Conseil des ministres ajoute

que cette mesure est autorisée par la jurisprudence de la Cour de justice, dès lors qu'elle ne permet pas concrètement de déduire des informations relatives aux communications effectuées par le conducteur.

A.42.4. Selon le Conseil des ministres, l'identification de l'adresse IP source, prévue à l'article 13 de la loi du 20 juillet 2022, est conforme à la jurisprudence de la Cour de justice. Par ailleurs, la nécessité de conserver l'identifiant de l'équipement terminal de l'utilisateur final, notamment l'identité internationale d'équipement mobile, l'identifiant permanent de l'équipement et l'adresse du contrôleur d'accès au réseau, visés par l'article 8 de cette loi, fait l'objet d'un exposé précis dans les travaux préparatoires. La conservation de ces données est en outre encadrée par l'article 13 de la loi.

A.42.5. Par ailleurs, la Cour a déjà, par l'arrêt n° 158/2021 du 18 novembre 2021 (ECLI:BE:GHCC:2021:ARR.158), répondu aux critiques relatives à la présomption d'utilisation par la personne identifiée, prévue à l'article 12 de la loi du 20 juillet 2022. En effet, dans le cadre de l'utilisation du réseau wifi, l'abonné de l'opérateur peut renverser la présomption prévue dans cette disposition en démontrant qu'il n'est pas le seul utilisateur de ce réseau. En ce qui concerne plus spécifiquement les services fixes d'accès à internet utilisés par des personnes physiques en dehors de leur lieu de résidence et de leur lieu d'exercice d'activité professionnelle, comme les services de communications électroniques offerts gratuitement à l'aide de bornes wifi, le législateur entend faciliter l'identification de l'abonné, notamment par la réception d'un SMS de l'opérateur. Enfin, quant à la critique relative à l'utilisation d'une borne wifi à l'insu de l'abonné, le Conseil des ministres précise qu'il incombe à celui-ci de prendre les mesures adéquates et nécessaires pour empêcher de telles intrusions. Aucune violation de la présomption d'innocence ou des droits de la défense ne ressort de ce qui précède.

A.42.6. Le Conseil des ministres observe, au sujet des critiques générales relatives à la conservation des métadonnées, que l'article 5 de la loi du 20 juillet 2022 vise à lutter contre la fraude et l'utilisation malveillante des réseaux ainsi qu'à permettre la sécurité et le bon fonctionnement des réseaux. Pour ce faire, il impose notamment la conservation de certaines métadonnées jugées nécessaires, ce qui suppose que les opérateurs réalisent une mise en balance des intérêts en présence dans chaque cas de conservation, ainsi qu'il ressort des travaux préparatoires. En effet, dans le cadre de la lutte contre la fraude et l'utilisation malveillante de réseaux, les opérateurs sont les mieux placés pour examiner concrètement la nécessité de conserver des métadonnées dans le cadre des objectifs prévus par le législateur. Le caractère nécessaire de cette mesure a par ailleurs été justifié avec précision dans les travaux préparatoires. Un test de nécessité est du reste prévu en amont de la conservation effectuée par les opérateurs. Enfin, l'article 5 de la loi du 20 juillet 2022 ne fait nullement double emploi avec l'article 107/2 de la loi du 13 juin 2005, dès lors que l'articulation entre ces dispositions fait l'objet d'une explication dans les travaux préparatoires de la loi du 20 juillet 2022. En réalité, celles-ci sont complémentaires, dès lors que l'article 107/2 de la loi du 13 juin 2005 oblige les opérateurs à prendre les mesures nécessaires pour gérer le risque en matière de sécurité des réseaux et des services, tandis que l'article 5 de la loi du 20 juillet 2022 permet aux opérateurs de collecter et de conserver des données de manière à répondre à l'obligation légale précitée. En effet, l'article 107/2 de la loi du 13 juin 2005, pris isolément, ne constitue pas une base légale suffisante pour permettre le traitement et la conservation des données visées, dès lors qu'il s'agit d'une ingérence dans le droit au respect de la vie privée et compte tenu de la protection particulière dont bénéficient les données de trafic et de localisation. Autrement dit, sans l'article 5 de la loi du 20 juillet 2022, les opérateurs ne seraient pas en mesure de collecter et de conserver lesdites données de manière conforme à la directive 2002/58/CE, qui est moins flexible et plus stricte que le RGPD, par rapport auquel elle constitue une *lex specialis*. Les droits et libertés des personnes concernées ne sont donc nullement amoindris par l'adoption de l'article 5 de la loi du 20 juillet 2022.

A.42.7. Au sujet de la prévisibilité et du contrôle de légalité de la conservation et de l'accès aux données de trafic et de localisation requis par les services de renseignement, le Conseil des ministres soutient que l'article 34 de la loi du 20 juillet 2022 met scrupuleusement en œuvre la jurisprudence de la Cour de justice relative à la directive 2002/58/CE. Il ressort d'ailleurs des concepts juridiques utilisés par l'article 34 précité que la prévisibilité de la mesure est garantie et que, dans chaque situation de menace grave pour la sécurité nationale, seules les données strictement nécessaires à la réalisation de l'objectif poursuivi sont conservées. Un raisonnement identique s'impose en ce qui concerne l'article 37 de la loi du 20 juillet 2022, qui fait par ailleurs l'objet d'un contrôle par une autorité indépendante.

A.43.1. Dans son mémoire en réplique, le Conseil des ministres apporte plusieurs précisions complémentaires au sujet des critiques des parties requérantes relatives à la conservation des données.

A.43.2. Tout d'abord, le Conseil des ministres soutient qu'il y a bien lieu d'opérer une distinction entre les données d'identification et les métadonnées dans le cadre de la loi du 20 juillet 2022. L'autre définition des métadonnées proposée par la partie requérante dans l'affaire n° 7931 n'est, à cet égard, pas correcte. En outre, la jurisprudence de la Cour de justice n'a pas identifié de manière exhaustive les données qui pouvaient faire l'objet d'une obligation de conservation ni les données d'identification qui pouvaient faire l'objet d'une ingérence sous la forme d'une obligation de conservation généralisée. En réalité, le législateur belge a réalisé un exercice plus complet et précis que celui auquel s'est livrée la Cour de justice, qui ne s'est prononcée que sur l'adresse IP et sur les données d'identité civile. Ces données sont d'ailleurs insuffisantes pour réaliser la finalité d'identification, dès lors qu'il importe de croiser les informations relatives à l'identité civile pour s'assurer de leur fiabilité. En outre, l'identité civile n'est pas récoltée par les opérateurs de services de communications interpersonnelles non fondées sur la numérotation. Par ailleurs, l'adresse IP à la source est elle aussi insuffisante, en ce que certaines infractions peuvent être commises à l'aide d'un service de communications électroniques pour lequel l'adresse IP n'est pas utilisée. Enfin, la conservation de la seule adresse IP, sans les date et heure de la communication ni le port utilisé, ne permet pas d'identifier l'utilisateur dans le cas des adresses IP partagées.

Le Conseil des ministres ajoute que, contrairement à ce que soutient la partie requérante dans l'affaire n° 7930, l'adresse IP à la source ne permet pas à elle seule de reconstituer l'historique complet d'un utilisateur d'internet. C'est dans cette logique que le législateur a choisi de traiter l'adresse IP en tant que donnée d'identification lorsqu'elle est utilisée à cette seule fin et en tant que métadonnée soumise à un régime très strict dans les autres cas. Il en va de même pour les autres données techniques qui permettent d'identifier l'utilisateur d'un service. De manière générale, le Conseil des ministres observe que l'ensemble des données visées à l'article 8 de la loi du 20 juillet 2022 répondent à l'objectif unique d'identifier l'utilisateur. La circonstance que ces données sont nombreuses n'emporte pas une ingérence plus grave que si leur nombre était plus réduit, dès lors qu'aucune de ces données ne révèle autre chose que l'identité de la personne visée.

A.43.3. À propos des conditions de l'obligation des données de conservation, le Conseil des ministres relève que le délai de conservation est pertinent pour apprécier le degré d'ingérence de la mesure dans les droits fondamentaux. En l'espèce, le fait que la loi du 20 juillet 2022 distingue plusieurs hypothèses de délai témoigne de la volonté du législateur de limiter au strict nécessaire l'obligation de conservation, y compris dans sa durée. Du reste, la jurisprudence de la Cour de justice citée par la partie requérante dans l'affaire n° 7930 n'est pas pertinente en l'espèce puisqu'elle concerne les données relatives au trafic et à la localisation, et non les données d'identification. En outre, le Conseil des ministres concède que la conservation des données, d'une part, et l'accès aux données, d'autre part, constituent des opérations distinctes. Cependant, la conservation à elle seule est inutile pour lutter contre la criminalité ou pour garantir la sécurité nationale. Il est donc artificiel d'envisager la conservation des données sans avoir à l'esprit les règles qui gouvernent l'accès à celles-ci. Par ailleurs, le Conseil des ministres met en évidence que les différents avis récoltés dans le cadre de l'élaboration de la loi du 20 juillet 2022 attestent d'un équilibre entre différents objectifs, illustrés par le point de vue des acteurs de terrain. Du reste, en ce qui concerne l'absence de données statistiques qui seraient, selon la partie requérante dans l'affaire n° 7930, indispensables pour autoriser une ingérence dans le droit au respect de la vie privée, le Conseil des ministres relève que le législateur n'est pas soumis à la production de sources documentaires ni à la vérification qu'une méthode particulière a été observée, sans préjudice des exigences prévues par la Constitution ou par la loi. La Cour, quant à elle, n'est pas compétente pour vérifier la manière de travailler du législateur ni le fondement scientifique d'une mesure législative.

A.43.4. Le Conseil des ministres ajoute, en ce qui concerne la lutte contre la fraude et l'utilisation malveillante de réseaux, ainsi que la sécurité et le bon fonctionnement des réseaux, dont il est question à l'article 5 de la loi du 20 juillet 2022, que les données visées dans cette disposition sont des informations qui sont toujours nécessaires pour permettre au service de médiation de remplir sa mission et de communiquer au plaignant l'identité de l'auteur d'appels malveillants. Il n'est donc pas nécessaire de laisser une marge d'appréciation à l'opérateur. Par ailleurs, la finalité de lutte contre la fraude et contre l'utilisation malveillante des réseaux, ainsi que la sécurité et le bon fonctionnement des réseaux ne sont pas exclues par la jurisprudence de la Cour de justice, laquelle ne s'est pas prononcée sur ces sujets. En outre, certaines données visées à l'article 5 de la loi du 20 juillet 2022 sont en toute hypothèse déjà utilisées par les opérateurs pour détecter les incidents ou les anomalies ainsi que pour gérer et optimiser les flux de trafic sur leurs réseaux. Enfin, selon le Conseil des ministres, l'article 15, paragraphe 1, de la directive 2002/58/CE et l'article 23 du RGPD constituent un fondement valable de l'article 5 de la loi du 20 juillet 2022, comme les travaux préparatoires de cette loi le mettent en évidence.

L'obligation de conservation ciblée des données et le critère de différenciation géographique

A.44.1. En ce qui concerne les critiques des parties requérantes à propos de l'obligation de conservation ciblée des métadonnées et à propos du critère de différenciation géographique, le Conseil des ministres commence par relever que si la Cour de justice a condamné l'obligation de conservation généralisée de données, elle a néanmoins formulé des suggestions d'approches alternatives, notamment une différenciation des catégories de personnes et une différenciation sur une base géographique. Selon le Conseil des ministres, le législateur a suivi cette seconde suggestion avec l'adoption de l'article 9 de la loi du 20 juillet 2022. Les critères géographiques énumérés dans cette disposition procèdent de la recherche d'un équilibre entre les intérêts en présence et constituent par ailleurs une application scrupuleuse de la jurisprudence de la Cour de justice, qui suggère qu'un critère géographique soit basé sur le risque de préparation ou de commission d'infraction, évalué de manière objective. Le législateur a traduit cette invitation en distinguant cinq catégories de lieux correspondant aux catégories listées par la Cour de justice, mais avec davantage de précision.

Par ailleurs, le Conseil des ministres souligne que le législateur a veillé à la proportionnalité de la mesure en prévoyant des critères quantitatifs progressifs, de sorte que, même dans les lieux visés par l'obligation de conservation, une distinction est faite en fonction de l'intensité de la matérialisation du critère géographique retenu. La détermination du niveau de ces critères relève, pour le surplus, de la marge d'appréciation du législateur et échappe au contrôle de la Cour. Le Conseil des ministres ajoute que les lieux pour lesquels une conservation est prévue sont liés à une variable, c'est-à-dire une donnée susceptible d'évoluer dans le temps, de sorte que le lieu concerné sera visé ou non par l'obligation de conservation en fonction de l'évolution de la variable. Le législateur a donc élaboré un dispositif clair et précis, dont l'application n'est pas figée. Par ailleurs, un mécanisme de contrôle périodique est établi afin de garantir que la conservation ne soit pas maintenue lorsque le lieu ne correspond plus aux critères prévus par la loi en raison de l'évolution de la situation concrète. L'obligation de conservation est donc limitée au strict nécessaire et cette nécessité fait l'objet d'un contrôle périodique strict. En outre, le législateur a prévu que l'atteinte d'un seuil, concernant un critère quantitatif, en raison de l'évolution d'une variable qui y est attachée, est parfaitement objectivée. Il a en effet lui-même déterminé, de manière précise, la source fiable et objective qui devait être prise en considération pour apprécier l'évolution des variables, à l'article 11 de la loi, qui énonce les sources prises en compte. En ce qui concerne l'entrée en vigueur différée de la loi du 20 juillet 2022, prévue à l'article 45, alinéa 1er, de cette loi, le Conseil des ministres relève qu'il revient en premier lieu au législateur de régler l'effet dans le temps des nouvelles dispositions législatives. Pour le surplus, l'entrée en vigueur différée témoigne de l'équilibre entre différents intérêts légitimes, à savoir les finalités de protection de l'État et de ses citoyens, le respect de la vie privée et les capacités techniques des opérateurs. Dès lors que le législateur a fait le choix de prévoir une obligation de conservation ciblée, cela engendre certaines difficultés techniques pour les opérateurs, de sorte qu'il est justifié et proportionné de leur laisser un certain temps afin de mettre en place les nouvelles mesures.

A.44.2. La mise en œuvre concrète de la différenciation géographique n'aboutit pas, selon le Conseil des ministres, à une obligation de conservation indifférenciée, comme le mettent en évidence les travaux préparatoires. La circonstance que la loi du 20 juillet 2022 peut entraîner, à un moment donné, une obligation de conservation généralisée n'est pas de nature à modifier ce constat, dès lors que, dans cette hypothèse théorique, l'obligation serait différenciée. Par ailleurs, si l'ensemble du territoire devait être visé, ce serait par la conjonction de l'application de critères objectifs et proportionnés. En outre, les critères géographiques sont utilisés sur la base de variables qui ne sont pas figées dans le temps, de sorte que, dans le cas où l'ensemble des zones du territoire devrait être caractérisé par un taux de criminalité élevé, il s'agirait d'une situation exceptionnelle et temporaire. La critique des parties requérantes selon laquelle le nombre des zones et lieux visés dans la loi du 20 juillet 2022 serait particulièrement élevé alors que la Belgique est un État à taille réduite n'est pas fondée. En effet, les travaux préparatoires exposent soigneusement les raisons pour lesquelles la loi comporte tel lieu ou tel critère de différenciation géographique. Par ailleurs, la Belgique présente certaines caractéristiques spécifiques qui la différencient des autres États voisins et qui engendrent un nombre et une densité plus grande de lieux justifiant l'imposition ciblée d'une obligation de conservation des métadonnées.

Le Conseil des ministres ajoute que les critères de différenciation géographiques cités à titre d'exemple par la Cour de justice ne sont pas cumulatifs. Du reste, s'il est vrai qu'il n'est pas possible de déterminer à l'avance quel pourcentage du territoire ou de la population pourrait être concerné par l'obligation de conservation différenciée des métadonnées, cette mesure ne doit pas pour autant être considérée comme étant disproportionnée. Au contraire, le système est proportionné en raison précisément du caractère évolutif et non figé des variables retenues par les critères établis par le législateur. En particulier, le Conseil des ministres soutient que le critère lié

aux faits de criminalité grave au niveau de l'arrondissement judiciaire ou de la zone de police n'est ni injustifié, ni disproportionné. L'arrondissement judiciaire est en effet le niveau auquel les données statistiques pertinentes sont principalement établies. Par ailleurs, le recours à la zone de police permet de pallier les disparités trop grandes qui pourraient survenir au sein d'un même arrondissement judiciaire et d'apporter davantage de précisions. Enfin, il n'est pas opportun de découper le territoire en des zones plus petites qu'une zone de police, dès lors que la fiabilité des données risque d'être altérée, d'une part, et qu'une charge de travail disproportionnée est susceptible d'être engendrée, notamment pour les opérateurs, d'autre part. Au sujet de la fiabilité des données statistiques récoltées, le Conseil des ministres soutient que le législateur a pris le soin de recourir aux sources les plus objectives possibles pour l'observation de l'évolution des variables utilisées, que les statistiques policières concernées sont actuelles et que celles-ci portent sur des faits indépendamment des suites procédurales qui y sont réservées, de sorte que ces données permettent de donner une image fidèle du caractère criminogène d'une zone.

A.44.3. À propos de la référence faite à l'article 11 de la loi du 20 juillet 2022 aux infractions graves définies à l'article 90*ter* du Code d'instruction criminelle, le Conseil des ministres relève que la Cour de justice ne définit pas elle-même la notion de criminalité grave, de sorte qu'il appartient aux États membres de déterminer celle-ci. Les travaux préparatoires apportent de nombreuses précisions dans ce cadre. En toute hypothèse, les parties requérantes ne démontrent pas en quoi la référence à l'article 90*ter* du Code d'instruction criminelle s'écarte de l'objectif de lutte contre la criminalité grave, compte tenu des compétences des États membres de l'Union européenne ni en quoi le législateur aurait excédé la marge nationale d'appréciation. Pour le surplus, le Conseil des ministres soutient que la référence à l'article 90*ter* du Code d'instruction criminelle est adéquate, dès lors que cette disposition vise des infractions pour lesquelles le juge d'instruction dispose de pouvoirs d'enquête spécifiques, précisément parce que le Code précité considère ces infractions comme étant graves. Il n'était dès lors pas pertinent de recourir à une définition *ad hoc* de la notion d'infraction grave dans la loi du 20 juillet 2022.

A.44.4. La circonstance que l'article 11 de la loi du 20 juillet 2022 autorise le Roi à étendre la liste des lieux et des zones visées par l'obligation de conservation ciblée des métadonnées ne viole aucunement le principe de légalité, dès lors qu'il n'existe aucune marge d'appréciation dans le cadre de cette extension, puisque l'ajout des zones géographiques doit répondre aux critères de la loi et que l'arrêté royal pris sur cette base doit être renouvelé tous les trois ans. Partant, cette mesure permet d'adapter la liste avec plus de souplesse que la loi, mais sans violer le principe de légalité. Il en va de même en ce qui concerne la question de la fixation du périmètre des zones, examinée par la section de législation du Conseil d'État qui a estimé qu'il importait que la détermination de ce périmètre soit attribuée à une seule autorité, à savoir, en l'espèce, le Roi.

A.44.5. À propos de la critique des parties requérantes relative à la conservation des métadonnées en dehors des zones géographiques identifiées, le Conseil des ministres soutient que la loi du 20 juillet 2022 ne vise pas à conserver les métadonnées d'une personne se situant en dehors d'une zone ou d'un lieu visé dans la loi, mais d'identifier la destination d'une communication émise depuis une telle zone ou un tel lieu.

A.45. Dans son mémoire en réplique, le Conseil des ministre ajoute, en ce qui concerne les critiques des parties requérantes relatives à l'obligation de conservation des métadonnées, ciblée sur une différenciation géographique et sur l'application de cette différenciation, que le critère basé sur le nombre de faits de criminalité grave est incontestablement objectif. Le Conseil des ministres relève que la partie requérante dans l'affaire n° 7930 ne démontre pas en quoi le seuil de criminalité retenu est disproportionné. En ce qui concerne les variables établies par la loi du 20 juillet 2022, le Conseil des ministres soutient qu'elles constituent des données récoltées de manière régulière et agrégées sur une période de trois ans afin de corriger les anomalies éventuelles liées à un évènement ponctuel. Du reste, il est impossible de déterminer à l'avance le lieu où le risque que des infractions soient commises est le plus élevé. Par ailleurs, les zones visées à l'article 11 de la loi du 20 juillet 2022 font l'objet d'une évaluation statistique annuelle. En outre, l'entrée en vigueur différée de cette disposition s'explique par des raisons techniques, dès lors que certaines zones visées correspondent à un découpage préexistant, tandis que la mise en œuvre d'autres zones est plus complexe techniquement, tant pour l'autorité que pour les opérateurs.

Le gel rapide de données

A.46. En ce qui concerne les critiques des parties requérantes à propos de la technique du « *quick-freeze* », qui est une mesure de conservation rapide des données, le Conseil des ministres observe que l'article 25 de la loi

du 20 juillet 2022 vise à compléter l'article 88*bis* du Code d'instruction criminelle, qui réglemente l'accès des autorités judiciaires, à des fins pénales, à des données de trafic et de localisation déjà conservées par les opérateurs. Il s'agit donc d'un dispositif complémentaire portant sur le gel de données pour le futur, dans le cadre d'une enquête judiciaire. L'article 25 de la loi du 20 juillet 2022 porte donc sur les mêmes catégories de données que celles visées à l'article 88*bis* du Code d'instruction criminelle. La mesure doit par ailleurs se limiter aux seules données susceptibles de contribuer à identifier l'auteur de l'infraction, de sorte que la portée du gel de données est clairement et spécifiquement limitée dans la décision du procureur du Roi.

L'article 25 de la loi du 20 juillet 2022 ne peut être mobilisé que lorsqu'il existe des indices sérieux que les infractions peuvent donner lieu à un emprisonnement correctionnel principal d'un an ou à une peine plus lourde, afin de garantir que la mesure ne s'applique que dans le cadre de la recherche et de la poursuite des infractions d'une certaine gravité, ce qui est conforme aux enseignements de la jurisprudence de la Cour de justice. Le Conseil des ministres relève encore que la mesure de gel des données est entourée de garanties procédurales strictes pour éviter les risques d'abus et d'accès illicite. Il observe que le gel est ponctuel, limité dans le temps et axé sur la cible d'une information ou d'une instruction. Les principes essentiels en matière d'information et d'instruction s'appliquent d'office, la durée de la mesure de gel est limitée à deux mois et la période de conservation des données par les opérateurs est de six mois. Les durées précitées sont renouvelables aux mêmes conditions, de sorte qu'il n'existe pas de prolongation automatique. Comme les travaux préparatoires l'indiquent, ces garanties sont par ailleurs conformes aux enseignements de la jurisprudence de la Cour et de la Cour de justice.

L'accès aux données

A.47.1. En ce qui concerne les critiques des parties requérantes à propos de l'accès aux données, le Conseil des ministres relève tout d'abord que l'article 13 de la loi du 20 juillet 2022, qui permet aux autorités compétentes en matière financière d'accéder aux données de trafic et de localisation, est conforme aux enseignements de la Cour de justice, qui attribuent aux États membres le soin de déterminer si une infraction relève de la criminalité grave. Dans ce cadre, l'article 13 inclut dans cette notion les infractions relatives aux abus de marché, étant entendu que les travaux préparatoires justifient de manière détaillée cette classification, qui est par ailleurs autorisée par le droit dérivé de l'Union européenne. Contrairement à ce qu'indiquent les parties requérantes, le Roi ne peut pas étendre ou compléter la liste des autorités compétentes, qui sont visées à l'article 13 de la loi du 20 juillet 2022. Il Lui appartient seulement de mettre en œuvre opérationnellement les principes qui se trouvent dans celle-ci. Par ailleurs, le pouvoir d'exécution du Roi visé à l'article 9 de la loi est facultatif, comme le confirment les travaux préparatoires, et est strictement balisé. Enfin, l'article 13 de la loi ne contient pas de délégation en matière d'autorités compétentes, dès lors qu'il ne porte pas sur cette question et vise une norme législative formelle de droit belge.

Le Conseil des ministres soutient par ailleurs que la liste des finalités énumérées à l'article 13 de la loi du 20 juillet 2022 est conforme à l'article 15, paragraphe 1, de la directive 2002/58/CE, tel qu'il est interprété par la Cour de justice. En effet, les États membres peuvent prévoir les motifs d'exception au sens de l'article 15, paragraphe 1, de cette directive lorsqu'ils concernent la prévention, la recherche, la détection et la poursuite d'utilisations non autorisées du système de communications électroniques, à savoir les utilisations qui remettent en cause l'intégrité ou la sécurité même du système, d'une part, et lorsqu'ils sont prévus à l'article 23, paragraphe 1, du RGPD, d'autre part. Le Conseil des ministres précise que l'article 13 de la loi du 20 juillet 2022 opère une distinction entre les données visées aux articles 126 et 127 de la loi du 13 juin 2005, auxquelles les autorités peuvent accéder pour les finalités visées à l'article 13 de la loi du 20 juillet 2022, et les adresses IP attribuées à la source d'une connexion, qui font l'objet d'un régime spécifique. Les finalités relatives à la première catégorie de données sont parfaitement conformes au droit de l'Union européenne, dès lors qu'elles proviennent de la jurisprudence de la Cour de justice et de l'article 23 du RGPD. Elles sont aussi justifiées dans les travaux préparatoires de la loi du 20 juillet 2022. Un raisonnement similaire s'impose en ce qui concerne les adresses IP, dès lors que l'encadrement de cette seconde catégorie de données reproduit strictement le cadre fixé par la jurisprudence européenne. Enfin, l'accès aux données conservées sur une base géographique, prévu à l'article 11 de la loi du 20 juillet 2022, n'est autorisé que dans le cadre de finalités qui s'avèrent une nouvelle fois conformes à la jurisprudence de la Cour de justice ou qui sont à tout le moins proportionnées à l'objectif poursuivi.

A.47.2. À propos des conditions d'accès aux données en particulier, le Conseil des ministres observe que l'article 13 de la loi du 20 juillet 2022 ne dispense pas les autorités visées de motiver la demande d'accès aux données au regard d'une des finalités prévues. En outre, la critique des parties requérantes selon laquelle les articles 26 et 27 de cette loi ne prévoiraient pas de contrôle préalable de l'accès aux données conservées à des fins pénales n'est pas fondée. En effet, l'article 46*bis*, § 1er, du Code d'instruction criminelle, modifié par l'article 26 de la loi du 20 juillet 2022, ne porte pas sur l'accès aux données de trafic et de localisation, de sorte que l'exigence d'un contrôle préalable, imposée par la Cour de justice, ne s'applique pas en l'espèce. En outre, l'article 46*bis* du Code d'instruction criminelle contient des garanties appropriées entourant l'accès aux données qu'il vise. Par ailleurs, l'article 27 de la loi du 20 juillet 2022 modifie l'article 88*bis* du Code d'instruction criminelle afin que soit prévue une intervention systématique du juge d'instruction, ce qui est conforme à la jurisprudence de la Cour de justice.

Enfin, la possibilité donnée au Roi d'imposer la collaboration des centres fermés ou des lieux d'hébergement au sens de la loi du 15 décembre 1980, prévue à l'article 26 de la loi du 20 juillet 2022, est justifiée avec précision dans les travaux préparatoires de la loi du 20 juillet 2022, qui énoncent les objectifs démontrant la nécessité d'une telle collaboration. Par ailleurs, l'article 26 de la loi du 20 juillet 2022 ne vise qu'une hypothèse d'identification indirecte, sur la base des coordonnées du centre ou du lieu d'hébergement visé dans les informations reçues de manière directe de la part de l'opérateur. Sans cette mesure, le procureur du Roi ne serait pas en mesure d'identifier un abonné qui réside dans un centre fermé ou dans un lieu d'hébergement au sens de la loi du 15 décembre 1980.

A.47.3. Dans son mémoire en réplique, le Conseil des ministres apporte plusieurs précisions complémentaires au sujet des critiques des parties requérantes relatives à l'accès aux données. Il relève tout d'abord que les critiques de la partie requérante dans l'affaire n° 7930 relatives à l'assimilation de l'abus de marché à une infraction relevant de la criminalité grave résultent d'une opinion politique différente de celle qui a été retenue par le législateur, ce qui ne suffit pas à justifier un moyen d'annulation. Ensuite, le Conseil des ministres précise que la circulaire visée à l'article 13 de la loi du 20 juillet 2022 n'ajoute rien au texte légal. Il s'agit d'une circulaire interprétative destinée à déterminer les autorités qui peuvent avoir accès aux données qui sont conservées, dès lors que l'article 13 doit se lire de concert avec d'autres dispositions législatives formelles, ce qui en altère la lisibilité. En revanche, la circulaire ne peut donner aucune habilitation à une autorité qui n'est pas visée par la loi.

En outre, le Conseil des ministres affirme que, dès lors que certaines infractions sont poursuivies par des autorités administratives et non juridictionnelles, il convient que ces autorités puissent avoir accès aux données et aux métadonnées nécessaires à l'exercice de leur mission, ce qui n'est nullement interdit par le droit dérivé de l'Union européenne. Ensuite, la loi du 20 juillet 2022 n'étend pas en substance les possibilités d'accès aux données visées, dès lors que plusieurs autorités désignées par cette loi disposaient déjà d'une faculté d'accéder à ces informations en vertu de la législation antérieure. Si certaines autorités reçoivent effectivement ce pouvoir en vertu de la loi du 20 juillet 2022, c'est en raison du fait qu'un nombre croissant d'infractions se produit en ligne ou à l'aide de services de communications électroniques. Enfin, contrairement à ce qu'indique la partie requérante dans l'affaire n° 7930, la notion de sauvegarde des intérêts vitaux au sens de l'article 13 de la loi du 20 juillet 2022 trouve bien un appui dans le RGPD, en particulier dans son considérant 73.

Les voies de recours

A.48. En ce qui concerne les critiques des parties requérantes à propos des voies de recours quant à l'accès aux données conservées, qui seraient insuffisantes en raison de l'absence d'information des personnes concernées en la matière, le Conseil des ministres soutient tout d'abord que l'article 37 de la loi du 30 juillet 2018 prévoit de manière générale un droit à l'information. Certaines exceptions sont toutefois établies afin d'assurer l'effectivité des enquêtes pénales, la protection de la sécurité publique, la protection de la sécurité nationale et la protection des droits fondamentaux d'autrui. Par ailleurs, pour certaines autorités particulières, la loi du 20 juillet 2022 prévoit des exigences spécifiques et adaptées en matière d'information, étant entendu que les autres types d'accès bénéficient de la protection générale de l'article 37 de la loi du 30 juillet 2018. Partant, un large éventail de recours effectifs est accessible aux personnes concernées par la conservation des données prévue par la loi du 20 juillet 2022 et par l'accès à ces données conservées. Pour le surplus, le Conseil des ministres soutient que les critiques des parties requérantes en la matière sont particulièrement sommaires.

Les données cryptées et le blocage de numéros ou de services

A.49. En ce qui concerne les critiques des parties requérantes à propos des données cryptées et du blocage de numéros ou de services, le Conseil des ministres relève que l'article 3 de la loi du 20 juillet 2022 réaffirme la liberté du chiffrement tout en prévoyant trois restrictions strictement limitées et répondant à des objectifs clairement justifiés. La première restriction vise à assurer l'efficacité des communications d'urgence vers les services d'urgence. La deuxième restriction vise à assurer l'efficacité de la loi du 20 juillet 2022 en soi afin d'éviter qu'un opérateur utilise des systèmes de chiffrement en vue d'échapper à l'application des obligations en matière de conservation des données. La troisième restriction concerne uniquement le cas spécifique des cartes SIM étrangères actives sur le territoire belge afin de garantir que la conclusion des contrats d'itinérance avec des opérateurs étrangers soit conforme aux exigences de la législation belge, de manière à permettre aux opérateurs belges de se conformer aux mêmes dispositions légales que pour leurs propres utilisateurs. Partant, l'article 3 de la loi du 20 juillet 2022 est justifié et proportionné à l'objectif poursuivi.

Au sujet du blocage de numéros autorisé à l'article 4 de la loi du 20 juillet 2022, le Conseil des ministres affirme que cette disposition vise à remédier à l'insuffisance du cadre juridique, de manière à lutter de manière plus efficace face à la nature des fraudes et des autres utilisations malveillantes, tant dans l'intérêt des utilisateurs que des services de communications électroniques. L'article 4 laisse aux opérateurs le soin de déterminer les mesures appropriées à prendre, telles que des mesures anti-spam ou un blocage de numéro, dès lors qu'ils sont les mieux placés pour évaluer l'opportunité de celles-ci. Par ailleurs, en matière de fraude et d'utilisation malveillante, il est essentiel d'agir très rapidement. En outre, l'article 4 fournit des exemples de mesures visant à garantir une plus grande sécurité juridique, et des limitations sont prévues. Dans ce cadre, il est interdit aux opérateurs de prendre connaissance du contenu des communications, il est prévu que l'IBPT peut vérifier l'existence d'une fraude ou d'une utilisation malveillante d'un réseau pour imposer des instructions aux opérateurs dans le but de protéger les intérêts des utilisateurs, et il appartient au Roi, le cas échéant, de préciser les mesures à prendre.

Les éléments de preuve recueillis illégalement

A.50. En ce qui concerne les critiques des parties requérantes à propos du sort des éléments de preuve recueillis illégalement, le Conseil des ministres soutient qu'il n'appartient pas à la Cour de se prononcer sur cet élément, dès lors qu'une telle demande excède le cadre du contrôle objectif de constitutionnalité de la loi du 20 juillet 2022. En réalité, le sort des preuves pénales recueillies illégalement est réglé dans le Code d'instruction criminelle et dans le titre préliminaire du Code de procédure pénale. Il appartient le cas échéant au juge de fond d'appliquer les dispositions pertinentes, dans chaque affaire concrète, compte tenu des circonstances de l'espèce et de la jurisprudence européenne applicable.

La protection du secret professionnel

A.51. En ce qui concerne les critiques des parties requérantes à propos de la protection du secret professionnel, le Conseil des ministres renvoie tout d'abord à ses écrits de procédures dans l'affaire n° 7907. Pour le surplus, il précise qu'il ressort de l'arrêt de la Cour n° 26/96 du 27 mars 1996 (ECLI:BE:GHCC:1996:ARR.026) que la différence de traitement entre les médecins et les avocats, d'une part, et les professionnels comptables et fiscaux, d'autre part, n'est pas discriminatoire. En effet, la protection procédurale mise en place par la loi du 20 juillet 2022 ne vaut que pour les médecins et pour les avocats parce qu'ils sont dépositaires du secret professionnel en vertu de l'article 458 du Code pénal, qu'ils entretiennent avec leurs clients et leurs patients une relation de confiance et qu'ils relèvent d'instances organisées par la loi veillant au respect de la déontologie professionnelle.

Les demandes faites par la partie requérante de poser des questions préjudicielles à la Cour de justice de l'Union européenne

A.52.1. En ce qui concerne les demandes faites par la partie requérante dans l'affaire n° 7931 de poser des questions préjudicielles à la Cour de justice formulées, le Conseil des ministres précise qu'il n'est pas opposé par principe à ces demandes, pourvu que les questions soient reformulées. En effet, la formulation proposée par cette

partie requérante est trop orientée, en ce qu'elle suggère que les dispositions attaquées ne sont pas conformes au droit de l'Union européenne.

A.52.2. Au sujet de la question préjudicielle portant sur la conservation des données de communication, le Conseil des ministres considère que les enseignements de l'arrêt de la Cour de justice du 6 octobre 2020 en cause de *La Quadrature du Net e.a.* (C-511/18, C-512/18 et C-520/18, ECLI:EU:C:2020:791) sont transposables en l'espèce. En cas de doute sur ce point, la Cour de justice pourrait être interrogée afin de déterminer si l'article 15, paragraphe 1, de la directive 2002/58/CE, lu en combinaison avec les articles 7, 8, 11 et 52, paragraphe 1, de la Charte, autorise une mesure législative imposant aux fournisseurs de services de communications électroniques de conserver les données techniques qui permettent d'identifier les auteurs d'infractions en ligne ou hors ligne.

A.52.3. Au sujet de la question préjudicielle portant sur la conservation et le traitement de certaines données de trafic et de localisation en vue de détecter et d'analyser une fraude présumée ou une utilisation malveillante présumée d'un réseau de communications électroniques, le Conseil des ministres soutient que ces mesures entrent dans les limites permises par la directive 2002/58/CE. En cas de doute sur ce point, la Cour de justice pourrait être interrogée afin de déterminer si l'article 15, paragraphe 1, de la directive 2002/58/CE, lu en combinaison avec les articles 7, 8 et 52, paragraphe 1, de la Charte, autorise une mesure législative ayant pour objet la conservation et le traitement de certaines données de trafic et de localisation nécessaires pour protéger les intérêts de l'opérateur et de l'utilisateur final contre la fraude et l'utilisation malveillante du réseau.

A.52.4. Au sujet de la question préjudicielle portant sur la conservation des données de trafic et de localisation en vue de lutter contre certaines infractions spécifiques, à savoir le faux informatique, la fraude informatique et le vol avec violence, sans tenir compte du seuil de la peine, le Conseil des ministres affirme que la notion de criminalité grave est une notion dynamique et évolutive, mais aussi qu'il appartient aux États membres de déterminer les infractions qui relèvent de cette catégorie. Il n'appartient pas à la Cour de justice de se prononcer sur le point de savoir si une infraction spécifique peut, en fonction des circonstances, relever de la criminalité grave.

En cas de doute à ce sujet, la Cour de justice pourrait être interrogée afin de déterminer si l'article 15, paragraphe 1, de la directive 2002/58/CE, lu en combinaison avec les articles 7, 8 et 52, paragraphe 1, de la Charte, autorise une mesure législative à se référer aux dispositions de droit national pour déterminer les infractions qui relèvent de la criminalité grave.

A.52.5. Au sujet des questions préjudicielles ayant pour objet les facultés offertes au juge d'instruction, au procureur du Roi et aux officiers de police judiciaire, le Conseil des ministres rappelle que les articles 26 et 27 de la loi du 20 juillet 2022 sont conformes à la directive 2002/58/CE. En cas de doute à ce sujet, la Cour de justice pourrait être saisie afin de déterminer, tout d'abord, si l'article 15, paragraphe 1, de la directive 2002/58/CE, lu en combinaison avec les articles 7, 8 et 52, paragraphe 1, de la Charte, autorise une mesure législative habilitant le Procureur du Roi à faire identifier l'abonné ou l'utilisateur habituel d'un service ou d'un moyen de communications électroniques, ainsi qu'à faire identifier les services de communications électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée. Ensuite, une autre question préjudicielle pourrait être posée afin de déterminer si l'article 15, paragraphe 1, de la directive 2002/58/CE, lu en combinaison avec les articles 7, 8 et 52, paragraphe 1, de la Charte, autorise une mesure législative habilitant le juge d'instruction ou, en cas de flagrant délit, le procureur du Roi à accéder aux données de trafic et de localisation à des fins de lutte contre la criminalité grave.

A.52.6. Au sujet de la question préjudicielle relative à l'information de la personne concernée, le Conseil des ministres soutient que cette question est inutile à la solution du litige. Il n'est toutefois pas opposé à ce que la question soit posée. En revanche, en ce qui concerne la dernière question préjudicielle, relative aux éléments de preuves recueillis en application de la loi du 20 juillet 2022 dans l'hypothèse où celle-ci devrait être annulée, le Conseil des ministres rappelle qu'il appartient au juge pénal concerné de se prononcer sur la question du sort de ces preuves, de sorte que la question est inutile.

- B –

Quant à la loi attaquée et à son contexte

B.1. Les recours en annulation portent sur la loi du 20 juillet 2022 « relative à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités » (ci-après : la loi du 20 juillet 2022).

Celle-ci apporte des modifications à la loi du 13 juin 2005 « relative aux communications électroniques » (ci-après : la loi du 13 juin 2005) (articles 2 à 17 de la loi du 20 juillet 2022), à la loi du 1er juillet 2011 « relative à la sécurité et la protection des infrastructures critiques » (ci-après : la loi du 1er juillet 2011) (article 18 de la loi du 20 juillet 2022), à la loi du 17 janvier 2003 « relative au statut du régulateur des secteurs des postes et des télécommunications belges » (ci-après : la loi du 17 janvier 2003) (articles 19 à 24 de la loi du 20 juillet 2022), au Code d'instruction criminelle (articles 25 à 27 de la loi du 20 juillet 2022), à la loi du 5 août 1992 « sur la fonction de police » (ci-après : la loi du 5 août 1992) (article 28 de la loi du 20 juillet 2022), à la loi du 30 novembre 1998 « organique des services de renseignement et de sécurité » (ci-après : la loi du 30 novembre 1998) (articles 29 à 39 de la loi du 20 juillet 2022), à la loi du 2 août 2002 « relative à la surveillance du secteur financier et aux services financiers » (ci-après : la loi du 2 août 2002) (articles 40 et 41 de la loi du 20 juillet 2022), à la loi du 7 avril 2019 « établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique » (ci-après : la loi du 7 avril 2019) (articles 42 et 43 de la loi du 20 juillet 2022) et à la loi du 24 janvier 1977 « relative à la protection de la santé des consommateurs en ce qui concerne les denrées alimentaires et les autres produits » (article 44 de la loi du 20 juillet 2022). La loi du 20 juillet 2022 comporte également plusieurs dispositions « transitoires » (articles 45 à 48 de la loi du 20 juillet 2022).

B.2.1. Par la loi du 20 juillet 2022, le législateur a entendu répondre à l'annulation, par l'arrêt de la Cour n° 57/2021 du 22 avril 2021 (ECLI:BE:GHCC:2021:ARR.057), de la loi du 29 mai 2016 « relatif à la collecte et à la conservation des données dans le secteur des communications électroniques » (ci-après : la loi du 29 mai 2016) (*Doc. parl.*, Chambre, 2021-2022, DOC 55-2572/001, p. 4). La Cour a rendu cet arrêt après avoir posé plusieurs

questions préjudicielles à la Cour de justice de l'Union européenne (ci-après : la Cour de justice) (voy. arrêt n° 96/2018 du 19 juillet 2018, ECLI:BE:GHCC:2018:ARR.096), laquelle y a répondu par l'arrêt du 6 octobre 2020 en cause de *La Quadrature du Net e.a.,* rendu en grande chambre (C-511/18, C-512/18 et C-520/18, ECLI:EU:C:2020:791).

B.2.2. Les travaux préparatoires de la loi du 20 juillet 2022 précisent à cet égard :

« À la suite de l'arrêt *La Quadrature du Net* rendu par la Cour de Justice [(CJUE)] le 6 octobre 2020 (affaires jointes C-511/18, C-512/18 et C-520/18), la Cour constitutionnelle belge a, par arrêt du 22 avril 2021, annulé les articles 2, *b)*, 3 à 11 et 14 de la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques. Cette loi est connue sous le nom de ' loi *data retention* '. Le présent projet vise essentiellement à réparer cette loi et à rétablir un cadre juridique conforme à la jurisprudence en matière de conservation des ' données de trafic et de localisation ' au sens 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 ', aussi appelée ' directive *e-privacy* '). Cette directive sera remplacée par un règlement, qui utilise une nouvelle terminologie, à savoir ' métadonnées ' au lieu de ' données de trafic et de localisation '.

Cette loi prévoyait l'obligation pour les fournisseurs au public de services de téléphonie, en ce compris par internet, d'accès à l'internet et de courrier électronique par internet (qu'ils soient opérateurs notifiés à l'IBPT ou non) de conserver certaines données de localisation et de trafic, précisées par arrêté royal, pendant une durée de 12 mois, afin que ces données soient disponibles pour des finalités répressives (enquêtes pénales) ou pour l'accomplissement des missions des services de renseignement.

La vice-première ministre fait remarquer que ces données ne concernent pas le contenu des communications. C'est pour cela qu'on parle de ' métadonnées ' (par exemple ' qui appelle qui '). Il ne s'agit donc pas du contenu des appels téléphoniques.

La loi du 29 mai 2016 prévoyait une obligation de conservation généralisée et indifférenciée de certaines métadonnées.

Or, par son arrêt *La Quadrature du Net*, la CJUE a jugé que la conservation généralisée et indifférenciée telle que prévue par la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques violait certains principes de droit européen et notamment le droit à la vie privée. Sur la base de la directive e-privacy et de la Charte, l'arrêt de la CJUE a suggéré certaines pistes alternatives à la conservation généralisée et indifférenciée en tout temps :

1) la conservation généralisée et indifférenciée de métadonnées en cas de menace, réelle et actuelle ou prévisible pour la sécurité nationale;

2) la conservation généralisée et indifférenciée des données d'identité civile pour la recherche des infractions ne relevant pas de la criminalité grave;

3) la conservation généralisée et indifférenciée des adresses IP à la source d'une connexion à des fins de lutte contre la criminalité grave, la prévention des menaces graves contre la sécurité publique et la sauvegarde de la sécurité nationale;

4) à des fins de lutte contre la criminalité grave et de sauvegarde de la sécurité publique, la conservation ciblée de métadonnées sur une base géographique ou sur la base des personnes dans certaines zones ou pour certaines catégories de personnes pré-identifiées comme présentant des risques particuliers, et la conservation rapide de métadonnées (' *quick-freeze* '), à savoir une demande de gel de métadonnées relatives à une personne sur une courte période.

Dans son arrêt d'annulation du 22 avril 2021, la Cour constitutionnelle a repris l'argumentaire de la CJUE.

Dans le projet de loi, certaines pistes évoquées par la CJUE ont été suivies et développées, d'autres pas comme la conservation ciblée sur la base des personnes dans certaines zones ou pour certaines catégories de personnes pré-identifiées comme présentant des risques particuliers.

Par ailleurs, la vice-première ministre souligne que des garanties complémentaires ont également été ajoutées au niveau du traitement de ces données par les opérateurs (les mesures de sécurité imposées aux opérateurs sont plus détaillées), ainsi qu'au niveau de la fourniture de ces données aux autorités (encadrement plus strict des conditions entourant cette fourniture et contrôle préalable de la demande de l'autorité envers l'opérateur). Les exigences de la jurisprudence ont ainsi été mises en œuvre.

Enfin, le projet de loi vise également à répondre aux attentes sociétales d'un monde de plus en plus digitalisé : les transactions électroniques (e-commerce) deviennent la norme dans beaucoup de secteurs. Afin de lutter contre certaines formes d'infractions se commettant exclusivement en ligne, il est donc nécessaire que les autorités chargées de la prévention, de la détection et de la poursuite de ces infractions puissent obtenir des opérateurs les données dont ils disposent, dans la mesure nécessaire à l'accomplissement de leurs missions respectives. C'est dans cette optique qu'il est prévu, au chapitre [10] du projet de loi, d'accorder au Service d'inspection des produits de consommation du SPF Santé publique, Sécurité de la Chaîne alimentaire et Environnement, la possibilité d'identifier des personnes morales ou physiques sur la base d'un numéro de téléphone ou d'une adresse IP. Il ne s'agit en d'autres termes que de données qui ne donnent pas d'information précise sur la vie privée des personnes concernées puisqu'elles concernent des données d'identification. Sans la fourniture de ces données, il y aurait une impossibilité matérielle pour ce service de remplir sa mission légale et les enquêtes resteraient immuablement à charge de ' X '.

L'arrêt d'annulation de la Cour constitutionnelle du 22 avril 2021 a également rendu nécessaire une modification de l'arrêté royal 19 septembre 2013 portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques (ci-après

‘ arrêté royal data ’). En outre, l’arrêt d’annulation a également rendu nécessaire la modification de certaines lois organiques, notamment le Code d’instruction criminelle, ou la loi sur la fonction de police. Ce sont ces lois organiques qui fixent les conditions de fourniture des données conservées par les opérateurs aux différentes autorités concernées » (*Doc. parl.*, Chambre, 2021-2022, DOC 55-2572/003, pp. 3-6).

B.2.3. Par l’arrêt n° 57/2021 précité, la Cour a jugé :

« B.18. L’arrêt de la Cour de justice du 6 octobre 2020 impose un changement de perspective par rapport au choix que le législateur a effectué : l’obligation de conservation des données relatives aux communications électroniques doit être l’exception, et non la règle. La réglementation prévoyant une telle obligation doit par ailleurs être soumise à des règles claires et précises concernant la portée et l’application de la mesure en cause et imposant des exigences minimales (point 133). Cette réglementation doit garantir que l’ingérence se limite au strict nécessaire et doit toujours ‘ répondre à des critères objectifs, établissant un rapport entre les données à conserver et l’objectif poursuivi ’ (points 132 et 133).

B.19. Il appartient au législateur d’élaborer une réglementation qui respecte les principes applicables en matière de protection des données à caractère personnel, à la lumière de la jurisprudence de la Cour de justice, et de tenir compte, le cas échéant, des précisions apportées par celle-ci en ce qui concerne les différents types de mesures législatives jugées compatibles avec 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. En particulier, il appartient également au législateur, dans ce contexte, d’opérer les distinctions qui s’imposent entre les différents types de données soumises à conservation, de manière à garantir que, pour chaque type de donnée, l’ingérence soit limitée au strict nécessaire ».

B.2.4. Par cet arrêt, la Cour a jugé qu’il appartient au législateur d’élaborer une nouvelle réglementation quant à l’obligation de conservation des données relatives aux communications électroniques, dans le respect des principes applicables en la matière, à la lumière de la jurisprudence de la Cour de justice relative à 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 (directive vie privée et communications électroniques » (ci-après : la directive 2002/58/CE), lui-même lu à la lumière des articles 7, 8, 11 et 52, paragraphe 1, de la Charte des droits fondamentaux de l’Union européenne (ci-après : la Charte).

B.2.5. L’article 15, paragraphe 1, de la directive 2002/58/CE énonce :

« Les États 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’État - la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d’infractions pénales ou d’utilisations non autorisées du système de communications électroniques, comme le prévoit l’article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États 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.2.6. Dans le dispositif de l’arrêt du 6 octobre 2020 précité, la Cour de justice a dit pour droit :

« 1) 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 (directive vie privée et communications électroniques), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009, 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 des mesures législatives prévoyant, aux fins prévues à cet article 15, paragraphe 1, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation. En revanche, l’article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, 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 des mesures législatives

- permettant, aux fins de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques de procéder à une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, dans des situations où l’État membre concerné fait face à une menace grave pour la sécurité nationale qui s’avère réelle et actuelle ou prévisible, la décision prévoyant cette injonction pouvant faire l’objet d’un contrôle effectif, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d’un effet contraignant, visant à vérifier l’existence d’une de ces situations ainsi que le respect des conditions et des garanties devant être prévues, et ladite injonction ne pouvant être émise que pour une période temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de cette menace;

- prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d’éléments objectifs et non discriminatoires, en fonction de catégories de

personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable;

- prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire;

- prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité et de la sauvegarde de la sécurité publique, une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques, et

- permettant, aux fins de la lutte contre la criminalité grave et, a fortiori, de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques, par le biais d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont disposent ces fournisseurs de services,

dès lors que ces mesures assurent, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus ».

B.3.1. Il ressort par ailleurs des travaux préparatoires de la loi du 20 juillet 2022 que le législateur a également souhaité réagir à l'annulation, par l'arrêt de la Cour n° 158/2021 du 18 novembre 2021 (ECLI:BE:GHCC:2021:ARR.158), de la loi du 1er septembre 2016 « 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 » (ci-après : la loi du 1er septembre 2016) (*Doc. parl.*, Chambre, 2021-2022, DOC 55-2572/003, p. 7).

B.3.2. Les travaux préparatoires de la loi du 20 juillet 2022 mentionnent à ce sujet :

« Le 18 novembre 2021, la Cour constitutionnelle a en effet rendu un arrêt au sujet de la loi du 1er septembre 2016. Cette loi a été adoptée après les attentats de Paris, afin de mettre fin à l'anonymat des utilisateurs de cartes prépayées permettant l'utilisation de services mobiles (appel, accès à Internet, envoi de SMS, etc.) en obligeant les opérateurs à les identifier.

Dans cet arrêt, la Cour ne remet pas en cause le principe de l'identification des utilisateurs de cartes prépayées, mais elle annule la modification apportée par la loi du 1er septembre 2016 à l'article 127 de la loi du 13 juin 2005, ' uniquement en ce qu'(elle) ne détermine pas les données d'identification qui sont collectées et traitées et les documents d'identification qui entrent en considération '. La Cour considère que l'article 22 de la Constitution exige que ces

données et documents soient énumérés dans la loi. Elle maintient les effets de la disposition annulée jusqu'à l'entrée en vigueur d'une norme législative qui énumère ces données d'identification et ces documents d'identification et au plus tard jusqu'au 31 décembre 2022 inclus.

L'arrêt du 18 novembre 2021 de la Cour constitutionnelle porte uniquement sur l'article 127 de la loi du 13 juin 2005. Lorsqu'on analyse cette décision, on constate toutefois que ses enseignements - à savoir le fait que les données à conserver par les opérateurs doivent être mentionnées dans la loi – s'appliquent également aux articles 126 et 126/1 de cette loi tels qu'ils figurent dans le projet de loi relatif à la ' conservation des données '. Il s'ensuit que ces articles 126 et 126/1 doivent également être modifiés » (*ibid.*, p. 7).

B.4. Il ressort des travaux préparatoires de la loi du 20 juillet 2022 que le législateur a examiné en profondeur tant l'arrêt n° 57/2021 précité que l'arrêt de la Cour de justice du 6 octobre 2020, sur lequel il est basé, mais aussi l'arrêt n° 158/2021 précité.

Quant à l'étendue des recours en annulation

B.5.1. La Cour doit déterminer l'étendue des recours en annulation sur la base du contenu des requêtes.

La Cour peut uniquement annuler des dispositions législatives explicitement attaquées contre lesquelles des moyens sont invoqués et, le cas échéant, des dispositions qui ne sont pas attaquées mais qui sont indissociablement liées aux dispositions qui doivent être annulées.

B.5.2.1. La partie requérante dans l'affaire n° 7907 demande l'annulation des articles 5, 4° et 6°, 8 à 11, 13 à 15, 19, 21, 22, 24 à 42 et 44 de la loi du 20 juillet 2022.

B.5.2.2. Les parties requérantes dans l'affaire n° 7929 demandent l'annulation des articles 2 à 17 de la loi du 20 juillet 2022.

B.5.2.3. Les parties requérantes dans les affaires n^{os} 7930, 7931 et 7932 demandent l'annulation de la loi du 20 juillet 2022 dans son intégralité.

La partie requérante dans l'affaire n° 7930 ne développe cependant des moyens que contre les articles 5, 6, 8, 9, 11, 12, 13, 27 et 45 de la loi du 20 juillet 2022. Elle dénonce par ailleurs l'existence d'une lacune législative en ce qui concerne les données couvertes par le secret professionnel.

Du reste, le moyen unique de la partie requérante dans l'affaire n° 7931 n'est dirigé que contre les articles 3, 5, 8, 9, 10, 11, 13, 24, 25, 26 et 27 de la loi du 20 juillet 2022.

En outre, les parties requérantes dans l'affaire n° 7932 ne développent des moyens que contre les articles 3, 4, 5, 6, 8, 9, 10, 11, 12, 13, 15, 33, 34 et 37 de la loi du 20 juillet 2022. Elles dénoncent également l'existence d'une lacune législative en ce qui concerne les données couvertes par le secret professionnel.

B.6. L'examen de la Cour porte donc sur les articles 3 à 6, 8 à 15, 19, 21, 22, 24 à 42 et 45 de la loi du 20 juillet 2022, ainsi que sur la lacune législative précitée.

Quant à l'intérêt

B.7.1. Le Conseil des ministres conteste l'intérêt à agir de l'Ordre des barreaux francophones et germanophone, qui est la partie requérante dans l'affaire n° 7907.

L'intérêt de l'Ordre des barreaux francophones et germanophone serait limité à l'article 27, 2°, de la loi du 20 juillet 2022, dès lors que les griefs dirigés contre les autres dispositions ne porteraient pas sur le secret professionnel de l'avocat.

B.7.2. La Constitution et la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle imposent à toute personne physique ou morale qui introduit un recours en annulation de justifier d'un intérêt. Ne justifient de l'intérêt requis que les personnes dont la situation pourrait être affectée directement et défavorablement par la norme attaquée; il s'ensuit que l'action populaire n'est pas admissible.

B.7.3. L’article 495 du Code judiciaire, alinéas 1er et 2, dispose :

« L’Ordre des Barreaux francophones et germanophone et l’Orde van Vlaamse balies ont, [chacun] en ce qui concerne les barreaux qui en font partie, pour mission de veiller à l’honneur, aux droits et aux intérêts professionnels communs de leurs membres et sont [compétents] en ce qui concerne l’aide juridique, le stage, la formation professionnelle des avocats-stagiaires et la formation de tous les avocats appartenant aux barreaux qui en font partie.

[Ils] prennent les initiatives et les mesures utiles en matière de formation, de règles disciplinaires et de loyauté professionnelle, ainsi que pour la défense des intérêts de l’avocat et du justiciable ».

B.7.4. Les Ordres des barreaux sont des groupements professionnels de droit public qui ont été institués par la loi et qui regroupent obligatoirement tous ceux qui exercent la profession d’avocat.

Sauf dans les cas où ils défendent leur intérêt personnel, les Ordres des barreaux ne peuvent agir en justice que dans le cadre de la mission que le législateur leur a confiée. Ainsi donc, ils peuvent en premier lieu agir en justice lorsqu’ils défendent les intérêts professionnels de leurs membres ou lorsque l’exercice de la profession d’avocat est en cause. Selon l’article 495, alinéa 2, du Code judiciaire, les Ordres peuvent également prendre des initiatives et des mesures « utiles [...] pour la défense des intérêts de l’avocat et du justiciable ».

B.7.5. Il ressort de l’article 495 du Code judiciaire, lu en combinaison avec les articles 2 et 87 de la loi spéciale du 6 janvier 1989 précitée, que les Ordres des barreaux ne peuvent agir devant la Cour comme partie requérante ou partie intervenante pour défendre l’intérêt collectif des justiciables qu’en ce qu’une telle action est liée à la mission et au rôle de l’avocat en ce qui concerne la défense des intérêts du justiciable.

Des mesures qui n’ont aucune incidence sur le droit d’accès au juge, sur l’administration de la justice ou sur l’assistance que les avocats peuvent offrir à leurs clients, que ce soit lors d’un recours administratif, lors d’une conciliation amiable ou lors d’un litige soumis aux juridictions judiciaires ou administratives, ne relèvent dès lors pas de l’article 495 du Code judiciaire, lu en combinaison avec les articles 2 et 87 de la loi spéciale du 6 janvier 1989 précitée.

B.7.6. Les dispositions attaquées visent à établir un cadre juridique en matière de conservation et d'accès aux données à caractère personnel dans le secteur des communications électroniques, à la suite de l'annulation de la loi du 1er septembre 2016 par l'arrêt de la Cour n° 57/2021 précité .

Le constat que les dispositions attaquées par l'Ordre des barreaux francophones et germanophone, à l'exception de l'article 27, 2°, de la loi du 20 juillet 2022, ne visent pas expressément les moyens de communications électroniques des avocats ne permet pas de déduire que celles-ci ne leur sont pas applicables.

La loi du 20 juillet 2022 revêt une portée générale et s'applique à l'ensemble des moyens de communications électroniques, dont ceux qui bénéficient de la protection de l'article 458 du Code pénal.

Les informations confidentielles confiées à un avocat dans l'exercice de sa profession bénéficient de la protection découlant, pour le justiciable, des garanties inscrites à l'article 6 de la Convention européenne des droits de l'homme, dès lors que la règle du secret professionnel imposée à l'avocat est un élément fondamental des droits de la défense du justiciable qui se confie à lui (voy. not. l'arrêt n° 174/2018 du 6 décembre 2018, ECLI:BE:GHCC:2018:ARR.174, B.25).

B.7.7. Il découle de ce qui précède que la loi du 20 juillet 2022 prévoit des mesures qui peuvent avoir une incidence sur l'exercice de la profession d'avocat.

B.7.8. L'exception d'irrecevabilité est rejetée.

Quant au fond

B.8.1. L'article 6 de la loi spéciale du 6 janvier 1989 précitée précise que la requête « indique l'objet du recours et contient un exposé des faits et moyens ».

B.8.2. Pour satisfaire aux exigences de l'article 6 de la loi spéciale du 6 janvier 1989 précitée, les moyens et branches de moyens doivent faire connaître, parmi les règles dont la Cour garantit le respect, celles qui seraient violées ainsi que les dispositions qui violeraient ces règles et exposer en quoi ces règles auraient été transgressées par ces dispositions.

Cette exigence n'est pas de pure forme. Elle vise à fournir à la Cour ainsi qu'aux institutions et aux personnes qui peuvent adresser un mémoire à la Cour un exposé clair et univoque des moyens.

B.8.3. Les moyens dans les affaires jointes comprennent un grand nombre de griefs, souvent répétitifs et redondants. Ces moyens portent principalement sur la compatibilité des dispositions attaquées avec le droit au respect de la vie privée et avec le droit à la protection des données à caractère personnel, garantis par l'article 22 de la Constitution, par l'article 8 de la Convention européenne des droits de l'homme, par les articles 7 et 8 de la Charte et par plusieurs dispositions du droit de l'Union européenne. D'autres normes de référence sont également invoquées, sans toutefois que leur violation soit systématiquement étayée. La Cour limite son examen aux normes de référence faisant l'objet de développements de la part des parties, conformément aux exigences mentionnées en B.8.2.

B.8.4. Pour autant que les moyens dans les affaires jointes satisfassent aux exigences qui précèdent, la Cour examine les griefs des parties requérantes dans l'ordre suivant :

1. L'utilisation de la cryptographie (article 3);

2. Les mesures employées au niveau du réseau ou de l'utilisateur final pour détecter la fraude et les utilisations malveillantes des réseaux et des services (article 4);

3. La conservation des données de trafic (article 5);

4. La conservation des données de localisation (article 6);

5. La conservation des données de souscription et d'identification (article 8)*;*

6. L'obligation d'identification des abonnés et des utilisateurs finaux de services de communication électronique (article 12);

7. La conservation ciblée des données sur la base d'un critère géographique (articles 9 à 11);

8. L'énumération des autorités compétentes et des finalités dans le cadre de l'accès aux données (article 13);

9. Les compétences des officiers de police judiciaire de l'IBPT (article 24);

10. Les compétences du procureur du Roi (articles 25 et 26);

11. Les compétences du juge d'instruction (article 27);

12. Les compétences des services de renseignement et de sécurité (articles 33, 34 et 37);

13. L'entrée en vigueur (article 45);

14. La protection du secret professionnel.

1. L'utilisation de la cryptographie (article 3)

B.9. Le moyen unique dans l'affaire n° 7931 et le cinquième moyen dans l'affaire n° 7932 portent sur l'article 3 de la loi du 20 juillet 2022, qui remplace l'article 107/5 de la loi du 13 juin 2005 comme suit :

« § 1er. Afin de favoriser la sécurité numérique, l'utilisation de la cryptographie est libre dans les limites prévues aux paragraphes 2 à 4.

§ 2. Le recours à la cryptographie ne peut pas empêcher les communications d'urgence, en ce compris l'identification de la ligne appelante ou la fourniture des données d'identification de l'appelant.

§ 3. Le recours à la cryptographie, utilisée par un opérateur, visant à garantir la sécurité des communications, ne peut pas empêcher l'exécution d'une demande ciblée d'une autorité compétente, dans les conditions prévues par la loi, dans le but d'identifier l'utilisateur final, de repérer et localiser des communications non accessibles au public.

§ 4. L'utilisation de la cryptographie par un opérateur étranger, dont l'utilisateur final ou l'abonné est situé sur le territoire belge, ne peut pas empêcher l'exécution d'une demande d'une autorité compétente telle que visée aux paragraphes 2 et 3.

Toute clause contractuelle prise par les opérateurs faisant obstacle à l'exécution de l'alinéa 1er est interdite et nulle de plein droit ».

B.10.1. Dans son moyen unique, pris de la violation des articles 11, 12, 22 et 29 de la Constitution, lus en combinaison ou non avec les articles 7, 8, 11, 47 et 52, paragraphe 1, de la Charte, avec l'article 8 de la Convention européenne des droits de l'homme, avec les articles 5, 6 et 15 de la directive 2002/58/CE et avec les articles 13 et 54 de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 « relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil » (ci-après : la directive (UE) 2016/680), la partie requérante dans l'affaire n° 7931 soutient que l'article 107/5, §§ 3 et 4, de la loi du 13 juin 2005, tel qu'il a été inséré par l'article 3 de la loi du 20 juillet 2022, est disproportionné, dès lors que les mesures de cryptage permettent précisément de garantir la protection des données à caractère personnel et de protéger le droit au respect de la vie privée.

B.10.2. Dans leur cinquième moyen, pris de la violation des articles 10, 11, 15, 22 et 29 de la Constitution, lus en combinaison ou non 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, avec l'article 5, paragraphe 4, du Traité sur l'Union européenne et avec la directive 2002/58/CE, la directive (UE) 2016/680 et le 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) » (ci-après : le RGPD), les parties requérantes dans l'affaire n° 7932 soutiennent que l'article 107/5, § 3, de la loi du 13 juin 2005, tel qu'il a été inséré par l'article 3 de la loi du 20 juillet 2022

constitue une ingérence disproportionnée dans le droit au respect de la vie privée et prévoit une mesure qui n'est pas nécessaire dans une société démocratique.

B.11.1. Il ressort de ce qui précède que la partie requérante dans l'affaire n° 7931 et les parties requérantes dans l'affaire n° 7932 ne formulent des griefs à l'encontre de l'article 107/5 de la loi du 13 juin 2005, tel qu'il a été remplacé par l'article 3 de la loi du 20 juillet 2022, qu'en ce qui concerne l'atteinte au droit au respect de la vie privée et au droit à la protection des données à caractère personnel, tels qu'ils sont garantis par l'article 22 de la Constitution, par l'article 8 de la Convention européenne des droits de l'homme et par les articles 7, 8 et 52 de la Charte. La Cour limite son examen à ces dispositions.

B.11.2. 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 ».

L'article 7 de la Charte dispose :

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

L'article 8 de la Charte dispose :

« 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 ».

L'article 52, paragraphe 1, de la Charte dispose :

« 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 ».

L'article 52, paragraphe 3, de la Charte dispose :

« 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 ».

B.11.3. Le Constituant a recherché la plus grande concordance possible entre l'article 22 de la Constitution et l'article 8 de la Convention européenne des droits de l'homme (*Doc. parl.*, Chambre, 1992-1993, n° 997/5, p. 2).

La portée de cet article 8 est analogue à celle de la disposition constitutionnelle précitée, de sorte que les garanties que fournissent ces deux dispositions forment un tout indissociable.

Lorsque la Charte contient des droits correspondant à des droits garantis par la Convention européenne des droits de l'homme, « leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention ». Cette disposition aligne le sens et la portée des droits qui sont garantis par la Charte sur les droits correspondants qui sont garantis par la Convention européenne des droits de l'homme.

Les explications relatives à la Charte (2007/C-303/02), publiées au *Journal officiel* du 14 décembre 2007, indiquent que, parmi les articles « dont le sens et la portée sont les mêmes que ceux des articles correspondants dans la CEDH », l'article 7 de la Charte correspond à l'article 8 de la Convention européenne des droits de l'homme.

La Cour de justice rappelle à cet égard que « l'article 7 de la Charte, relatif au droit au respect de la vie privée et familiale, contient des droits correspondant à ceux garantis par l'article 8, paragraphe 1, de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950 (ci-après : la CEDH), et qu'il convient donc, conformément à l'article 52, paragraphe 3, de la Charte, de donner audit article 7 le même sens et la même portée que ceux conférés à l'article 8, paragraphe 1, de la CEDH, tel qu'il est interprété par la jurisprudence de la Cour européenne des droits de l'homme » (CJUE, 17 décembre 2015, C-419/14, *WebMindLicenses Kft.*, ECLI:EU:C:2015:832, point 70; 14 février 2019, C-345/17, *Buivids*, ECLI:EU:C:2019:122, point 65).

En ce qui concerne l'article 8 de la Charte, la Cour de justice considère qu'« ainsi que le prévoit expressément l'article 52, paragraphe 3, seconde phrase, de la Charte, l'article 52, paragraphe 3, première phrase, de celle-ci ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue que la CEDH », et que « l'article 8 de la Charte concerne un droit fondamental distinct de celui consacré à l'article 7 de celle-ci et qui n'a pas d'équivalent dans la CEDH » (CJUE, grande chambre, 21 décembre 2016, C-203/15 et C-698/15, *Tele2 Sverige AB*, ECLI:EU:C:2016:970, point 129).

Il découle de ce qui précède que, dans le champ d'application du droit de l'Union européenne, l'article 22 de la Constitution, l'article 8 de la Convention européenne des droits de l'homme et l'article 7 de la Charte garantissent des droits fondamentaux analogues, tout comme l'article 8 de cette Charte qui vise spécifiquement la protection des données à caractère personnel.

B.12.1. L'article 107/5 de la loi du 13 juin 2005, inséré par l'article 3 de la loi du 20 juillet 2022, prévoit que l'utilisation de la cryptographie est libre, sous réserve des trois exceptions qu'il énumère.

B.12.2. Les travaux préparatoires de la disposition attaquée mettent en évidence que le législateur a souhaité favoriser l'utilisation de la cryptographie, dès lors qu'il s'agit d'un système efficace pour assurer la sécurité des communications, ce qui permet de protéger la vie privée, le potentiel scientifique et économique, la compétitivité des entreprises, le secret médical et le secret des affaires (*Doc. parl.*, Chambre, 2021-2022, DOC 55-2572/001, p. 17).

B.12.3. L'article 107/5 de la loi du 13 juin 2005, tel qu'il a été remplacé par l'article 3 de la loi du 20 juillet 2022, établit des exceptions à la libre utilisation de la cryptographie, afin d'éviter que le recours à ce procédé empêche les communications d'urgence, dont l'identification de la ligne appelante ou la fourniture des données d'identification de l'appelant (§ 2), afin d'éviter qu'un opérateur ne puisse exécuter une demande ciblée d'une autorité compétente, dans les conditions prévues par la loi, dans le but d'identifier l'utilisateur final, de repérer et de localiser des communications non accessibles au public (§ 3) et afin d'éviter qu'un opérateur étranger dont l'utilisateur final ou l'abonné est situé sur le territoire belge empêche l'exécution d'une demande d'une autorité compétente, étant entendu que, dans ce dernier cas, toute clause contractuelle contraire est frappée de nullité (§ 4).

B.12.4. Comme il est dit en B.10.1 et B.10.2, les griefs des parties requérantes portent sur les deux dernières exceptions.

B.12.5. Ces exceptions visent à éviter que le recours à la cryptographie empêche un opérateur de remplir les obligations en matière de conservation des données qui sont fixées par la loi, notamment dans le cas d'un utilisateur qui aurait fait appel aux services d'un opérateur étranger (*ibid.*, pp. 19-21). Il s'agit d'objectifs légitimes au sens de l'article 8 de la Convention européenne des droits de l'homme, de l'article 52, paragraphe 1, de la Charte et de l'article 15, paragraphe 1, de la directive 2002/58/CE, qui est transposé par la loi du 20 juillet 2022.

B.13.1. Il ressort tant de l'arrêt de la Cour n° 57/2021 précité que de l'arrêt de la Cour de justice en cause de *La Quadrature du Net e.a.* précité, sur lequel il est basé, que l'article 15, paragraphe 1, de la directive 2002/58/CE, lu à la lumière des articles 7, 8 et 52, paragraphe 1, de la Charte, ne s'oppose pas à la conservation des données d'identification, des données

relatives au trafic et des données de localisation, dans le respect de certaines conditions, notamment que les mesures concernées prévoient, aux termes de règles claires et précises, que la conservation des données soit subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus.

B.13.2. Concernant la conservation de communications internet cryptées et l'accès à celles-ci, la Cour européenne des droits de l'homme a jugé, dans l'arrêt *Podchasov c. Russie* (CEDH, 13 février 2024, ECLI:CE:ECHR:2024:0213JUD003369619) :

« 63. Dans le contexte de la collecte et du traitement de données à caractère personnel, il est essentiel de fixer des règles claires et détaillées régissant la portée et l'application des mesures et imposant un minimum d'exigences concernant, notamment, la durée, le stockage, l'utilisation, l'accès des tiers, les procédures destinées à préserver l'intégrité et la confidentialité des données et les procédures de destruction de celles-ci, de manière à ce que les justiciables disposent de garanties suffisantes contre les risques d'abus et d'arbitraire (*ibid.*, § 99; voy. également *P.N. c. Allemagne*, n° 74440/17, § 62, 11 juin 2020). Le droit interne doit notamment assurer que les données enregistrées sont pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées, et qu'elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées. Le droit interne doit aussi contenir des garanties aptes à protéger efficacement les données à caractère personnel enregistrées contre les usages impropres et abusifs (voy. *S. et Marper*, précité, § 103). D'après les principes clés en la matière, la conservation des données doit être proportionnée au but pour lequel elles ont été recueillies et être limitée dans le temps (ibid., § 107).

64. Dans le contexte de la surveillance secrète, où un pouvoir de l'exécutif s'exerce en secret, le risque d'arbitraire apparaît avec netteté. Pour satisfaire à l'exigence de « prévisibilité », la loi doit être rédigée avec suffisamment de clarté pour indiquer à tous de manière adéquate en quelles circonstances et sous quelles conditions elle habilite la puissance publique à prendre pareilles mesures secrètes. En outre, puisque l'application de mesures de surveillance secrète des communications échappe au contrôle des intéressés comme du public, la « loi » irait à l'encontre de la prééminence du droit si le pouvoir d'appréciation accordé à l'exécutif ou à un juge ne connaissait pas de limites. En conséquence, elle doit définir l'étendue et les modalités d'exercice d'un tel pouvoir avec une clarté suffisante pour fournir à l'individu une protection adéquate contre l'arbitraire (voy. *Roman Zakharov*, précité, §§ 229-30). Pour une description détaillée des garanties que doit prévoir la loi pour répondre aux exigences de « qualité de la loi » et pour garantir que les mesures de surveillance secrète soient appliquées uniquement lorsqu'elles sont « nécessaires dans une société démocratique », voir *Roman Zakharov*, §§ 231-34, et *Big Brother Watch et autres*, §§ 335-39, tous deux précités.

65. La Cour rappelle enfin que la confidentialité des communications est un élément fondamental du droit au respect de la vie privée et de la correspondance, tel que garanti par

l'article 8. Les utilisateurs de services de télécommunications et de services internet doivent se voir garantir le respect de leur vie privée et de leur liberté d'expression, même si cette garantie ne peut être absolue et doit parfois s'effacer devant d'autres impératifs légitimes, tels que la prévention des troubles à l'ordre public ou la lutte contre la criminalité, ou encore la protection des droits et des libertés d'autrui (voy. *K.U. c. Finlande*, n° 2872/02, § 49, CEDH 2008, et *Delfi AS c. Estonie* [GC], n° 64569/09, § 149, CEDH 2015) » (traduction libre).

Dans cet arrêt, la Cour européenne des droits de l'homme a jugé que la législation russe en cause était disproportionnée aux objectifs légitimes poursuivis, à savoir la protection de la sécurité nationale, la défense de l'ordre et la prévention du crime, ainsi que la protection des droits d'autrui. Dans la mise en balance opérée par la Cour européenne des droits de l'homme, l'obligation pesant en vertu de la législation russe sur les organisateurs de communication numérique de décrypter toutes les données conservées à la demande des autorités compétentes, en ce compris les contenus de communications chiffrées de bout en bout (*end-to-end*) a été jugée disproportionnée en raison du risque d'affaiblissement du mécanisme de chiffrement pour tous les utilisateurs de services de communication numérique (CEDH, 13 février 2024, *Podchasov c. Russie*, précité, §§ 68-80).

B.13.3. À la différence de la législation russe en cause dans l'arrêt *Podchasov c. Russie* précité, l'article 107/5, §§ 3 et 4, de la loi du 13 juin 2005 encourage le recours à la cryptographie (§ 1er) et se limite à modaliser l'étendue des pouvoirs des opérateurs concernant l'utilisation de cette cryptographie afin qu'une demande ciblée d'une autorité compétente, qui viserait à identifier l'utilisateur final et à rechercher et localiser des communications non accessibles au public, dans le cas prévu par une autre disposition légale et dans les conditions visées à l'article 15, paragraphe 1, de la directive 2002/58/CE, soit effectivement possible.

En outre, les données qui doivent être conservées pour pouvoir satisfaire à une demande ciblée d'une autorité compétente sont déterminées avec précision et ne portent pas sur le contenu de la communication. L'on n'aperçoit pas en quoi les conditions visées à l'article 107/5, §§ 3 et 4, de la loi du 13 juin 2005 produiraient des effets disproportionnés pour les utilisateurs.

B.13.4. En ce qu'ils portent sur l'article 3 de la loi du 20 juillet 2022, le moyen unique dans l'affaire n° 7931 et le cinquième moyen dans l'affaire n° 7932 ne sont pas fondés.

2. Les mesures employées au niveau du réseau ou de l'utilisateur final pour détecter la fraude et les utilisations malveillantes des réseaux et des services (article 4)

B.14. Le sixième moyen dans l'affaire n° 7932 porte sur l'article 4 de la loi du 20 juillet 2022, qui insère, dans la loi du 13 juin 2005, un article 121/8 rédigé comme suit :

« § 1er. Sans prendre connaissance du contenu des communications, les opérateurs prennent les mesures appropriées, proportionnées, préventives et curatives, compte tenu des possibilités techniques les plus récentes, de manière à détecter les fraudes et utilisations malveillantes sur leurs réseaux et services et éviter que les utilisateurs finaux ne subissent un préjudice ou ne soient importunés.

Le Roi peut préciser les mesures à prendre par les opérateurs en vertu de l'alinéa 1er.

L'Institut a le pouvoir de donner des instructions contraignantes, y compris des instructions concernant les délais d'exécution, en vue de l'application du présent paragraphe.

§ 2. Lorsque cela se justifie au regard de la gravité des circonstances, qui doivent être examinées au cas par cas, les mesures appropriées visées au paragraphe 1er, alinéa 1er, peuvent comprendre notamment :

- des mesures au niveau du réseau, tels que le blocage des numéros, de services, des URLs, de noms de domaine, d'adresses IP ou de tout autre élément d'identification de la communication électronique;

- des mesures au niveau de l'utilisateur final, telles que la désactivation complète ou partielle de certains services ou équipements ».

B.15.1. Les parties requérantes soutiennent que l'article 121/8, § 2, de la loi du 13 juin 2005, tel qu'il a été inséré par l'article 4 de la loi du 20 juillet 2022, n'est pas compatible avec les articles 10, 11, 22 et 29 de la Constitution, lus en combinaison ou non 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 et avec la directive 2002/58/CE. Selon elles, des mesures de blocage et de désactivation peuvent être mises en œuvre pour des finalités plus larges que celles qui sont visées à l'article 121/8, § 1er, de la loi du 13 juin 2005, notamment à

des fins de censure. Par ailleurs, aucune évaluation par un organe indépendant ni aucun critère d'évaluation n'est établi pour vérifier si ces mesures s'inscrivent dans les finalités prévues à l'article 121/8, § 1er, précité. Partant, selon les parties requérantes, l'article 121/8, § 2, de la loi du 13 juin 2005 viole la liberté d'expression et d'information.

B.15.2. Il ressort de ce qui précède que les parties requérantes formulent des griefs contre l'article 4 de la loi du 20 juillet 2022 en ce qui concerne la liberté d'expression et d'information.

B.15.3. L'article 10 de la Convention européenne des droits de l'homme dispose :

« 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 frontière. Le présent article n'empêche pas les États de soumettre les entreprises de radiodiffusion, de cinéma ou de télévision à un régime d'autorisations.

2. L'exercice de ces libertés comportant des devoirs et des responsabilités peut être soumis à certaines formalités, conditions, restrictions ou sanctions prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire ».

L'article 11 de la Charte dispose :

« 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 ».

B.15.4. En ce qu'ils reconnaissent le droit à la liberté d'expression, l'article 10 de la Convention européenne des droits de l'homme et l'article 11, paragraphe 1, de la Charte ont une portée analogue à celle de l'article 19 de la Constitution, qui reconnaît la liberté de manifester ses opinions en toute matière.

Dès lors, les garanties fournies par ces dispositions forment un ensemble indissociable.

B.15.5. L'article 19 de la Constitution dispose :

« La liberté des cultes, celle de leur exercice public, ainsi que la liberté de manifester ses opinions en toute matière, sont garanties, sauf la répression des délits commis à l'occasion de l'usage de ces libertés ».

L'article 19 de la Constitution interdit que la liberté d'expression soit soumise à des restrictions préventives, mais non que les infractions qui sont commises à l'occasion de la mise en œuvre de cette liberté soient sanctionnées.

B.15.6. La Cour n'associe à son examen de l'article 19 de la Constitution que l'article 10 de la Convention européenne des droits de l'homme et les articles 11 et 52 de la Charte, dès lors que la violation des autres dispositions citées en B.15.1 ne fait l'objet d'aucun développement.

B.16.1. La liberté d'expression peut, en vertu de l'article 10, paragraphe 2, de la Convention européenne des droits de l'homme, être soumise, sous certaines conditions, à des formalités, conditions, restrictions ou sanctions, en vue de la sécurité nationale, de l'intégrité territoriale, de la sûreté publique, de la défense de l'ordre et de la prévention du crime, de la protection de la santé ou de la morale, de la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire. Les exceptions dont elle est assortie appellent toutefois « une interprétation étroite, et le besoin de la restreindre doit se trouver établi de manière contraignante » (CEDH, grande chambre, 20 octobre 2015, *Pentikäinen c. Finlande*, ECLI:CE:ECHR:2015:1020JUD001188210, § 87).

B.16.2. Une ingérence dans la liberté d'expression doit être prévue par une loi suffisamment accessible et précise. Elle doit donc être formulée en des termes clairs et suffisamment précis pour que chacun puisse – en s'entourant au besoin de conseils éclairés – prévoir, à un degré raisonnable, dans les circonstances de la cause, les conséquences d'un acte déterminé. Ces exigences ne peuvent cependant pas aboutir à une rigidité excessive, empêchant de tenir compte des circonstances ou conceptions sociales changeantes dans l'interprétation d'une norme législative (CEDH, grande chambre, 22 octobre 2007, *Lindon, Otchakovsky-Laurens et July c. France*, ECLI:CE:ECHR:2007:1022JUD002127902, § 41;

grande chambre, 7 juin 2012, *Centro Europa 7 S.R.L. et Di Stefano c. Italie,* ECLI:CE:CEDH:2012:0607JUD003843309, §§ 141-142; grande chambre, 15 octobre 2015, *Perinçek c. Suisse*, ECLI:CE:CEDH:2015:1015JUD002751008, §§ 131-133). Il doit ensuite être démontré que la restriction est nécessaire dans une société démocratique, qu'elle répond à un besoin social impérieux et qu'elle est proportionnée aux buts légitimes poursuivis.

B.17. Il ressort des travaux préparatoires que, par l'article 121/8, § 2, de la loi du 13 juin 2005, tel qu'il a été inséré par l'article 4 de la loi du 20 juillet 2022, le législateur entendait faire face à la situation dans laquelle l'utilisateur final du réseau de communications est victime d'une fraude, en incitant les opérateurs à réagir en faveur de cet utilisateur et en prévoyant que dans des cas graves de fraude ou d'utilisation malveillante du réseau, des « mesures fortes » et rapides puissent être prises. Dans ce cadre, l'énumération des mesures de blocage et de désactivation visées dans cet article a aussi pour objectif d'offrir une plus grande sécurité juridique aux opérateurs (*Doc. parl.*, Chambre, 2021-2022, DOC 55-2572/001, pp. 21-22).

Ces objectifs sont légitimes et peuvent fonder une restriction de la liberté d'expression. Il faut encore examiner si la mesure attaquée est pertinente et proportionnée au regard de ces objectifs.

B.18. Afin d'éviter des cas graves de fraude et d'utilisation malveillante du réseau au préjudice de l'utilisateur final, le législateur pouvait prévoir la possibilité de prendre les mesures visées à l'article 121/8, § 2, dès lors que celles-ci sont de nature à réaliser les objectifs précités. Par ailleurs, les parties requérantes ne démontrent pas en quoi ces mesures ne sont pas pertinentes au regard de ces objectifs.

B.19.1. Enfin, les mesures visées à l'article 121/8, § 2, de la loi du 13 juin 2005 ne vont pas au-delà de ce qui est nécessaire pour réaliser les objectifs poursuivis par le législateur.

B.19.2. Tout d'abord, les notions de « fraude » et d'« utilisation malveillante du réseau ou du service » sont définies à l'article 2, 5/5° et 5/6°, de la loi du 13 juin 2005, tel qu'il a été

modifié par l'article 2 de la loi du 20 juillet 2022. Aux termes de ces dispositions, la fraude renvoie à « un acte malhonnête fait dans l'intention de tromper en contrevenant à la loi, aux règlements ou au contrat et de se procurer ou de procurer à autrui un avantage illicite au préjudice de l'opérateur ou de l'utilisateur final, commis par le biais de l'utilisation d'un service de communications électroniques » (5/5°), tandis que l'utilisation malveillante du réseau ou du service consiste en une « utilisation du réseau ou du service de communications électroniques afin d'importuner son correspondant ou de provoquer des dommages » (5/6°).

B.19.3. Il appartient aux opérateurs de vérifier l'existence d'une fraude ou d'une utilisation malveillante du réseau ou du service et d'apprécier, au cas par cas, la « gravité des circonstances » avant de pouvoir prendre les mesures prévues à l'article 121/8, § 2, de la loi du 13 juin 2005, tel qu'il a été inséré par l'article 4 de la loi du 20 juillet 2022. Il ressort des travaux préparatoires de la disposition attaquée que, dans cette hypothèse, les opérateurs agissent soit d'initiative, soit à la suite d'un signalement de l'utilisateur final ou d'un tiers; dans tous les cas, il est interdit aux opérateurs de prendre connaissance du contenu des communications (*Doc. parl.*, Chambre, 2021-2022, DOC 55-2572/003, pp. 85-87).

Dans ce cadre, les opérateurs agissent sous le contrôle de l'Institut belge des services postaux et des télécommunications (ci-après : l'IBPT), qui, en vertu de l'article 14, § 1er, 3°, *a)*, de la loi du 17 janvier 2003, est chargé de contrôler le respect de la loi du 13 juin 2005 et de ses arrêtés d'exécution. L'article 121/8 de la loi du 13 juin 2005 ajoute que l'IBPT « a le pouvoir de donner des instructions contraignantes, y compris des instructions concernant les délais d'exécution » (§ 1er, alinéa 3), en ce qui concerne les mesures prises par les opérateurs sur la base de cette disposition.

À l'occasion du contrôle qu'il exerce sur les mesures prises par les opérateurs sur la base de l'article 121/8, § 2, de la loi du 13 juin 2005, l'IBPT vérifie notamment l'existence d'une fraude ou d'une utilisation malveillante du réseau, le caractère approprié et proportionné de la mesure ainsi que la gravité des circonstances de l'espèce.

Enfin, en vertu de l'article 2, § 1er, de loi du 17 janvier 2003 « concernant les recours et le traitement des litiges à l'occasion de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et télécommunications belges », les décisions de l'IBPT « peuvent faire

l'objet d'un recours en pleine juridiction devant la Cour des marchés statuant comme en référé », étant entendu que « toute personne ayant un intérêt pour agir peut introduire le recours ».

B.20. Le sixième moyen dans l'affaire n° 7932 n'est pas fondé.

3. La conservation des données de trafic (article 5)

B.21.1. Les premier et deuxième moyens dans l'affaire n° 7930, le moyen unique dans l'affaire n° 7931, la première branche du premier moyen et la première branche du troisième moyen dans l'affaire n° 7932 portent sur l'article 5 de la loi du 20 juillet 2022, qui dispose :

« À l'article 122 de la [loi du 13 juin 2005], modifié en dernier lieu par la loi du 21 décembre 2021, les modifications suivantes sont apportées :

1° dans le paragraphe 1er, l'alinéa 2 est abrogé;

2° dans le paragraphe 2, les modifications suivantes sont apportées :

a) l'alinéa 1er est remplacé par ce qui suit :

' Par dérogation au paragraphe 1er, et dans le seul but d'établir les factures des abonnés ou d'effectuer les paiements d'interconnexion, les opérateurs peuvent conserver et traiter les données de trafic nécessaires à cette fin. ';

b) dans l'alinéa 2, les mots ' 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 ' sont remplacés par les mots ' du RGPD et de la loi du 30 juillet 2018 ';

c) dans l'alinéa 3, le mot ' énumérées ' est remplacé par le mot ' visées ';

3° dans le paragraphe 3, les modifications suivantes sont apportées :

a) dans l'alinéa 1er, 2°, les mots ' la manifestation de volonté libre, spécifique et basée sur des informations par laquelle l'intéressé ou son représentant légal accepte que des données relatives au trafic se rapportant à lui soient traitées ' sont remplacés par les mots ' le consentement au sens de l'article 4, 11), du RGPD ';

b) dans l'alinéa 1er, 3°, les mots ' de manière simple ' sont remplacés par les mots ' facilement et à tout moment ';

c) dans l'alinéa 2, les mots ' 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 ' sont remplacés par les mots ' du RGPD et de la loi du 30 juillet 2018 ';

4° le paragraphe 4 est remplacé par ce qui suit :

' § 4. Par dérogation au paragraphe 1er, de manière à pouvoir prendre les mesures appropriées visées à l'article 121/8, § 1er, de permettre d'établir la fraude ou l'utilisation malveillante du réseau ou du service ou d'identifier son auteur et son origine, et pour autant qu'il les traite ou les génère dans le cadre de la fourniture de ce réseau ou de ce service, l'opérateur :

1° conserve, dans le cadre de la fourniture d'un service de communications interpersonnelles et pendant quatre mois à partir de la date de la communication, les données de trafic nécessaires à ces fins parmi les données de trafic suivantes :

- l'identifiant de l'origine de la communication;

- l'identifiant de la destination de la communication;

- les dates et heures précises de début et de fin de la communication;

- la localisation des équipements terminaux des parties à la communication au début et à la fin de la communication;

2° conserve pendant douze mois à partir de la date de la communication les données de trafic suivantes relatives aux communications entrantes dans le cadre de la fourniture de services de communications interpersonnelles afin d'identifier l'auteur de la communication :

- le numéro de téléphone à l'origine de la communication entrante, ou;

- l'adresse IP ayant servi à l'envoi de la communication entrante, l'horodatage et le port utilisé, et;

- les dates et heures précises du début et de fin de la communication entrante;

3° conserve les données visées au 1° qui sont relatives à une fraude spécifique identifiée ou une utilisation malveillante du réseau spécifique identifiée le temps nécessaire à son analyse et à sa résolution, le cas échéant au-delà du délai de quatre mois visé au 1°;

4° conserve les données de trafic visées au 2° et relatives à une utilisation malveillante spécifique du réseau, le temps nécessaire au traitement de cette dernière, le cas échéant au-delà du délai de douze mois visé au 2°;

5° traite les données de trafic nécessaires à ces fins, en ce compris, lorsque c'est nécessaire, les données visées au paragraphe 2.

Par dérogation au paragraphe 1er, de manière à pouvoir prendre les mesures appropriées visées à l'article 121/8, § 1er, de permettre d'établir la fraude ou l'utilisation malveillante du réseau ou du service ou d'identifier son auteur et son origine, l'opérateur peut conserver et traiter d'autres données que celles visées à l'alinéa 1er considérées nécessaires à ces fins.

Le Roi peut préciser et étendre, par arrêté délibéré en Conseil des ministres et après avis de l'Institut et de l'Autorité de protection des données, les données de trafic dont la conservation doit être considérée comme nécessaire pour la poursuite des finalités prévues au présent paragraphe.

En cas de fraude présumée ou d'utilisation malveillante présumée, les opérateurs peuvent transmettre aux autorités compétentes toutes les données légalement conservées en relation avec la fraude présumée ou l'utilisation malveillante présumée. ';

5° il est inséré un paragraphe 4/1 rédigé comme suit :

' § 4/1. Par dérogation au paragraphe 1er, les opérateurs peuvent conserver et traiter les données de trafic qui sont nécessaires pour assurer la sécurité et le bon fonctionnement de leurs réseaux et services de communications électroniques, et en particulier pour détecter et analyser une atteinte potentielle ou réelle à cette sécurité, en ce compris identifier l'origine de cette atteinte.

Les opérateurs peuvent les conserver pour une durée de douze mois à partir de la date de la communication.

Les opérateurs peuvent conserver les données visées à l'alinéa 1er relatives à une atteinte spécifique à la sécurité du réseau pendant la durée nécessaire pour la traiter, le cas échéant au-delà du délai de douze mois visé à l'alinéa 2.

En cas d'atteinte à la sécurité de leurs réseaux et services de communications électroniques, les opérateurs peuvent transmettre aux autorités compétentes toutes les données légalement conservées en relation avec l'atteinte à la sécurité de leurs réseaux et services de communications électroniques. ';

6° il est inséré un paragraphe 4/2 rédigé comme suit :

' § 4/2. Par dérogation au paragraphe 1er, les opérateurs conservent et traitent les données de trafic nécessaires pour répondre à une obligation imposée par une norme législative formelle, pour la durée requise à cette fin. ';

7° le paragraphe 5 est remplacé par ce qui suit :

' § 5. Les données énumérées dans le présent article ne peuvent être traitées que par les personnes chargées par l'opérateur de la facturation ou de la gestion du trafic, du traitement des demandes de renseignements des abonnés, de la lutte contre les fraudes ou l'utilisation malveillante du réseau, de la sécurité du réseau, du respect de ses obligations légales, du marketing des services de communications électroniques propres ou de la fourniture de services

qui font usage de données de trafic ou de localisation et par les membres de sa Cellule de coordination visée à l'article 127/3. ';

8° dans le paragraphe 6, les mots ' L'Institut ' sont remplacés par les mots ' L'Institut, le Service de médiation pour les télécommunications. ' ».

B.21.2. Du fait de cette modification, l'article 122 de la loi du 13 juin 2005 dispose :

« § 1er. Les opérateurs suppriment les données de trafic concernant les abonnés ou les utilisateurs finaux de leurs données de trafic ou rendent ces données anonymes, dès qu'elles ne sont plus nécessaires pour la transmission de la communication.

§ 2. Par dérogation au paragraphe 1er, et dans le seul but d'établir les factures des abonnés ou d'effectuer les paiements d'interconnexion, les opérateurs peuvent conserver et traiter les données de trafic nécessaires à cette fin.

Sans préjudice de l'application du RGPD et de la loi du 30 juillet 2018, l'opérateur informe, avant le traitement, l'abonné ou, le cas échéant, l'utilisateur final auquel les données se rapportent :

1° des types de données de trafic traitées;

2° des objectifs précis du traitement;

3° de la durée du traitement.

Le traitement des données visées à l'alinéa 1er, est seulement autorisé jusqu'à la fin de la période de contestation de la facture ou jusqu'à la fin de la période au cours de laquelle une action peut être menée pour en obtenir le paiement.

§ 3. Par dérogation au § 1er et dans le seul but d'assurer le marketing des services de communications électroniques propres et d'établir le profil d'utilisation visé à l'article 110, § 4, alinéa premier, article 110/1 et article 111, § 3, alinéa 2, ou des services à données de trafic ou de localisation, les opérateurs ne peuvent traiter les données visées au § 1er qu'aux conditions suivantes :

1° L'opérateur informe l'abonné ou, le cas échéant, l'utilisateur final auquel se rapportent les données, avant d'obtenir le consentement de celui-ci en vue du traitement :

a) des types de données de trafic traitées;

b) des objectifs précis du traitement;

c) de la durée du traitement.

2° L'abonné ou, le cas échéant, l'utilisateur final, a, préalablement au traitement, donné son consentement pour le traitement.

Par consentement pour le traitement au sens du présent article, on entend le consentement au sens de l'article 4, 11), du RGPD.

3° L'opérateur concerné offre gratuitement à ses abonnés ou ses utilisateurs finaux la possibilité de retirer le consentement donné facilement et à tout moment.

4° Le traitement des données en question se limite aux actes et à la durée nécessaires pour fournir le service à données de trafic ou de localisation en question pour l'établissement du plan d'utilisation visé à l'article 110, § 4, alinéa 1er, article 110/1 et article 111, § 3, alinéa 2 ou pour l'action de marketing en question.

Ces conditions sont d'application sous réserve des conditions complémentaires découlant de l'application du RGPD et de la loi du 30 juillet 2018.

§ 4. Par dérogation au paragraphe 1er, de manière à pouvoir prendre les mesures appropriées visées à l'article 121/8, § 1er, de permettre d'établir la fraude ou l'utilisation malveillante du réseau ou du service ou d'identifier son auteur et son origine, et pour autant qu'il les traite ou les génère dans le cadre de la fourniture de ce réseau ou de ce service, l'opérateur :

1° conserve, dans le cadre de la fourniture d'un service de communications interpersonnelles et pendant quatre mois à partir de la date de la communication, les données de trafic nécessaires à ces fins parmi les données de trafic suivantes :

- l'identifiant de l'origine de la communication;

- l'identifiant de la destination de la communication;

- les dates et heures précises de début et de fin de la communication;

- la localisation des équipements terminaux des parties à la communication au début et à la fin de la communication;

2° conserve pendant douze mois à partir de la date de la communication les données de trafic suivantes relatives aux communications entrantes dans le cadre de la fourniture de services de communications interpersonnelles afin d'identifier l'auteur de la communication :

- le numéro de téléphone à l'origine de la communication entrante, ou;

- l'adresse IP ayant servi à l'envoi de la communication entrante, l'horodatage et le port utilisé, et;

- les dates et heures précises du début et de fin de la communication entrante;

3° conserve les données visées au 1° qui sont relatives à une fraude spécifique identifiée ou une utilisation malveillante du réseau spécifique identifiée le temps nécessaire à son analyse et à sa résolution, le cas échéant au-delà du délai de quatre mois visé au 1°;

4° conserve les données de trafic visées au 2° et relatives à une utilisation malveillante spécifique du réseau, le temps nécessaire au traitement de cette dernière, le cas échéant au-delà du délai de douze mois visé au 2°;

5° traite les données de trafic nécessaires à ces fins, en ce compris, lorsque c'est nécessaire, les données visées au paragraphe 2.

Par dérogation au paragraphe 1er, de manière à pouvoir prendre les mesures appropriées visées à l'article 121/8, § 1er, de permettre d'établir la fraude ou l'utilisation malveillante du réseau ou du service ou d'identifier son auteur et son origine, l'opérateur peut conserver et traiter d'autres données que celles visées à l'alinéa 1er considérées nécessaires à ces fins.

Le Roi peut préciser et étendre, par arrêté délibéré en Conseil des ministres et après avis de l'Institut et de l'Autorité de protection des données, les données de trafic dont la conservation doit être considérée comme nécessaire pour la poursuite des finalités prévues au présent paragraphe.

En cas de fraude présumée ou d'utilisation malveillante présumée, les opérateurs peuvent transmettre aux autorités compétentes toutes les données légalement conservées en relation avec la fraude présumée ou l'utilisation malveillante présumée.

§ 4/1. Par dérogation au paragraphe 1er, les opérateurs peuvent conserver et traiter les données de trafic qui sont nécessaires pour assurer la sécurité et le bon fonctionnement de leurs réseaux et services de communications électroniques, et en particulier pour détecter et analyser une atteinte potentielle ou réelle à cette sécurité, en ce compris identifier l'origine de cette atteinte.

Les opérateurs peuvent les conserver pour une durée de douze mois à partir de la date de la communication.

Les opérateurs peuvent conserver les données visées à l'alinéa 1er relatives à une atteinte spécifique à la sécurité du réseau pendant la durée nécessaire pour la traiter, le cas échéant au-delà du délai de douze mois visé à l'alinéa 2.

En cas d'atteinte à la sécurité de leurs réseaux et services de communications électroniques, les opérateurs peuvent transmettre aux autorités compétentes toutes les données légalement conservées en relation avec l'atteinte à la sécurité de leurs réseaux et services de communications électroniques.

§ 4/2. Par dérogation au paragraphe 1er, les opérateurs conservent et traitent les données de trafic nécessaires pour répondre à une obligation imposée par une norme législative formelle, pour la durée requise à cette fin.

§ 5. Les données énumérées dans le présent article ne peuvent être traitées que par les personnes chargées par l'opérateur de la facturation ou de la gestion du trafic, du traitement des demandes de renseignements des abonnés, de la lutte contre les fraudes ou l'utilisation

malveillante du réseau, de la sécurité du réseau, du respect de ses obligations légales, du marketing des services de communications électroniques propres ou de la fourniture de services qui font usage de données de trafic ou de localisation et par les membres de sa Cellule de coordination visée à l'article 127/3.

§ 6. L'Institut, le Service de médiation pour les télécommunications, l'Autorité belge de la concurrence, les juridictions de l'ordre judiciaire et le Conseil d'Etat peuvent, dans le cadre de leurs compétences, être informés des données de trafic et de facture pertinentes en vue du règlement de litiges, parmi lesquels des litiges relatifs à l'interconnexion et la facturation ».

B.22.1. La partie requérante dans l'affaire n° 7930 prend les premier et deuxième moyens de la violation des articles 11, 12, 22 et 29 de la Constitution, de l'article 15, paragraphe 1, et des articles 5, 6 et 9 de la directive 2002/58/CE, lus à la lumière des articles 7, 8, 11, 47 et 52, paragraphe 1, de la Charte, des articles 6, 8, 10, 11 et 18 de la Convention européenne des droits de l'homme et des articles 13 et 54 de la directive (UE) 2016/680, en ce que l'article 5, 4° et 5°, de la loi du 20 juillet 2022 instaure une obligation généralisée de conservation des données de communications, sans que cette conservation soit nécessaire et strictement limitée au regard du but poursuivi. La partie requérante ne formule aucun grief explicite contre l'article 5, 1° à 3° et 6° à 8°.

B.22.2. La partie requérante dans l'affaire n° 7931 prend un moyen unique de la violation des articles 11, 12, 22 et 29 de la Constitution, lus en combinaison ou non avec les articles 7, 8, 11, 47 et 52, paragraphe 1, de la Charte, avec l'article 8 de la Convention européenne des droits de l'homme, avec les articles 5, 6 et 15 de la directive 2002/58/CE et avec les articles 13 et 54 de la directive (UE) 2016/680. Elle soutient que l'article 5, 4°, de la loi du 20 juillet 2022 prévoit une obligation de conservation systématique et indifférenciée de certaines données afin de lutter contre la criminalité en général, alors qu'une telle conservation n'est admise que dans le cadre de la lutte contre la criminalité grave, et en ce que l'obligation de conservation qu'il établit est en toute hypothèse disproportionnée.

À titre subsidiaire, la partie requérante demande de poser une question préjudicielle à la Cour de justice. Par ailleurs, selon la partie requérante, l'article 5, 5°, de la loi du 20 juillet 2022 n'est pas nécessaire au regard des autres obligations qui incombent aux opérateurs et prévoit un délai de conservation trop long.

B.22.3. Les parties requérantes dans l'affaire n° 7932 prennent un premier moyen de la violation des articles 10, 11, 13, 15, 22, 23 et 29 de la Constitution, lus en combinaison ou non avec les articles 5, 6, 8, 9, 10, 11, 14 et 18 de la Convention européenne des droits de l'homme, avec les articles 7, 8, 11, 47 et 52 de la Charte, avec l'article 5, paragraphe 4, du Traité sur l'Union européenne et avec l'article 6 de la directive 2002/58/CE, avec la directive (UE) 2016/680 et avec le RGPD. Dans la première branche de ce moyen, les parties requérantes soutiennent que l'article 5, 4° et 5°, de la loi du 20 juillet 2022 prévoit une conservation généralisée et indifférenciée des données qui n'est admissible que dans le cadre de la protection de la sécurité nationale, sans qu'il soit prévu que les données conservées soient effacées ou rendues anonymes lorsque la conservation n'est plus nécessaire. Par ailleurs, l'article 5 de la loi du 20 juillet 2022 prévoit une identité de traitement entre toutes les données, sans distinction en fonction de la finalité (lutte contre la criminalité grave).

Les mêmes parties requérantes prennent un troisième moyen de la violation des articles 10, 11, 15, 22 et 29 de la Constitution, lus en combinaison ou non avec les articles 5, 6, 8, 9, 10, 11, 14 et 18 de la Convention européenne des droits de l'homme, avec les articles 7, 8, 11, 47 et 52 de la Charte, avec l'article 5, paragraphe 4, du Traité sur l'Union européenne ainsi qu'avec la directive 2002/58/CE, avec la directive (UE) 2016/680 et avec le RGPD. Dans la première branche de ce moyen, elles affirment que l'article 5, 4°, de la loi du 20 juillet 2022 crée une obligation de conservation généralisée et indifférenciée des données afin de lutter contre la fraude et les utilisations malveillantes du réseau ou du service, et ce, au profit des opérateurs dans le cadre de leurs missions, ce qui est trop vague et trop large.

B.23. Il ressort de ce qui précède que les griefs des parties requérantes portent sur l'article 5, 4° et 5°, de la loi du 20 juillet 2022. Par ailleurs, ces griefs sont principalement pris de la violation du droit au respect de la vie privée et du droit à la protection des données à caractère personnel, garantis par l'article 22 de la Constitution, par l'article 8 de la Convention européenne des droits de l'homme, par les articles 7, 8 et 52, paragraphe 1, de la Charte, par la directive 2002/58/CE, par la directive (UE) 2016/680 et par le RGPD.

B.24.1. L'article 22 de la Constitution réserve au législateur compétent le pouvoir de fixer dans quels cas et à quelles conditions il peut être porté atteinte au droit au respect de la vie privée. Il garantit ainsi à tout citoyen qu'aucune ingérence dans l'exercice de ce droit ne peut avoir lieu qu'en vertu de règles adoptées par une assemblée délibérante, démocratiquement élue.

Une délégation à un autre pouvoir n'est toutefois pas contraire au principe de légalité, pour autant que l'habilitation soit définie de manière suffisamment précise et qu'elle porte sur l'exécution de mesures dont les éléments essentiels ont été fixés préalablement par le législateur.

Par conséquent, les éléments essentiels du traitement des données à caractère personnel doivent être fixés dans la loi, le décret ou l'ordonnance même. À cet égard, quelle que soit la matière concernée, les éléments suivants constituent, en principe, des éléments essentiels : (1°) la catégorie de données traitées, (2°) la catégorie de personnes concernées, (3°) la finalité poursuivie par le traitement, (4°) la catégorie de personnes ayant accès aux données traitées et (5°) le délai maximal de conservation des données.

B.24.2. Outre l'exigence de légalité formelle, l'article 22 de la Constitution, lu en combinaison avec l'article 8 de la Convention européenne des droits de l'homme et avec les articles 7, 8 et 52 de la Charte, impose que l'ingérence dans l'exercice du droit au respect de la vie privée et du droit à la protection des données à caractère personnel soit définie en des termes clairs et suffisamment précis qui permettent d'appréhender de manière prévisible les hypothèses dans lesquelles le législateur autorise une pareille ingérence.

En matière de protection des données, cette exigence de prévisibilité implique qu'il doit être prévu de manière suffisamment précise dans quelles circonstances les traitements de données à caractère personnel sont autorisés (CEDH, grande chambre, 4 mai 2000, *Rotaru c. Roumanie*, ECLI:CE:ECHR:2000:0504JUD002834195, § 57; grande chambre, 4 décembre 2008, S. et *Marper c. Royaume-Uni*, ECLI:CE:ECHR:2008:1204JUD003056204, § 99). L'exigence selon laquelle la limitation doit être prévue par la loi implique notamment que la base légale qui permet l'ingérence dans ces droits doit elle-même définir la portée de la limitation de l'exercice du droit concerné (CJUE, 6 octobre 2020, C-623/17, *Privacy International*, ECLI:EU:C:2020:790, point 65).

Toute personne doit dès lors pouvoir avoir une idée suffisamment claire des données traitées, des personnes concernées par un traitement de données déterminé et des conditions et finalités dudit traitement.

B.25. Il ressort des travaux préparatoires de l'article 5, 4° et 5°, de la loi du 20 juillet 2022 que celui-ci vise notamment à transposer l'article 15 de la directive 2002/58/CE, en ce que cet article 15 déroge à l'article 6, paragraphe 5, de cette directive et autorise les États membres à prendre des mesures en vue d'assurer la prévention, la recherche, la détection et la poursuite d'utilisations non autorisées du système de communications électroniques (*Doc. parl.*, Chambre, 2021-2022, DOC 55-2572/001, pp. 28, 29, 36 et 37).

Ces objectifs sont légitimes au sens de l'article 8 de la Convention européenne des droits de l'homme et de l'article 52 de la Charte.

Dans ce cadre, le législateur a précisé qu'il n'était pas possible de prévoir une conservation de données « réactive et ciblée dès le départ » en raison de la structure même des réseaux et des services concernés (*ibid.*, pp. 27-28). Il a en outre estimé que le système de conservation des données de trafic prévu à l'article 5, 4° et 5°, de la loi du 20 juillet 2022 l'est « dans l'intérêt des utilisateurs finaux des services de l'opérateur » (*ibid*., p. 26) et vise à permettre aux victimes d'une fraude ou d'une utilisation malveillante du réseau d'identifier l'auteur de celle-ci (*ibid.*, p. 28). Par ailleurs, ce système est présenté comme étant « intrinsèquement lié à la fourniture du service de communications électroniques » (*ibid*., p. 26) et comme permettant de moderniser la loi du 13 juin 2005 au regard de l'importance croissante de l'objectif de lutte contre la fraude et l'utilisation malveillante du réseau dans le droit de l'Union européenne (*ibid.*, p. 29).

B.26. Il appartient à la Cour de vérifier si l'ingérence qu'engendre l'article 122, §§ 4 et 4/1, de la loi du 13 juin 2005, tel qu'il a été inséré par l'article 5, 4° et 5°, de la loi du 20 juillet 2022, dans le droit au respect de la vie privée et dans le droit à la protection des données à caractère personnel ne produit pas des effets disproportionnés pour les personnes qui font l'objet des mesures visées dans cette disposition.

B.27.1. L'article 122, § 4, de la loi du 13 juin 2005 prévoit, à charge des opérateurs, une obligation de conservation de plusieurs données de trafic en vue de « prendre les mesures appropriées visées à l'article 121/8, § 1er, de permettre d'établir la fraude ou l'utilisation malveillante de réseau ou du service ou d'identifier son auteur et son origine », pour autant que les opérateurs traitent ces données « dans le cadre de la fourniture de ce réseau ou de ce service ».

B.27.2. Les données de trafic visées sont « l'identifiant de l'origine de la communication », « l'identifiant de la destination de la communication », les « dates et heures précises de début et de fin de la communication » et « la localisation des équipements terminaux des parties à la communication au début et à la fin de la communication » (alinéa 1er, 1°). Il est aussi prévu que les opérateurs conservent plusieurs données de trafic relatives aux communications entrantes afin d'identifier l'auteur de la communication, à savoir « le numéro de téléphone à l'origine de la communication entrante », « l'adresse IP ayant servi à l'envoi de la communication entrante, l'horodatage et le port utilisé », ainsi que « les dates et heures précises du début et de la fin de la communication entrante » (alinéa 1er, 2°).

En vertu de l'article 122, § 4, alinéa 1er, 5°, de la loi du 13 juin 2005, les opérateurs traitent les différentes données visées en vue des finalités précitées.

B.27.3. La liste des données de trafic énumérées à l'article 122, § 4, alinéa 1er, de la loi du 13 juin 2005 n'est pas exhaustive.

Tout d'abord, l'article 122, § 4, alinéa 2, énonce que, « de manière à pouvoir prendre les mesures appropriées visées à l'article 121/8, § 1er, [à] permettre d'établir la fraude ou l'utilisation malveillante du réseau ou du service ou [à] identifier son auteur et son origine, l'opérateur peut conserver et traiter d'autres données que celles visées à l'alinéa 1er considérées comme nécessaires à cette fin ». Cette faculté donnée aux opérateurs de conserver et de traiter des données autres que celles visées à l'article 122, § 4, alinéa 1er, n'est pas soumise à un avis préalable de l'IBPT ni de l'Autorité de protection des données ou à une notification à ces autorités. Les travaux préparatoires de la disposition attaquée ne fournissent aucune justification quant à cette faculté (*Doc. parl.*, Chambre, 2021-2022, DOC 55-2572/003, pp. 87-92).

Ensuite, l'article 122, § 4, alinéa 3, prévoit que « le Roi peut préciser et étendre, par arrêté délibéré en Conseil des ministres et après avis de l'[IBPT] et de l'Autorité de protection des données, les données de trafic dont la conservation doit être considérée comme nécessaire pour la poursuite des finalités prévues au présent paragraphe ». Les travaux préparatoires de la disposition attaquée justifient cette habilitation par le fait que les fraudes évoluent de manière significative dans le temps et que les données conservées peuvent différer selon le type de service de communications électroniques, la taille de l'opérateur, les outils dont celui-ci dispose et les utilisateurs du service (*Doc. parl.*, Chambre, 2021-2022, DOC 55-2572/001, p. 35).

B.27.4. Les données de trafic visées à l'article 122, § 4, alinéa 1er, 1°, de la loi du 13 juin 2005 sont en principe conservées durant quatre mois. Les données qui sont visées à l'article 122, § 4, alinéa 1er, 2°, sont en principe conservées pendant douze mois.

B.27.5. Ces délais de conservation des données peuvent être prolongés. L'article 122, § 4, alinéa 1er, 3°, de la loi du 13 juin 2005 dispose que les données visées au 1° qui sont relatives à une fraude spécifique ou à une utilisation malveillante du réseau spécifique peuvent être conservées « le temps nécessaire à son analyse et à sa résolution, le cas échéant au-delà du délai de quatre mois visé au 1° ». L'article 122, § 4, 4°, précise que les données visées au 2° qui sont relatives à une utilisation malveillante spécifique du réseau peuvent être conservées « le temps nécessaire au traitement de cette dernière, le cas échéant au-delà du délai de douze mois visé au 2° ».

B.28.1. L'article 122, § 4/1, de la loi du 13 juin 2005 prévoit quant à lui, à charge des opérateurs, la possibilité de conserver et de traiter les données de trafic « nécessaires pour assurer la sécurité et le bon fonctionnement de leurs réseaux et services de communication électroniques, et en particulier pour détecter et analyser une atteinte potentielle ou réelle à cette sécurité, en ce compris identifier l'origine de cette atteinte ». Cette faculté donnée aux opérateurs n'est pas soumise à un avis préalable de l'IBPT et de l'Autorité de protection des données ni à une notification à ces autorités.

B.28.2. Les données de trafic dont il est question à l'article 122, § 4/1, alinéa 1er, de la loi du 13 juin 2005 peuvent être conservées pour une durée d'en principe douze mois. Les données relatives à une atteinte « spécifique » à la sécurité du réseau peuvent cependant être conservées « pendant la durée nécessaire pour la traiter, le cas échéant au-delà du délai de douze mois visé à l'alinéa 2 » (article 122, § 4/1, alinéa 3).

B.29. L'article 122, § 4, de la loi du 13 juin 2005 prévoit, d'une part, une conservation généralisée et systématique des données de trafic qu'il vise et impose, d'autre part, une obligation de conservation et de traitement aux opérateurs, tout en leur laissant le soin d'identifier, parmi celles qui sont visées à l'article 122, § 4, alinéa 1er, 1° et 2°, les données qu'il y a lieu de conserver. Autrement dit, l'obligation de conservation des données ne constitue pas l'exception mais la règle dans le cadre de l'article 122, § 4, de la loi du 13 juin 2005.

Ce constat vaut d'autant plus qu'en vertu de l'article 122, § 4, alinéa 4, de la loi du 13 juin 2005, les données de trafic conservées par les opérateurs qui présentent un lien avec une fraude présumée ou avec une utilisation malveillante présumée peuvent être transférées aux autorités compétentes, notamment aux autorités judiciaires, aux services de police et aux officiers de police judiciaire de l'IBPT (*Doc. parl.*, Chambre, 2021-2022, DOC 55-2572/001, p. 35), de sorte que la conservation et le traitement de données effectués par les opérateurs sur la base de l'article 122, § 4, de la loi du 13 juin 2005 peuvent donner lieu à des poursuites pénales.

B.30.1. En ce qui concerne l'article 122, § 4/1, de la loi du 13 juin 2005, il y a lieu de relever que cette disposition ne précise pas quelles données peuvent être conservées. Par ailleurs, les données relatives à une atteinte « spécifique » à la sécurité du réseau peuvent être conservées « au-delà du délai de douze mois visé à l'alinéa 2 », sans que le libellé de l'article 122, § 4/1, de la loi du 13 juin 2005 ni les travaux préparatoires de la loi du 20 juillet 2022 précisent ce que recouvre l'hypothèse d'une atteinte spécifique.

B.30.2. À la date du prononcé du présent arrêt, la Cour de justice n'aura pas encore été amenée à statuer sur l'interprétation de l'article 15 de la directive 2002/58/CE en ce qu'il autorise les États membres à prendre des mesures de conservation de données de

communications électroniques en vue d'assurer la prévention, la recherche, la détection et la poursuite d'utilisations non autorisées du système de communications électroniques.

B.30.3. Les points de vue des parties devant la Cour divergent quant à l'interprétation à donner à l'article 15 de la directive 2002/58/CE, en ce qu'il porte sur la finalité précitée et, dans ce cadre, en ce qu'il doit ou non s'interpréter comme autorisant l'adoption de mesures nationales telles que celles qui sont prévues à l'article 5, 4° et 5°, de la loi du 20 juillet 2022.

B.31. Lorsqu'une question d'interprétation du droit de l'Union européenne est soulevée dans une affaire pendante devant une juridiction nationale dont les décisions ne sont pas susceptibles de recours en vertu du droit national, cette juridiction est tenue de poser la question à la Cour de justice, conformément à l'article 267, troisième alinéa, du Traité sur le fonctionnement de l'Union européenne.

Ce renvoi n'est toutefois pas nécessaire lorsque cette juridiction constate que la question soulevée n'est pas pertinente, que la disposition du droit de l'Union en cause a déjà fait l'objet d'une interprétation de la part de la Cour ou que l'interprétation correcte du droit de l'Union s'impose avec une telle évidence qu'elle ne laisse place à aucun doute raisonnable (CJCE, 6 octobre 1982, C-283/81, *CILFIT*, ECLI:EU:C:1982:335, point 21; CJUE, grande chambre, 6 octobre 2021, C-561/19, *Consorzio Italian Management et Catania Multiservizi SpA*, ECLI:EU:C:2021:799, point 33). À la lumière de l'article 47 de la Charte, ces motifs doivent ressortir à suffisance de la motivation de l'arrêt par lequel la juridiction refuse de poser la question préjudicielle (CJUE, grande chambre, 6 octobre 2021, C-561/19 précité, point 51).

L'exception du défaut de pertinence a pour effet que la juridiction nationale n'est pas tenue de poser une question lorsque « la question n'est pas pertinente, c'est-à-dire dans les cas où la réponse à cette question, quelle qu'elle soit, ne pourrait avoir aucune influence sur la solution du litige » (CJUE, 15 mars 2017, C-3/16, *Aquino*, ECLI:EU:C:2017:209, point 43; grande chambre, 6 octobre 2021, C-561/19 précité, point 34).

L'exception selon laquelle l'interprétation correcte du droit de l'Union s'impose avec évidence implique que la juridiction nationale doit être convaincue que la même évidence s'imposerait également aux autres juridictions de dernier ressort des autres États membres et à

la Cour de justice. Elle doit à cet égard tenir compte des caractéristiques propres au droit de l'Union, des difficultés particulières que présente l'interprétation de ce dernier et du risque de divergences de jurisprudence au sein de l'Union. Elle doit également tenir compte des différences entre les versions linguistiques de la disposition concernée dont elle a connaissance, notamment lorsque ces divergences sont exposées par les parties et sont avérées. Enfin, elle doit également avoir égard à la terminologie propre à l'Union et aux notions autonomes dans le droit de l'Union, ainsi qu'au contexte de la disposition applicable à la lumière de l'ensemble des dispositions du droit de l'Union, de ses finalités et de l'état de son évolution à la date à laquelle l'application de la disposition en cause doit être faite (CJUE, grande chambre, 6 octobre 2021, C-561/19 précité, points 40-46).

Pour le surplus, une juridiction nationale statuant en dernier ressort peut s'abstenir de soumettre une question préjudicielle à la Cour de justice « pour des motifs d'irrecevabilité propres à la procédure devant cette juridiction, sous réserve du respect des principes d'équivalence et d'effectivité » (CJCE, 14 décembre 1995, C-430/93 et C-431/93, *Van Schijndel et Van Veen,* ECLI:EU:C:1995:441, point 17; CJUE, 15 mars 2017, C-3/16 précité, point 56; grande chambre, 6 octobre 2021, C-561/19 précité, point 61).

B.32. Dès lors que l'affaire présentement examinée soulève un doute sur l'interprétation de l'article 15 de la directive 2002/58/CE, il convient de poser à la Cour de justice la première question préjudicielle formulée dans le dispositif.

4. La conservation des données de localisation (article 6)

B.33.1. Les premier et deuxième moyens dans l'affaire n° 7930 ainsi que la deuxième branche du premier moyen et la première branche du troisième moyen dans l'affaire n° 7932 portent sur l'article 6 de la loi du 20 juillet 2022, qui modifie l'article 123 de la loi du 13 juin 2005 comme suit :

« 1° le paragraphe 1er est remplacé par ce qui suit :

' Art. 123. § 1er. Sans préjudice de l'application du RGPD et de la loi du 30 juillet 2018, les opérateurs de réseaux mobiles ne peuvent conserver et traiter de données de localisation

autres que les données relatives au trafic se rapportant à un abonné ou un utilisateur final que dans les cas suivants :

1° lorsque cela est nécessaire pour le bon fonctionnement et la sécurité du réseau ou du service, les données étant conservées maximum douze mois à partir de la date de la communication, sauf en cas d'atteinte spécifique à la sécurité du réseau nécessitant de prolonger la conservation des données concernées au-delà de ce délai;

2° lorsque cela est nécessaire pour détecter ou analyser les fraudes ou l'utilisation malveillante du réseau, les données étant conservées maximum quatre mois à partir de la date de la communication, sauf en cas de fraude ou d'utilisation malveillante spécifique nécessitant de prolonger la conservation des données concernées au-delà de ce délai;

3° lorsque les données ont été rendues anonymes;

4° lorsque le traitement s'inscrit dans le cadre de la fourniture d'un service qui fait usage de données de trafic ou de localisation;

5° lorsque le traitement est nécessaire pour répondre à une obligation imposée par une norme législative formelle. ';

2° dans le paragraphe 2, dans le 2°, les mots ' la manifestation de volonté libre, spécifique et basée sur des informations par laquelle l'intéressé ou son représentant légal accepte que des données de localisation se rapportant à lui soient traitées ' sont remplacés par les mots ' le consentement au sens de l'article 4, 11), du RGPD ';

3° dans le paragraphe 4, l'alinéa 1er est remplacé par ce qui suit :

' Les données visées au présent article ne peuvent être traitées que par des personnes qui travaillent sous l'autorité de l'opérateur ou du tiers qui fournit le service qui fait usage de données de trafic ou de localisation, ou par la Cellule de coordination de l'opérateur visée à l'article 127/3. ' ».

B.33.2. Du fait de la modification visée ci-dessus, l'article 123 de la loi du 13 juin 2005 dispose désormais :

« § 1er. Sans préjudice de l'application du RGPD et de la loi du 30 juillet 2018, les opérateurs de réseaux mobiles ne peuvent conserver et traiter de données de localisation autres que les données relatives au trafic se rapportant à un abonné ou un utilisateur final que dans les cas suivants :

1° lorsque cela est nécessaire pour le bon fonctionnement et la sécurité du réseau ou du service, les données étant conservées maximum douze mois à partir de la date de la communication, sauf en cas d'atteinte spécifique à la sécurité du réseau nécessitant de prolonger la conservation des données concernées au-delà de ce délai;

2° lorsque cela est nécessaire pour détecter ou analyser les fraudes ou l'utilisation malveillante du réseau, les données étant conservées maximum quatre mois à partir de la date de la communication, sauf en cas de fraude ou d'utilisation malveillante spécifique nécessitant de prolonger la conservation des données concernées au-delà de ce délai;

3° lorsque les données ont été rendues anonymes;

4° lorsque le traitement s'inscrit dans le cadre de la fourniture d'un service qui fait usage de données de trafic ou de localisation;

5° lorsque le traitement est nécessaire pour répondre à une obligation imposée par une norme législative formelle.

§ 2. Le traitement dans le cadre de la fourniture d'un service à données de trafic ou de localisation est soumis aux conditions suivantes :

1° L'opérateur informe l'abonné ou, le cas échéant, l'utilisateur final auquel se rapportent les données, avant d'obtenir le consentement de celui-ci pour le traitement :

a) des types de données de localisation traités;

b) des objectifs précis du traitement;

c) de la durée du traitement;

d) des tiers éventuels auxquels ces données seront transmises;

e) de la possibilité de retirer à tout moment, définitivement ou temporairement, le consentement donné pour le traitement.

2° L'abonné ou, le cas échéant, l'utilisateur final, a préalablement au traitement, donné son consentement pour le traitement.

Par consentement pour le traitement au sens du présent article, on entend le consentement au sens de l'article 4, 11), du RGPD.

3° Le traitement des données en question se limite aux actes et à la durée nécessaires pour fournir le service à données de trafic ou de localisation en question.

4° L'opérateur concerné offre gratuitement à ses abonnés ou à ses utilisateurs finaux la possibilité de retirer le consentement donné, facilement et à tout moment, définitivement ou temporairement.

§ 4. Les données visées au présent article ne peuvent être traitées que par des personnes qui travaillent sous l'autorité de l'opérateur ou du tiers qui fournit le service qui fait usage de données de trafic ou de localisation, ou par la Cellule de coordination de l'opérateur visée à l'article 127/3.

Le traitement est limité à ce qui est strictement nécessaire pour pouvoir fournir au service concerné les données de trafic ou de localisation.

§ 5. En cas de communication d'urgence aux centrales de gestion des services d'urgence offrant de l'aide sur place, les opérateurs annulent, pour autant que cela soit techniquement possible, en vue de permettre le traitement de la communication d'urgence par les centrales de gestion concernées, le refus temporaire ou l'absence de consentement de l'abonné ou de l'utilisateur final concernant le traitement de données de localisation par ligne distincte.

Cette annulation est gratuite ».

B.33.3.1. La partie requérante dans l'affaire n° 7930 prend les premier et deuxième moyens de la violation des articles 11, 12, 22 et 29 de la Constitution, de l'article 15, paragraphe 1, et des articles 5, 6 et 9 de la directive 2002/58/CE, lus à la lumière des articles 7, 8, 11, 47 et 52, paragraphe 1, de la Charte, des articles 6, 8, 10, 11 et 18 de la Convention européenne des droits de l'homme et des articles 13 et 54 de la directive (UE) 2016/680, en ce que l'article 6 de la loi du 20 juillet 2022 instaure une obligation généralisée de conservation des données de communication, sans que cette conservation s'avère nécessaire et strictement limitée au regard du but poursuivi.

B.33.3.2. Les parties requérantes dans l'affaire n° 7932 prennent un premier moyen de la violation des articles 10, 11, 13, 15, 22, 23 et 29 de la Constitution, lus en combinaison ou non avec les articles 5, 6, 8, 9, 10, 11, 14 et 18 de la Convention européenne des droits de l'homme, avec les articles 7, 8, 11, 47 et 52 de la Charte, avec l'article 5, paragraphe 4, du Traité sur l'Union européenne ainsi qu'avec l'article 6 de la directive 2002/58/CE, avec la directive (UE) 2016/680 et avec le RGPD. Dans une deuxième branche, elles allèguent que l'article 6 de la loi du 20 juillet 2022 autorise la conservation pendant douze mois des données qu'il vise afin d'assurer le bon fonctionnement et la sécurité du réseau, alors que l'article 9 de la directive 2002/58/CE exclut un tel traitement.

Les parties requérantes prennent un troisième moyen de la violation des articles 10, 11, 15, 22 et 29 de la Constitution, lus en combinaison ou non avec les articles 5, 6, 8, 9, 10, 11, 14 et 18 de la Convention européenne des droits de l'homme, avec les articles 7, 8, 11, 47 et 52 de la Charte, avec l'article 5, paragraphe 4, du Traité sur l'Union européenne ainsi qu'avec la directive 2002/58/CE, avec la directive (UE) 2016/680 et avec le RGPD. Dans une première branche, elles soutiennent que l'article 6 de la loi du 20 juillet 2022 crée une obligation de

conservation généralisée et indifférenciée des données au profit des opérateurs agissant dans le cadre de leurs missions, ce qui est trop vague et trop large.

B.34. Il ressort de ce qui précède que les griefs des parties requérantes portent sur l'article 123, § 1er, de la loi du 13 juin 2005, tel qu'il a été remplacé par l'article 6, 1°, de la loi du 20 juillet 2022. Ces griefs sont principalement pris de la violation du droit au respect de la vie privée et du droit à la protection des données à caractère personnel, garantis par l'article 22 de la Constitution, par l'article 8 de la Convention européenne des droits de l'homme, par les articles 7, 8 et 52, paragraphe 1, de la Charte, par la directive 2002/58/CE, par la directive (UE) 2016/680 et par le RGPD.

B.35.1. Il ressort des travaux préparatoires de l'article 6, 1°, de la loi du 20 juillet 2022 que celui-ci vise à transposer l'article 9 de la directive 2002/58/CE (*Doc. parl.*, Chambre, 2021-2022, DOC 55-2572/001, pp. 39-40), qui dispose :

« Données de localisation autres que les données relatives au trafic

1. Lorsque des données de localisation, autres que des données relatives au trafic, concernant des utilisateurs ou abonnés de réseaux publics de communications ou de services de communications électroniques accessibles au public ou des abonnés à ces réseaux ou services, peuvent être traitées, elles ne le seront qu'après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés, dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée. Le fournisseur du service doit informer les utilisateurs ou les abonnés, avant d'obtenir leur consentement, du type de données de localisation autres que les données relatives au trafic qui sera traité, des objectifs et de la durée de ce traitement, et du fait que les données seront ou non transmises à un tiers en vue de la fourniture du service à valeur ajoutée. Les utilisateurs ou les abonnés ont la possibilité de retirer à tout moment leur consentement pour le traitement des données de localisation autres que les données relatives au trafic.

2. Lorsque les utilisateurs ou les abonnés ont donné leur consentement au traitement des données de localisation autres que les données relatives au trafic, ils doivent garder la possibilité d'interdire temporairement, par un moyen simple et gratuit, le traitement de ces données pour chaque connexion au réseau ou pour chaque transmission de communication.

3. Le traitement des données de localisation autres que les données relatives au trafic effectué conformément aux paragraphes 1 et 2 doit être restreint aux personnes agissant sous l'autorité du fournisseur du réseau public de communications ou service de communications électroniques accessible au public ou du tiers qui fournit le service à valeur ajoutée, et doit se limiter à ce qui est nécessaire pour assurer la fourniture du service à valeur ajoutée ».

B.35.2. En ce que l'article 123, § 1er, de la loi du 13 juin 2005 prévoit la conservation des données de localisation autres que les données de trafic se rapportant à un abonné ou à un utilisateur final lorsque les données ont été rendues anonymes (3°) et lorsque le traitement s'inscrit dans le cadre de la fourniture d'un service qui fait usage de données de trafic ou de localisation (4°) – à condition que, dans ce dernier cas, l'abonné ou l'utilisateur final ait préalablement donné son consentement en vertu de l'article 123, § 2 –, cette disposition s'inscrit dans les cas visés à l'article 9, paragraphe 1, de la directive 2002/58/CE.

B.35.3. L'article 123, § 1er, de la loi du 13 juin 2005, en revanche, vise également d'autres hypothèses de conservation des données de localisation, autres que les données de trafic, que celles qui sont autorisées par l'article 9 de la directive 2002/58/CE, comme la section de législation du Conseil d'État et l'Autorité de protection des données l'ont relevé dans leurs avis sur l'avant-projet de loi à l'origine de la loi du 20 juillet 2022 (*ibid.*, pp. 306-308 et 677-678).

En ce qui concerne ces autres hypothèses, il y a lieu de se référer à l'article 15, paragraphe 1, de la directive 2002/58/CE, qui permet de limiter la portée des droits prévus notamment en son article 9, « 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'État - la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques ».

B.36. Les griefs des parties requérantes portent plus particulièrement sur les hypothèses de conservation des données de localisation, autres que les données de trafic, qui relèvent du régime de limitation prévu à l'article 15, paragraphe 1, de la directive 2002/58/CE et qui sont visées à l'article 123, § 1er, 1°, 2° et 5°, de la loi du 13 juin 2005, tel qu'il a été remplacé par l'article 6 de la loi du 20 juillet 2022.

B.37.1. L'article 123, § 1er, de la loi du 13 juin 2005 prévoit que les opérateurs de réseaux mobiles ne peuvent conserver et traiter les données de localisation précitées se rapportant à un abonné ou à un utilisateur final que « lorsque cela est nécessaire pour le bon fonctionnement et

la sécurité du réseau ou du service » (1°) et « lorsque cela est nécessaire pour détecter ou analyser les fraudes ou l'utilisation malveillante du réseau » (2°).

Les données visées à l'article 123, § 1er, 1°, de la loi du 13 juin 2005 sont en principe conservées pendant douze mois à partir de la date de la communication. Celles qui sont visées à l'article 123, § 1er, 2°, de la loi du 13 juin 2005 sont en principe conservées pendant quatre mois.

B.37.2. Les hypothèses visées à l'article 123, § 1er, 1° et 2°, de la loi du 13 juin 2005 permettent de garantir la prévention, la recherche, la détection et la poursuite d'utilisations non autorisées du système de communications électroniques au sens de l'article 15, paragraphe 1, de la directive 2002/58/CE.

B.38. Il appartient à la Cour de vérifier si l'ingérence qu'engendre l'article 123, § 1er, 1° et 2°, de la loi du 13 juin 2005, tel qu'il a été remplacé par l'article 6, 1°, de la loi du 20 juillet 2022, dans le droit au respect de la vie privée et dans le droit à la protection des données à caractère personnel est nécessaire, raisonnable et proportionnée au sein d'une société démocratique en vue de prévenir les utilisations non autorisées du système de communications électroniques.

B.39.1. Les opérateurs déterminent les données de localisation autres que les données relatives au trafic qui peuvent être conservées et traitées. Ils apprécient également, dans chaque cas, la nécessité de cette conservation et de ce traitement.

Par ailleurs, en ce qui concerne le délai de conservation des données citées visées à l'article 123, § 1er, 1° et 2°, de la loi du 13 juin 2005, il est prévu que la durée de douze mois précitée peut être prolongée « en cas d'atteinte spécifique à la sécurité du réseau nécessitant de prolonger la conservation des données concernées au-delà de ce délai » et que la durée de quatre mois précitée peut être prolongée « en cas de fraude ou d'utilisation malveillante spécifique nécessitant de prolonger la conservation des données concernées au-delà de ce délai ».

B.39.2. L’article 123, § 1er, 1° et 2°, de la loi du 13 juin 2005 laisse aux opérateurs le soin d’identifier, parmi les données de localisation, les données qu’il est nécessaire de conserver et de traiter, et de prolonger le délai de conservation des données concernées en cas d’atteinte spécifique à la sécurité du réseau, d’une part, et en cas de fraude ou d’utilisation malveillante spécifique, d’autre part.

B.39.3. Pour les mêmes motifs que ceux qui sont énoncés en B.30 et B.31, dès lors que l’affaire présentement examinée soulève un doute quant à l’interprétation de l’article 15, paragraphe 1, de la directive 2002/58/CE, il convient de poser à la Cour de justice la deuxième question préjudicielle formulée dans le dispositif.

Par ailleurs, il y a lieu de poser la troisième question préjudicielle mentionnée dans le dispositif.

B.40.1. Enfin, l’article 123, § 1er, 5°, de la loi du 13 juin 2005 autorise la conservation des données de localisation, autres que les données de trafic, se rapportant à un abonné ou à un utilisateur final, « lorsque le traitement est nécessaire pour répondre à une obligation imposée par une norme législative formelle ».

Dans cette hypothèse, les griefs des parties requérantes ne sauraient, en soi, être imputés à l’article 123 de la loi du 13 juin 2005, mais, le cas échéant, aux obligations imposées par une norme législative formelle auxquelles il est fait référence.

B.40.2. Les premier et deuxième moyens dans l’affaire n° 7930 ainsi que le premier moyen, en sa deuxième branche, et le troisième moyen, en sa première branche, dans l’affaire n° 7932, relatifs à l’article 123, § 1er, 5°, de la loi du 13 juin 2005, ne sont pas fondés en ce qu’ils sont pris de la violation des dispositions citées en B.34. L’examen au regard des autres normes de référence, citées en B.33.3.1 et B.33.3.2, à supposer que la violation de celles-ci soit valablement invoquée par les parties requérantes, ne saurait, en toute hypothèse, mener à une autre conclusion.

5. La conservation des données de souscription et d'identification (article 8)

B.41.1. Les premier et deuxième moyens dans l'affaire n° 7930, le moyen unique dans l'affaire n° 7931 ainsi que les première, deuxième et cinquième branches du deuxième moyen dans l'affaire n° 7932 portent sur l'article 8 de la loi du 20 juillet 2022, qui dispose :

« L'article 126 de la [loi du 13 juin 2005], remplacé par l'article 5 de la loi du 30 juillet 2013, annulé lui-même par l'arrêt n° 84/2015 de la Cour constitutionnelle, et par l'article 4 de la loi du 29 mai 2016, annulé lui-même par l'arrêt n° 57/2021 de la Cour constitutionnelle, est remplacé par ce qui suit :

' Art. 126. § 1er. Sans préjudice du RGPD et de la loi du 30 juillet 2018, les opérateurs qui offrent aux utilisateurs finaux des services de communications électroniques, ainsi que les opérateurs fournissant les réseaux de communications électroniques sous-jacents qui permettent la fourniture de ces services, conservent les données suivantes, pour autant qu'ils les traitent ou les génèrent dans le cadre de la fourniture de ces réseaux ou services :

1° le numéro de Registre national ou un numéro équivalent, le nom et le prénom de l'utilisateur final qui est une personne physique ou la dénomination de l'abonné qui est une personne morale;

2° l'alias éventuel choisi par l'utilisateur final lors de la souscription au service ou de l'activation du service;

3° les coordonnées de l'abonné qui ont été fournies lors de la souscription au service, notamment son numéro de téléphone, son adresse e-mail et son adresse postale;

4° la date et l'heure de la souscription au service et de l'activation du service et les éléments permettant de déterminer le lieu à partir duquel cette souscription et cette activation ont été effectuées, à savoir notamment :

- l'adresse physique du point de vente où la souscription ou l'activation ont eu lieu, ou;

- l'adresse physique du point de terminaison du réseau ayant servi à la souscription ou à l'activation, ou;

- l'adresse IP ayant servi à la souscription ou à l'activation ainsi que le port source de la connexion et l'horodatage, ou;

- dans le cadre d'un réseau téléphonique mobile, la localisation géographique de l'équipement terminal qui a permis la souscription ou l'activation au moyen d'un numéro de téléphone;

5° l'adresse physique de livraison du service;

6° l'adresse de facturation du service et les données relatives au type et au moyen de paiement, à la date des paiements, et la référence de l'opération de paiement en cas de paiement en ligne;

7° le service principal et les services annexes que l'abonné peut utiliser;

8° la date à partir de laquelle ces services peuvent être utilisés, la date de la première utilisation de ces services et la date de fin de ces services;

9° en cas de transfert de l'identifiant de l'abonné, tel son numéro de téléphone, l'identité de l'opérateur qui transfère l'identifiant et l'identité de l'opérateur auquel l'identifiant est transféré et la date à laquelle le transfert est effectué;

10° le numéro de téléphone attribué;

11° l'adresse de messagerie principale et les adresses de messagerie employées comme alias;

12° l'identité internationale d'abonné mobile, " International Mobile Subscriber Identity ", en abrégé " IMSI ";

13° l'identifiant permanent d'abonnement, " Subscription Permanent Identifier ", en abrégé " SUPI ";

14° l'identifiant caché d'abonnement, " Subscription Concealed Identifier ", en abrégé " SUCI ";

15° l'adresse IP à la source de la connexion, l'horodatage de l'attribution ainsi que, en cas d'utilisation partagée d'une adresse IP de l'utilisateur final, les ports qui lui ont été attribués;

16° l'identifiant de l'équipement terminal de l'utilisateur final, ou lorsque l'opérateur ne le traite pas ou ne le génère pas, l'identifiant de l'équipement qui est le plus proche de cet équipement terminal, à savoir notamment :

- l'identité internationale d'équipement mobile, " International Mobile Equipment Identity ", en abrégé " IMEI ";

- l'identifiant permanent de l'équipement, " Permanent Equipment Identifier ", en abrégé " PEI ";

- l'adresse du contrôleur d'accès au réseau, " Media Access Control address ", en abrégé " MAC ";

17° les autres identifiants relatifs à l'utilisateur final, à l'équipement terminal ou à l'équipement le plus proche de cet équipement terminal, qui résultent de l'évolution technologique et qui sont déterminés par le Roi, pour autant que cet arrêté soit confirmé par la loi dans les six mois suivant la publication de cet arrêté.

Les opérateurs ne doivent pas conserver les adresses MAC visées à l'alinéa 1er, 16°, troisième tiret, pour les services de communications électroniques qu'ils offrent uniquement à des entreprises ou à des personnes morales.

L'arrêté royal visé à l'alinéa 1er, 17°, ne porte pas sur le contenu des communications électroniques, ni sur des métadonnées de communications électroniques qui donnent des informations sur le destinataire de la communication, comme l'adresse IP du destinataire de la communication, ou sur la localisation de l'équipement terminal.

Le Roi :

1° peut préciser les données visées à l'alinéa 1er;

2° fixe les exigences en matière de précision et de fiabilité auxquelles ces données doivent répondre.

§ 2. Les opérateurs conservent les données visées au paragraphe 1er, alinéa 1er, 1° à 14°, aussi longtemps que le service de communications électroniques est utilisé ainsi que douze mois après la fin du service.

Les opérateurs conservent les données visées au paragraphe 1er, alinéa 1er, 15° et 16°, pour une durée de douze mois après la fin de la session.

Par dérogation à l'alinéa 2, la durée de conservation des données visées au paragraphe 1er, alinéa 1er, 16°, troisième tiret, est réduite à six mois après la fin de la session lorsque l'opérateur conserve une autre donnée visée au paragraphe 1er, alinéa 1er, 16°.

Les opérateurs conservent les données visées au paragraphe 1er, alinéa 1er, 17°, pour la durée fixée par le Roi. Cette durée ne peut pas être plus longue que la durée de conservation visée à l'alinéa 1er.

L'arrêté royal visé au paragraphe 1er, alinéa 1er, 17°, et alinéa 4 et au paragraphe 2, alinéa 4, est proposé par le ministre de la Justice, le ministre de l'Intérieur, le ministre de la Défense et le ministre, fait l'objet d'un avis de l'Autorité de protection des données et de l'Institut et est délibéré en Conseil des ministres. ' ».

B.41.2.1. La partie requérante dans l'affaire n° 7930 prend les premier et deuxième moyens de la violation des articles 11, 12, 22 et 29 de la Constitution, de l'article 15, paragraphe 1, et des articles 5, 6 et 9 de la directive 2002/58/CE, lus à la lumière des articles 7, 8, 11, 47 et 52, paragraphe 1, de la Charte, des articles 6, 8, 10, 11 et 18 de la Convention européenne des droits de l'homme et des articles 13 et 54 de la directive (UE) 2016/680, en ce que l'article 8 de la loi du 20 juillet 2022 instaure une obligation généralisée de conservation des données de communication, sans que cette conservation s'avère nécessaire et strictement limitée au regard du but poursuivi.

B.41.2.2. La partie requérante dans l'affaire n° 7931 prend un moyen unique de la violation des articles 11, 12, 22 et 29 de la Constitution, lus en combinaison ou non avec les articles 7, 8, 11, 47 et 52, paragraphe 1, de la Charte, avec l'article 8 de la Convention européenne des droits de l'homme, avec les articles 5, 6 et 15 de la directive 2002/58/CE et avec les articles 13 et 54 de la directive (UE) 2016/680. Elle soutient que l'article 8 de la loi du 20 juillet 2022 prévoit une obligation de conservation systématique et indifférenciée des données d'identification qui n'est pas nécessaire au regard de l'objectif poursuivi. À titre subsidiaire, la partie requérante demande de poser une question préjudicielle à la Cour de justice.

B.41.2.3. Les parties requérantes dans l'affaire n° 7932 prennent un deuxième moyen de la violation des articles 10, 11, 15, 22 et 29 de la Constitution, lus en combinaison ou non avec les articles 5, 6, 8, 9, 10, 11, 14 et 18 de la Convention européenne des droits de l'homme, avec les articles 7, 8, 11, 47 et 52 de la Charte, avec l'article 5, paragraphe 4, du Traité sur l'Union européenne, avec la directive 2002/58/CE, avec la directive (UE) 2016/680 et avec le RGPD. Dans les première et troisième branches, elles soutiennent que l'article 8 de la loi du 20 juillet 2022 prévoit une conservation de données qui n'est pas nécessaire ainsi qu'un délai de conservation trop long, de sorte qu'il n'est pas compatible avec le droit au respect de la vie privée ni avec l'article 5, § 1er, *c)* et *d),* du RGPD. Dans une deuxième branche, elles allèguent qu'en tant que l'article 8 de la loi du 20 juillet 2022 s'applique aux services de communication électroniques « *over the top* » (ci-après : les services OTT), tels que « WhatsApp » et « Skype », il engendre une identité de traitement qui est contraire au principe d'égalité et de non-discrimination et au principe de légalité.

B.42. Les premier et deuxième moyens dans l'affaire n° 7930, le moyen unique dans l'affaire n° 7931, ainsi que la première et la troisième branches du deuxième moyen dans l'affaire n° 7932 sont principalement pris de la violation du droit au respect de la vie privée et du droit à la protection des données à caractère personnel, garantis par l'article 22 de la Constitution, par l'article 8 de la Convention européenne des droits de l'homme, par les articles 7, 8 et 52, paragraphe 1, de la Charte, par la directive 2002/58/CE, par la directive (UE) 2016/680 et par le RGPD.

B.43.1. Il ressort des travaux préparatoires de l'article 8 de la loi du 20 juillet 2022 que, par cette disposition, le législateur a entendu réagir à l'arrêt de la Cour n° 158/2021 en énumérant lui-même les différentes données d'identification qu'il y a lieu de conserver (*Doc. parl.*, Chambre, 2021-2022, DOC 55-2572/002, pp. 5-7).

B.43.2. En outre, il ressort de ces travaux préparatoires que le législateur a également souhaité instaurer, pour les opérateurs visés à l'article 126, § 1er, alinéa 1er, l'obligation de conserver les données d'identification précitées (*ibid.*, pp. 7-10).

À cet égard, l'Autorité de protection des données a relevé, dans son avis sur l'amendement qui est à l'origine de l'article 8 de la loi du 20 juillet 2022 :

« 23. En transposant le Code de communications électroniques européen (ci-après : ' CCEE ') dans la loi télécom, le législateur a redéfinit, entre autres, les notions d'' opérateur ' et de ' services de communications électroniques ', qui sont utilisées pour déterminer le champ d'application personnel des obligations imposées aux opérateurs de conserver les données de trafic et de localisation des abonnés et de l'obligation d'identification des abonnés et des utilisateurs finaux des services de communications électroniques. Comme l'Autorité l'a déjà soulevé dans son avis n° 108/2021, ces nouvelles définitions aboutissent à étendre considérablement le champ d'application des obligations de conservation des données et d'identification des abonnés et utilisateurs finaux. Avec la transposition du CCE dans la loi télécom, les entreprises qui fournissent des services de communications électroniques ' over-the-top ', à l'instar de services de téléphonie par Internet (*Voice over IP*), de services de messageries (p.ex. : WhatsApp, Signal, Telegram, Facebook Messenger), ou encore de services de courrier électroniques en ligne (p.ex. : Gmail ou Hotmail) sont soumises à des obligations de conservation de données et doivent procéder à l'identification de leurs abonnés ou utilisateurs finaux. De même, les entreprises qui fournissent des ' services consistant entièrement ou principalement en la transmission de signaux, tels que les services de transmission utilisés pour la fourniture de services de machine à machine ' – il s'agit de services portant sur l'internet des objets – doivent, à présent, être considérées comme des opérateurs soumis à des obligations de conservation des données et à l'obligation d'identifier leurs abonnés et utilisateurs finaux.

24. Ainsi, les nouvelles définitions des notions d' ' opérateur ' et de ' services de communications électroniques ', couplées, notamment, à l'obligation d'identification imposée par les nouveaux articles 126 et 127 de la loi télécom (introduits par les amendements n° 1 et 6), aboutissent à rendre impossible – ou en tout cas très difficile – toute correspondance anonyme sur Internet. En outre, pour les services de messagerie ' OTT ' (comme Signal ou WhatsApp), l'Autorité relève que la collecte et la conservation des adresses IP attribuées à la source de la connexion permet, non seulement d'identifier de manière indirecte l'utilisateur, mais également (potentiellement) de le localiser. En effet, il est souvent possible de localiser un équipement terminal (et donc la personne qui l'utilise) à partir de l'adresse IP qui lui a été attribuée. La collecte systématique des adresses IP attribuées à la source de la connexion et leur horodatage permettent ainsi potentiellement de suivre les déplacements des utilisateurs de ces services; ce

qui constitue une ingérence particulièrement importante dans le droit au respect de la vie privée de ces utilisateurs.

25. Ceci constitue un changement de paradigme par rapport au paradigme de, et aux règles de confidentialité imposées par, la directive ePrivacy. L'Autorité insiste sur la nécessité de tenir un débat parlementaire approfondi sur les implications de ce changement, notamment, au regard du droit à la vie privée et du droit à la liberté d'expression. En tout état de cause, l'Autorité rappelle que toute ingérence dans les droits et libertés des personnes concernées n'est admissible que si elle s'avère nécessaire et proportionnée à l'objectif d'intérêt général poursuivi » (Autorité de protection des données, avis n° 66/2022 du 1er avril 2022, points 23 à 25).

B.44.1. Dans le dispositif de l'arrêt du 6 octobre 2020 en cause de La *Quadrature du Net e.a.,* la Cour de justice a dit pour droit 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, ne s'oppose pas, notamment, à des mesures législatives « prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire », d'une part, et « prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité et de la sauvegarde de la sécurité publique, une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques », d'autre part.

B.44.2. Comme la section de législation du Conseil d'État l'a observé dans son avis sur l'avant-projet de loi qui est à l'origine de la loi du 20 juillet 2022, la Cour de justice opère donc une distinction entre, d'une part, la conservation généralisée et indifférenciée des adresses IP attribuées à une source de connexion, qui peut être imposée aux opérateurs aux seules fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, et ce, pour une période temporellement limitée au strict nécessaire, et, d'autre part, la conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques, qui peut être imposée aux opérateurs à des fins plus larges, à savoir la sauvegarde de la sécurité nationale, la lutte contre la criminalité, que celle-ci soit grave ou non, et la sauvegarde de la sécurité publique, même lorsque cette sécurité ne fait pas l'objet de menaces graves, et ce, sans

que ces données doivent être conservées pour une période limitée au strict nécessaire (*Doc. parl.*, Chambre, 2021-2022, DOC 55-2572/001, p. 296).

B.44.3. Par ailleurs, la Cour de justice estime que les adresses IP attribuées à la source de connexion doivent faire l'objet d'un régime particulier, dès lors que celles-ci « [peuvent] être utilisées pour effectuer notamment le traçage exhaustif du parcours de navigation d'un internaute et, par suite, de son activité en ligne, ces données permettent d'établir le profil détaillé de ce dernier. Ainsi, la conservation et l'analyse de ces adresses IP que nécessite un tel traçage constituent des ingérences graves dans les droits fondamentaux de l'internaute consacrés par les articles 7 et 8 de la Charte » (CJUE, arrêt du 6 octobre 2020 précité, C-511/18, C-512/18 et C-520/18, point 153).

B.45. Par l'arrêt du 30 avril 2024 en cause de *La Quadrature du Net e.a.* rendu en assemblée plénière *(Données personnelles et lutte contre la contrefaçon)* (C-470/21, ECLI:EU:C:2024:370), la Cour de justice a précisé cela en ces termes :

« 75. [...] [I]l y a lieu de relever que, selon la jurisprudence de la Cour, si [...] les adresses IP constituent des données relatives au trafic aux fins de la directive 2002/58, ces adresses se distinguent des autres catégories de données relatives au trafic ainsi que des données de localisation.

76. À cet égard, la Cour a relevé que les adresses IP sont générées sans être rattachées à une communication déterminée et servent principalement à identifier, par l'intermédiaire des fournisseurs de services de communications électroniques, le propriétaire d'un équipement terminal à partir duquel une communication au moyen d'Internet est effectuée. Ainsi, en matière de courrier électronique et de téléphonie par Internet, pour autant que seules les adresses IP de la source de la communication sont conservées et non celles du destinataire de celle-ci, ces adresses ne révèlent, en tant que telles, aucune information sur les tierces personnes ayant été en contact avec la personne à l'origine de la communication. Dans cette mesure, cette catégorie de données présente un degré de sensibilité moindre que les autres données relatives au trafic (voir, en ce sens, arrêt du 6 octobre 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 152).

77. Certes, au point 156 de l'arrêt du 6 octobre 2020, *La Quadrature du Net e.a.* (C-511/18, C-512/18 et C-520/18, EU:C:2020:791), la Cour a jugé que, en dépit du constat d'une moindre sensibilité des adresses IP lorsqu'elles servent exclusivement à identifier l'utilisateur d'un service de communications électroniques, l'article 15, paragraphe 1, de la directive 2002/58 s'oppose à ce qu'une conservation généralisée et indifférenciée des seules adresses IP attribuées à la source d'une connexion soit effectuée pour des objectifs autres que la lutte contre la criminalité grave, la prévention des menaces graves contre la sécurité publique ou la sauvegarde de la sécurité nationale. Toutefois, la Cour s'est expressément fondée, pour parvenir à cette conclusion, sur le caractère grave de l'ingérence dans les droits fondamentaux

consacrés aux articles 7, 8 et 11 de la Charte qu'est susceptible de comporter une telle conservation des adresses IP.

78. En effet, la Cour a considéré, au point 153 du même arrêt, que, dans la mesure où les adresses IP peuvent, notamment, lorsqu'elles sont utilisées pour effectuer le ' traçage exhaustif du parcours de navigation d'un internaute ' et, par suite, de son activité en ligne, permettre d'établir le « profil détaillé » de ce dernier, la conservation et l'analyse desdites adresses IP que nécessite un tel traçage constituent des ingérences graves dans les droits fondamentaux de la personne concernée consacrés aux articles 7 et 8 de la Charte, pouvant également avoir des effets dissuasifs sur l'exercice par les utilisateurs des moyens de communications électroniques de leur liberté d'expression garantie à l'article 11 de la Charte.

79. Toutefois, il y a lieu de souligner que toute conservation généralisée et indifférenciée d'un ensemble, le cas échéant vaste, d'adresses IP statiques et dynamiques utilisées par une personne dans une période donnée ne constitue pas nécessairement une ingérence grave dans les droits fondamentaux garantis aux articles 7, 8 et 11 de la Charte.

80. À cet égard, tout d'abord, les affaires ayant donné lieu à l'arrêt du 6 octobre 2020, *La Quadrature du Net e.a.* (C-511/18, C-512/18 et C-520/18, EU:C:2020:791), portaient sur des réglementations nationales qui impliquaient une obligation de conservation d'un ensemble de données nécessaires pour déterminer la date, l'heure, la durée et le type de la communication, identifier le matériel de communication utilisé ainsi que localiser les équipements terminaux et les communications, données au nombre desquelles figuraient, notamment, le nom et l'adresse de l' utilisateur, les numéros de téléphone de l'appelant et de l'appelé ainsi que l'adresse IP pour les services Internet. De surcroît, dans deux de ces affaires, les réglementations nationales en cause semblaient couvrir également les données relatives à l'acheminement des communications électroniques par les réseaux, celles-ci permettant également d'identifier la nature des informations consultées en ligne (voir, en ce sens, arrêt du 6 octobre 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 et C-520/18, EU:C:2020:791, points 82 et 83).

81. La conservation des adresses IP opérée dans le cadre de telles réglementations nationales était donc de nature, au regard des autres données dont ces réglementations imposaient la conservation et de la possibilité de combiner ces différentes données, à permettre de tirer des conclusions précises sur la vie privée des personnes dont les données étaient concernées et, partant, de conduire à une ingérence grave dans les droits fondamentaux, consacrés aux articles 7 et 8 de la Charte, relatifs à la protection de la vie privée et des données à caractère personnel de ces personnes, ainsi qu'à l'article 11 de cette charte, relatif à la liberté d'expression de celles-ci.

82. En revanche, l'obligation faite aux fournisseurs de services de communications électroniques, par une mesure législative au titre de l'article 15, paragraphe 1, de la directive 2002/58, d'assurer la conservation généralisée et indifférenciée des adresses IP peut, le cas échéant, être justifiée par l'objectif de la lutte contre les infractions pénales en général lorsqu'il est effectivement exclu que cette conservation puisse engendrer des ingérences graves dans la vie privée de la personne concernée en raison de la possibilité de tirer des conclusions précises sur celle-ci moyennant, notamment, une mise en relation de ces adresses IP avec un ensemble de données de trafic ou de localisation qui auraient également été conservées par ces fournisseurs.

83. Partant, un État membre qui entend imposer aux fournisseurs de services de communications électroniques une obligation de conservation généralisée et indifférenciée des adresses IP en vue d'atteindre un objectif lié à la lutte contre les infractions pénales en général doit s'assurer que les modalités de conservation de ces données soient de nature à garantir qu'est exclue toute combinaison desdites adresses IP avec d'autres données conservées, dans le respect de la directive 2002/58, qui permettrait de tirer des conclusions précises sur la vie privée des personnes dont les données seraient ainsi conservées.

84. Afin d'assurer que soit exclue une telle combinaison de données permettant de tirer des conclusions précises sur la vie privée de la personne en cause, les modalités de conservation doivent concerner la structure même de la conservation qui, en substance, doit être organisée de manière à garantir une séparation effectivement étanche des différentes catégories de données conservées.

85. À cet égard, il appartient certes à l'État membre qui entend imposer aux fournisseurs de services de communications électroniques une obligation de conservation généralisée et indifférenciée des adresses IP en vue d'atteindre un objectif lié à la lutte contre les infractions pénales en général de prévoir, dans sa législation, des règles claires et précises relatives auxdites modalités de conservation, ces modalités devant répondre à des exigences strictes. La Cour peut toutefois fournir des précisions relatives à ces modalités.

86. En premier lieu, les règles nationales mentionnées au point précédent doivent assurer que chaque catégorie de données, y compris les données relatives à l'identité civile et les adresses IP, est conservée de manière pleinement séparée des autres catégories de données conservées.

87. En deuxième lieu, ces règles doivent garantir que, sur un plan technique, la séparation des différentes catégories de données conservées, notamment les données relatives à l'identité civile, les adresses IP, les différentes données relatives au trafic autres que les adresses IP et les différentes données de localisation, est effectivement étanche, moyennant un dispositif informatique sécurisé et fiable.

88. En troisième lieu, en tant que lesdites règles prévoient la possibilité d'une mise en relation des adresses IP conservées avec l'identité civile de la personne concernée dans le respect des exigences découlant de l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 de la Charte, elles ne doivent permettre une telle mise en relation que par l'usage d'un procédé technique performant ne remettant pas en cause l'efficacité de la séparation étanche de ces catégories de données.

89. En quatrième lieu, la fiabilité de cette séparation étanche doit faire l'objet d'un contrôle régulier par une autorité publique autre que celle qui cherche à obtenir l'accès aux données à caractère personnel conservées par les fournisseurs de services de communications électroniques.

90. Pour autant que sont prévues, dans la législation nationale applicable, de telles exigences strictes relatives aux modalités de conservation généralisée et indifférenciée des adresses IP et des autres données conservées par les fournisseurs de services de communications électroniques, l'ingérence résultant de cette conservation des adresses IP ne saurait, en raison de la structure même de ladite conservation, être qualifiée de ‘ grave ’.

91. En effet, dans le cas où un tel dispositif législatif est institué, les modalités de conservation des adresses IP ainsi prescrites excluent que ces données puissent être combinées avec d'autres données conservées dans le respect de la directive 2002/58, permettant de tirer des conclusions précises sur la vie privée de la personne concernée.

92. Par conséquent, en présence d'un dispositif législatif répondant aux exigences exposées aux points 86 à 89 du présent arrêt, garantissant qu'aucune combinaison de données ne permettra de tirer des conclusions précises sur la vie privée de la personne en cause, l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 de la Charte, ne s'oppose pas à ce que l'État membre concerné impose une obligation de conservation généralisée et indifférenciée des adresses IP aux fins d'un objectif de lutte contre les infractions pénales en général.

93. Enfin, un tel dispositif législatif doit, ainsi qu'il ressort du point 168 de l'arrêt du 6 octobre 2020, *La Quadrature du Net e.a.* (C-511/18, C-512/18 et C-520/18, EU:C:2020:791), prévoir une durée de conservation limitée au strict nécessaire et assurer, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus ainsi que contre tout accès à ces données et toute utilisation illicites de celles-ci ».

B.46.1. L'article 126, § 1er, alinéa 1er, de la loi du 13 juin 2005 vise dix-sept données d'identification que les opérateurs précités doivent conserver lorsqu'ils traitent ou génèrent ces données dans le cadre des services et réseaux qu'ils fournissent. Il s'agit du numéro de registre national ou d'un numéro équivalent, des nom et prénom de l'utilisateur final qui est une personne physique ou de la dénomination de l'abonné qui est une personne morale (1°); de l'alias éventuel choisi par l'utilisateur final lors de la souscription au service ou de l'activation du service (2°); des coordonnées de l'abonné qui ont été fournies lors de la souscription au service, notamment son numéro de téléphone, son adresse e-mail et son adresse postale (3°); de la date et de l'heure de la souscription au service et de l'activation du service ainsi que les éléments permettant de déterminer le lieu à partir duquel cette souscription et cette activation ont été effectuées, à savoir notamment l'adresse physique du point de vente où la souscription ou l'activation ont eu lieu, ou l'adresse physique du point de terminaison du réseau ayant servi à la souscription ou à l'activation, ou l'adresse IP ayant servi à la souscription ou à l'activation ainsi que le port source de la connexion et l'horodatage, ou dans le cadre d'un réseau téléphonique mobile, la localisation géographique de l'équipement terminal qui a permis la souscription ou l'activation au moyen d'un numéro de téléphone (4°); de l'adresse physique de livraison du service (5°); de l'adresse de facturation du service et des données relatives au type et au moyen de paiement, à la date des paiements, et la référence de l'opération de paiement en

cas de paiement en ligne (6°); du service principal et des services annexes que l'abonné peut utiliser (7°); de la date à partir de laquelle ces services peuvent être utilisés, de la date de la première utilisation de ces services et de la date de fin de ces services (8°); en cas de transfert de l'identifiant de l'abonné, tel son numéro de téléphone, de l'identité de l'opérateur qui transfère l'identifiant et l'identité de l'opérateur auquel l'identifiant est transféré et la date à laquelle le transfert est effectué (9°); du numéro de téléphone attribué (10°); de l'adresse de messagerie principale et des adresses de messagerie employées comme alias (11°); de l'identité internationale d'abonné mobile, « International Mobile Subscriber Identity » (en abrégé « IMSI ») (12°); de l'identifiant permanent d'abonnement, « Subscription Permanent Identifier » (en abrégé « SUPI ») (13°); de l'identifiant caché d'abonnement, « Subscription Concealed Identifier » (en abrégé « SUCI ») (14°); de l'adresse IP à la source de la connexion, de l'horodatage de l'attribution ainsi que, en cas d'utilisation partagée d'une adresse IP de l'utilisateur final, des ports qui lui ont été attribués (15°); de l'identifiant de l'équipement terminal de l'utilisateur final, ou lorsque l'opérateur ne le traite pas ou ne le génère pas, de l'identifiant de l'équipement qui est le plus proche de cet équipement terminal, à savoir notamment l'identité internationale d'équipement mobile, « *International Mobile Equipment Identity* » (en abrégé « IMEI »), l'identifiant permanent de l'équipement, « *Permanent Equipment Identifier* » (PEI), et l'adresse du contrôleur d'accès au réseau, « *Media Access Control address* » (en abrégé « MAC ») (16°); des autres identifiants relatifs à l'utilisateur final, à l'équipement terminal ou à l'équipement le plus proche de cet équipement terminal, qui résultent de l'évolution technologique et qui sont déterminés par le Roi, pour autant que cet arrêté soit confirmé par la loi dans les six mois suivant la publication de cet arrêté, à condition que ces autres identifiants ne concernent pas le contenu des communications électroniques, ni les métadonnées de communications électroniques qui donnent des informations sur le destinataire de la communication, comme l'adresse IP du destinataire de la communication, ou sur la localisation de l'équipement terminal.

B.46.2. En vertu de l'article 126, § 1er, alinéa 4, de la loi du 13 juin 2005, le Roi peut préciser les données précitées et fixer les exigences en matière de précision et de fiabilité auxquelles ces données doivent répondre.

B.46.3. L'article 126 de la loi du 13 juin 2005 ne précise pas lui-même les finalités pour lesquelles ces données doivent être conservées. Il renvoie à cet égard à l'article 127/1, § 3, de la loi du 13 juin 2005, tel qu'il a été inséré par l'article 13 de la loi du 20 juillet 2022, qui dispose :

« Les données conservées en vertu des articles 126 et 127 le sont pour les autorités et les finalités visées au paragraphe 2, 1° à 8°.

Seules les autorités visées au paragraphe 2 peuvent obtenir d'un opérateur des données conservées en vertu des articles 126 et 127, pour les finalités prévues dans ce même paragraphe, pour autant que prévu par et aux conditions fixées dans une norme législative formelle.

Par dérogation à l'alinéa 2, les autorités visées au paragraphe 2, 10°, ne peuvent pas obtenir d'un opérateur des adresses IP attribuées à la source de la connexion.

Par dérogation à l'alinéa 2, une demande d'une autorité d'obtenir d'un opérateur des adresses IP attribuées à la source d'une connexion n'est autorisée qu'aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave, de la prévention des menaces graves contre la sécurité publique et de la sauvegarde des intérêts vitaux d'une personne physique, lorsque cette autorité serait en mesure, à l'aide des informations en sa possession et des adresses IP attribuées à la source de la connexion obtenues de l'opérateur, de tracer le parcours de navigation d'un utilisateur final sur Internet ».

L'article 127/1, § 2, de la loi du 13 juin 2005 énonce :

« Seules les autorités suivantes peuvent obtenir d'un opérateur des données conservées en vertu des articles 122 et 123, pour les finalités ci-dessous, pour autant que prévu par et aux conditions fixées dans une norme législative formelle :

1° les services de renseignement et de sécurité, afin d'accomplir les missions qui leur sont attribuées par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité;

2° les autorités compétentes aux fins de la prévention de menaces graves pour la sécurité publique;

3° les autorités chargées de la sauvegarde des intérêts vitaux de personnes physiques;

4° les autorités compétentes pour l'examen d'une défaillance de la sécurité du réseau ou du service de communications électroniques ou des systèmes d'information;

5° les autorités administratives ou judiciaires compétentes pour la prévention, la recherche, la détection ou la poursuite d'une infraction commise en ligne ou par le biais d'un réseau ou service de communications électroniques;

6° les autorités administratives ou judiciaires compétentes pour la prévention, la recherche, la détection ou la poursuite d'un fait qui relève de la criminalité grave;

7° les autorités administratives chargées de préserver un intérêt économique ou financier important de l'Union européenne ou de la Belgique, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale;

8° les autorités administratives ou judiciaires compétentes pour la prévention, la recherche, la détection ou la poursuite d'un fait qui constitue une infraction pénale mais qui ne relève pas de la criminalité grave;

9° l'[IBPT] dans le cadre du contrôle de la présente loi et les autorités compétentes pour la protection des données dans le cadre de leurs missions de contrôle;

10° les autorités qui sont légalement habilitées à réutiliser des données à des fins de recherche scientifique ou historique ou à des fins statistiques ».

B.46.4. En ce qui concerne le délai de conservation des données précitées, l'article 126, § 2, de la loi du 13 juin 2005 prévoit que les données visées au paragraphe 1er, alinéa 1er, 1° à 14°, sont conservées tant que le service de communications électroniques est utilisé et douze mois après la fin de ce service. En ce qui concerne les données visées au paragraphe 1er, alinéa 1er, 15° et 16°, celles-ci sont conservées pendant douze mois après la fin de la session. Toutefois, l'adresse du contrôleur d'accès au réseau (MAC) est conservée pendant six mois après la fin de la session lorsque l'opérateur conserve une autre donnée visée au paragraphe 1er, alinéa 1er, 16°, du même article. Enfin, les données visées au paragraphe 1er, alinéa 1er, 17°, de cet article sont conservées pendant la durée fixée par le Roi, sans que celle-ci puisse excéder douze mois après la fin du service.

B.47.1. L'ensemble des données visées à l'article 126, § 1er, alinéa 1er, de la loi du 13 juin 2005, dont l'« adresse IP à la source de la connexion » (4° et 15°), peuvent être conservées pour les finalités énumérées à l'article 127/1, § 2, 1° à 8°, de cette loi. Ces finalités sont définies de manière large et couvrent notamment l'examen d'une défaillance de la sécurité du réseau ou du service de communications électroniques ou des systèmes d'information (4°), la prévention, la recherche, la détection ou la poursuite d'une infraction commise en ligne ou par le biais d'un réseau ou service de communications électroniques (5°) et la prévention, la recherche, la détection ou la poursuite d'un fait qui constitue une infraction pénale mais qui ne relève pas de la criminalité grave (8°).

B.47.2. L’article 126, § 1er, alinéa 1er, de la loi du 13 juin 2005 vise certaines données relatives à l’identité civile des utilisateurs de moyens de communications électroniques. Comme il est dit en B.44.2, ces données peuvent être conservées de manière généralisée et indifférenciée à des fins de sauvegarde de la sécurité nationale, de lutte contre la criminalité, que celle-ci soit grave ou non, et de sauvegarde de la sécurité publique. Les finalités énumérées à l’article 127/1, § 2, 1° à 8°, peuvent être considérées comme correspondant à cette exigence.

B.47.3. Comme il est dit en B.44.3, il convient d’éviter que les données en cause puissent être combinées avec d’autres données conservées permettant de tirer des conclusions précises sur la vie privée des personnes concernées.

B.48.1. Le Conseil des ministres allègue, à cet égard, dans son mémoire complémentaire du 30 mai 2024, que l’exigence d’une séparation étanche entre les catégories de données concernées, telle qu’elle est mentionnée dans l’arrêt précité de la Cour de justice du 30 avril 2024, est nécessaire dans le cadre d’un accès d’une autorité aux bases de données conservées par les opérateurs de communications électroniques, en raison du risque que cette autorité analyse ces données et exploite les possibilités offertes par cette base de données de combiner ces données entre elles pour tirer des conclusions précises sur la vie privée des personnes concernées.

Or, conformément à l’article 127/1, § 2, de la loi du 13 juin 2005, les autorités qui peuvent obtenir des données que les opérateurs doivent conserver en vertu des articles 122 et 123 de la même loi n’accèdent pas elles-mêmes aux banques de données des opérateurs de communications électroniques avec la possibilité de les analyser et de les combiner (extraction de données, « *pull* »). Ces autorités doivent adresser, dans les conditions fixées par la loi attaquée et les lois organiques qui leur sont applicables, une demande ciblée de fourniture de certaines données conservées par l’opérateur de communications électroniques (fourniture de données, « *push* »), sans pour autant que ce dernier laisse entrer ces autorités dans la base de données.

B.48.2. L’article 124 de la loi du 13 juin 2005 dispose, à cet égard :

« S’il n’y est pas autorisé par toutes les personnes directement ou indirectement concernées, nul ne peut :

1° prendre intentionnellement connaissance de l’existence d’une information de toute nature transmise par voie de communication électronique et qui ne lui est pas destinée personnellement;

2° identifier intentionnellement les personnes concernées par la transmission de l’information et son contenu;

3° sans préjudice de l’application des articles 122 et 123 prendre connaissance intentionnellement de données en matière de communications électroniques et relatives a une autre personne;

4° modifier, supprimer, révéler, stocker ou faire un usage quelconque de l’information, de l’identification ou des données obtenues intentionnellement ou non ».

Les articles 127/2 et 127/3 disposent :

« Art. 127/2. § 1er. Les opérateurs veillent à garantir la qualité des métadonnées de communications électroniques conservées et, pour ce qui concerne les données conservées pour les autorités, à ce qu’elles soient de la même qualité que les données traitées dans le cadre de la fourniture du réseau ou du service de communications électroniques.

Les opérateurs mettent tout en œuvre pour établir les liens techniques entre les données conservées pour les autorités qui sont nécessaires pour répondre à leurs demandes.

§ 2. Pour ce qui concerne les données d’identification de l’abonné et les métadonnées de communications électroniques, conservées pour les autorités, les opérateurs :

1° garantissent que les données conservées sont soumises aux mêmes exigences de sécurité et de protection que les données sur le réseau ou traitées par le service;

2° 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;

3° ne peuvent utiliser les données conservées pour d’autres finalités que la fourniture de ces données aux autorités, sauf lorsqu’ils obtiennent le consentement des abonnés concernés conformément à l’article 4, 11), du RGDP et sans préjudice d’autres dispositions légales.

§ 3. Pour ce qui concerne les données d’identification de l’abonné et les métadonnées de communications électroniques, les opérateurs :

1° conservent les données sur le territoire de l'Union européenne et fournissent en Belgique les données demandées par une autorité belge;

2° veillent à ce que les données conservées soient détruites de tout support lorsqu'est expiré le délai de conservation applicable à ces données ou que ces données soient rendues anonymes;

3° 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, conformément à l'article 107/2;

4° garantissent que l'accès aux données conservées pour répondre aux demandes des autorités n'est effectué que par un ou plusieurs membres de la Cellule de coordination visée à l'article 127/3, § 1er, de manière manuelle ou automatisée;

5° assurent une traçabilité de l'exploitation des données conservées.

§ 4. La traçabilité visée au paragraphe 3, 5°, s'effectue à l'aide d'un journal.

L'opérateur prend les mesures nécessaires pour que chaque consultation des données qu'il conserve pour les autorités génère de manière automatisée un enregistrement dans le journal des données suivantes : l'identité de la personne ayant consulté les données, le moment de la consultation et les données consultées.

Ce journal comprend également les informations et documents suivants, qui, le cas échéant, y sont introduits de manière manuelle :

1° l'identité de l'autorité demanderesse, l'objet, la date et l'heure de la demande, une copie de la demande ou un lien vers cette dernière;

2° pour ce qui concerne la réponse de l'opérateur à la demande de l'autorité: l'identité de son destinataire, la date et l'heure de son envoi ainsi que le moyen de communication utilisé pour l'envoyer.

Le journal peut comprendre d'autres documents ou informations, pour autant que ces informations et documents ne révèlent pas d'informations confidentielles sur l'enquête menée par l'autorité, telles que sa finalité ou son contexte.

Les données de ce journal sont conservées pendant une période de dix ans. Á l'échéance de la période de conservation, les données du journal sont détruites.

L'opérateur adopte des mesures appropriées pour assurer la sécurité du journal. Toute modification des données reprises dans le journal est interdite. Toute consultation du journal est journalisée.

Le Roi peut préciser, après avis de l'Autorité de protection des données et de l'Institut, les exigences à respecter par les opérateurs concernant le journal.

Dans le cadre du contrôle de l'opérateur, l'Institut ainsi que l'inspecteur général et les inspecteurs désignés par l'inspecteur général, au sein de l'Autorité de protection des données, visés à l'article 66, § 1er, de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données, peuvent consulter ce journal ou exiger une copie de tout ou partie de ce journal.

§ 5. Si l'Institut dispose d'indices qui pourraient indiquer une infraction d'un opérateur au paragraphe 2, 3 ou 4, il peut l'obliger à se soumettre à un contrôle de sécurité effectué par un organisme qualifié indépendant, proposé par l'opérateur à l'Institut pour accord.

Cet organisme ne prend pas connaissance des demandes des autorités envers les opérateurs, en ce compris le journal visé au paragraphe 4.

Le rapport et les résultats de ce contrôle de sécurité sont communiqués à l'Institut. Le coût du contrôle est à la charge de l'opérateur.

Art. 127/3. § 1er. Auprès de chaque opérateur est constituée une Cellule de coordination, chargée de fournir aux autorités légalement habilitées, à leur demande, des données de communications électroniques.

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.

Ces autorités adressent leurs demandes à cette cellule.

Le cas échéant, plusieurs opérateurs peuvent créer une Cellule de coordination commune. En pareil cas, chaque opérateur prend les mesures nécessaires pour que cette Cellule de coordination commune soit en mesure de répondre aux demandes qui lui sont adressées.

Le Roi détermine, après avis des autorités compétentes pour la protection des données et de l'Institut, les exigences auxquelles la Cellule de coordination doit répondre, en particulier au niveau de la disponibilité et de l'accessibilité.

§ 2. Les membres de la Cellule de coordination et les préposés apportant une aide technique sont soumis au secret professionnel. Ces membres ne communiquent aux préposés que les données strictement nécessaires pour obtenir cette aide.

Chaque opérateur veille à la confidentialité des données traitées par la Cellule de coordination.

Les membres de la Cellule de coordination disposent d'un avis de sécurité positif et non périmé, visé à l'article 22*quinquies*/1 de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

L'autorité administrative compétente pour le traitement des avis est le ministre de la Justice.

Le Roi définit des mesures de sécurité alternatives à un avis de sécurité, qui sont adaptées aux personnes pour lesquelles un avis de sécurité ne peut être rendu, à défaut d'informations suffisantes les concernant.

Par dérogation à l'alinéa 3, une personne visée à l'alinéa 5 peut faire partie de la Cellule de coordination, en respectant ces mesures de sécurité alternatives et sans disposer d'un avis de sécurité.

Le Roi détermine, après avis des autorités compétentes pour la protection des données et de l'Institut :

1° pour les opérateurs autres que ceux qui disposent déjà d'un officier de sécurité en raison d'autres activités que la Cellule de coordination, les catégories d'opérateurs qui sont dispensés de l'obligation de désigner un tel officier en fonction du nombre de demandes reçues de la part des autorités judiciaires, ainsi que les règles qui s'appliquent en l'absence d'un tel officier;

2° les exigences auxquelles un membre de la Cellule de coordination doit répondre, en particulier en matière d'emploi des langues;

3° les règles permettant l'accès des autorités belges habilitées aux coordonnées de la Cellule de coordination et de ses membres.

§ 3. Chaque opérateur établit une procédure interne permettant de répondre aux demandes d'accès des autorités aux données à caractère personnel concernant les utilisateurs finaux. 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 est considéré comme responsable du traitement au sens du RGDP pour les données traitées sur la base des articles 122, 123, 126, 126/1, 126/2, 126/3 et 127.

§ 4. Le Roi détermine, après avis des autorités compétentes pour la protection des données et de l'Institut, les règles régissant la collaboration entre les opérateurs et les autorités belges ou avec certaines d'entre elles. Sont déterminés, entre autres, les éléments suivants, le cas échéant et par autorité concernée :

a) le mode de transfert, la forme et le contenu des demandes et des réponses;

b) le degré d'urgence de traitement des demandes;

c) le délai de réponse;

d) la disponibilité requise du service;

e) les modalités de test de la collaboration;

f) les tarifs de rétribution de cette collaboration.

Si nécessaire et pour l'application du présent article, le Roi peut prévoir des règles différentes pour différentes catégories d'opérateurs, notamment selon le nombre de demandes qu'ils reçoivent des autorités judiciaires et des services de renseignement et de sécurité, le lieu de leur établissement et la fourniture ou non d'un réseau de communications électroniques en Belgique ».

B.48.3. Comme le soutient le Conseil des ministres dans son mémoire complémentaire du 30 mai 2024, la loi attaquée fixe ainsi des conditions strictes qui empêchent tant les opérateurs que les autorités compétentes d'utiliser les adresses IP pour effectuer le traçage exhaustif du parcours de navigation d'un internaute et, ensuite, de son activité en ligne, ainsi que pour établir, à l'aide de ces données, le profil détaillé de ce dernier.

B.48.4. Du reste, l'on n'aperçoit pas en quoi l'applicabilité aux services OTT de l'article 8 de la loi du 20 juillet 2022 serait contraire au principe d'égalité et de non-discrimination et au principe de légalité.

B.49. Les premier et deuxième moyens dans l'affaire n° 7930, le moyen unique dans l'affaire n° 7931, ainsi que le deuxième moyen dans l'affaire n° 7932, en sa première et sa troisième branches, ne sont pas fondés en ce qu'ils sont pris de la violation de l'article 22 de la Constitution, lu en combinaison avec l'article 8 de la Convention européenne des droits de l'homme, avec les articles 7, 8 et 52, paragraphe 1, de la Charte et avec l'article 15, paragraphe 1, de la directive 2002/58/CE.

6. L'obligation d'identification des abonnés et des utilisateurs finaux de services de communication électronique (article 12)

B.50. Les premier et deuxième moyens dans l'affaire n° 7930 et les troisième, quatrième et sixième branches du deuxième moyen dans l'affaire n° 7932 portent sur l'article 12 de la loi du 20 juillet 2022, qui remplace l'article 127 de la loi du 13 juin 2005 comme suit :

« § 1er. Le présent article s'applique aux opérateurs qui fournissent en Belgique, aux utilisateurs finaux, un service de communications électroniques.

Il est interdit de distribuer en Belgique, en ce compris par internet, aux utilisateurs finaux, sans l'accord de l'entreprise étrangère qui fournit le service de communications électroniques accessible au public :

- des cartes prépayées ou des abonnements de cette entreprise qui leur permettent d'y utiliser un service de communications électroniques;

- des objets connectés dans lesquels un produit de cette entreprise est intégré et qui leur permettent d'y utiliser un service d'accès à internet ou un service de communication interpersonnelle d'un opérateur.

La personne qui distribue en Belgique ces cartes prépayées, ces abonnements ou ces objets connectés fournit aux officiers de police judiciaire de l'Institut, à leur demande, la preuve de cet accord.

En cas d'accord de l'entreprise, cette dernière est opérateur et se conforme à l'article 9, § 1er.

§ 2. Pour l'application du présent article, il faut entendre par :

1° ' service de communications électroniques payant ' : le service de communications électroniques pour lequel un paiement de l'abonné à l'opérateur est nécessaire pour utiliser le service ou continuer à l'utiliser, ainsi que tout service de communications électroniques offert sans surcoût par l'opérateur à l'abonné conjointement à ce service;

2° ' service de communications électroniques gratuit ' : le service de communications électroniques offert par l'opérateur à l'abonné autre que le service de communications électroniques payant;

3° ' méthode d'identification directe ' : la méthode par laquelle l'opérateur collecte et conserve pour les besoins des autorités visées à l'article 127/1, § 3, alinéa 1er :

- des données fiables relatives à l'identité civile d'une personne physique, qui est son abonné ou qui agit pour le compte d'une personne morale qui est l'abonnée de l'opérateur afin de remplir l'obligation d'identification de la personne morale et, le cas échéant;

- une copie du document d'identification de cette personne physique;

4° ' méthode d'identification indirecte ' : la méthode par laquelle l'opérateur collecte et conserve des données qui permettent aux autorités visées à l'article 127/1, § 3, alinéa 1er, d'obtenir d'un tiers l'identité de ses abonnés;

5° ' point de vente ' : le point de vente physique de cartes prépayées ou d'abonnements d'un opérateur.

§ 3. L'opérateur qui fournit un service de communications électroniques payant identifie ses abonnés au moyen d'une méthode d'identification directe ou indirecte, à l'exception des méthodes d'identification indirecte visées au paragraphe 10, alinéa 1er, 1° et 2°.

Par dérogation à l'alinéa 2, l'opérateur visé à cet alinéa peut également identifier l'abonné au moyen de la méthode d'identification indirecte visée au paragraphe 10, alinéa 1er, 2°, lorsqu'il offre un service de communications électroniques pour lequel les méthodes d'identification directe et indirecte autorisées par l'alinéa 2 impliquent des contraintes importantes pour les abonnés et l'opérateur, à savoir :

- les services fixes d'accès à internet utilisés par des personnes physiques en dehors de leur lieu de résidence et du lieu où elles exercent une activité professionnelle, tels que les services de communications électroniques offerts à l'aide de bornes WiFi des opérateurs;

- les autres services déterminés par le Roi.

L'opérateur qui fournit un service de communications électroniques gratuit identifie ses abonnés au moyen d'une méthode d'identification indirecte visée au paragraphe 10.

§ 4. Il est interdit aux points de vente de conserver des données d'identification ou des copies de documents d'identification ou d'en faire un usage quelconque autre que l'identification de l'abonné.

Les opérateurs prennent les mesures d'ordre technique et organisationnel adéquates et proportionnées pour la mise en œuvre de l'interdiction visée à l'alinéa 1er, en ce compris en permettant aux points de vente d'introduire directement les données d'identification et les copies de documents d'identification dans leurs systèmes informatiques.

Si une introduction directe dans les systèmes informatiques de l'opérateur n'est temporairement pas possible en raison d'une défaillance de ces systèmes, les données d'identification et les copies de documents d'identification gardées par le point de vente lors de cette défaillance sont détruites au plus tard après l'activation du service de communications électroniques.

Sauf disposition légale contraire, les données d'identification et les copies de document d'identification collectées en vertu du présent article sont conservées à partir de la date d'activation du service jusqu'à douze mois après la fin du service de communications électroniques.

§ 5. L'opérateur met tout en œuvre pour assurer la fiabilité de l'identification de l'abonné qui est une personne physique.

Lorsque l'opérateur identifie l'abonné à l'aide d'un document d'identification, il s'assure :

- que les données d'identification collectées correspondent aux données sur ce document;

- que la date de validité de ce document n'est pas dépassée au moment de l'identification de l'abonné.

Lorsque l'opérateur identifie l'abonné à l'aide d'un document d'identification, il met tout en œuvre pour vérifier :

- que ce document est l'original, lisible et présente l'apparence d'authenticité;

- que ce document est relatif à la personne identifiée.

Afin d'assurer la fiabilité visée à l'alinéa 1er et d'éviter les fraudes à l'identité, l'opérateur ou le point de vente peut réaliser de manière automatique une comparaison entre les paramètres biométriques sur la photo du document d'identification de l'abonné et ceux de son visage, aux conditions suivantes :

1° l'outil de comparaison a été autorisé par le ministre et le ministre de la Justice, après vérification que cet outil assure la fiabilité de l'identification de l'abonné pour les besoins des autorités, en tenant compte en particulier du risque de fraude à l'identité de la part de la personne qui s'identifie;

2° l'opérateur offre à l'abonné au moins une manière alternative de s'identifier;

3° l'abonné a donné son consentement explicite au sens de l'article 4, 11), du RGPD, ce qui implique notamment que l'abonné soit informé des finalités pour lesquelles ces données seront récoltées, à savoir la mise en œuvre de l'obligation légale d'identification de l'abonné de manière fiable et la lutte contre la fraude à l'identité;

4° l'opérateur et le point de vente ne peuvent communiquer ces données biométriques à un tiers au sens de l'article 4, 10), du RGPD et ne peuvent les traiter que dans les limites nécessaires en vue d'accomplir les finalités de comparaison faciale visées au présent alinéa;

5° il est interdit de conserver ces données biométriques au-delà de cette comparaison.

Lorsque l'abonné s'identifie à l'aide d'une carte d'identité électronique belge et que l'opérateur n'a pas mis en œuvre la méthode de comparaison faciale visée à l'alinéa 4, l'opérateur peut demander à l'abonné l'introduction du code PIN.

§ 6. Les documents d'identification qui sont admis pour identifier l'abonné qui est une personne physique sont les suivants :

1° la carte d'identité électronique belge;

2° le passeport belge;

3° le certificat d'inscription au registre des étrangers – séjour temporaire, délivré avant le 11 octobre 2021, en cours de validité (carte A);

4° le titre de séjour limité (carte A);

5° le certificat d'inscription au registre des étrangers, délivré avant le 11 octobre 2021, en cours de validité (carte B);

6° le titre de séjour illimité (carte B);

7° la carte d'identité d'étranger, délivrée avant le 11 octobre 2021, en cours de validité (carte C);

8° le titre d'établissement (carte K);

9° le titre de séjour de résident de longue durée – UE, délivré avant le 11 octobre 2021, en cours de validité (carte D);

10° le titre de séjour de résident de longue durée – UE (carte L);

11° l'attestation d'enregistrement, délivrée avant le 10 mai 2021, en cours de validité (carte E);

12° le document d'enregistrement ' Art 8 DIR 2004/38/CE ' E (carte EU);

13° le document attestant de la permanence de séjour, délivré avant le 10 mai 2021, en cours de validité (carte E+);

14° le document de séjour permanent ' Art 19 DIR 2004/38/CE ' (carte EU+);

15° la carte de séjour de membre de la famille d'un citoyen de l'Union, délivrée avant le 11 octobre 2021, en cours de validité (carte F);

16° la carte de séjour de membre de la famille d'un citoyen de l'Union ' membre famille UE – Art 10 DIR 2004/38/CE ' (carte F);

17° la carte de séjour permanent de membre de la famille d'un citoyen de l'Union, délivrée avant le 11 octobre 2021, en cours de validité (carte F+);

18° la carte de séjour permanent de membre de la famille d'un citoyen de l'Union ' membre famille UE – Art. 20 DIR 2004/38/CE ' (carte F+);

19° la carte bleue européenne (carte H);

20° le permis pour personne faisant l'objet d'un transfert temporaire intragroupe ' ICT ' (carte I);

21° le permis pour mobilité de longue durée ' mobile ICT ' (carte J);

22° la carte de séjour pour bénéficiaires de l'accord de retrait ' Art. 50 TUE ' (carte M);

23° la carte de séjour permanent pour bénéficiaires de l'accord de retrait ' Art. 50 TUE ' (carte M);

24° la carte pour petit trafic frontalier pour bénéficiaires de l'accord de retrait ' Art. 50 TUE – Travailleur frontalier ' (carte N);

25° l'acte de notoriété;

26° l'annexe 12 délivrée en application de l'article 6 de l'arrêté royal du 25 mars 2003 relatif aux cartes d'identité ou en application de l'article 36*bis* de l'arrêté royal du 8 octobre 1981 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers;

27° l'attestation d'immatriculation (carte orange);

28° la carte d'identité étrangère, lorsqu'un passeport international n'est pas nécessaire pour séjourner en Belgique;

29° les cartes d'identité spéciales délivrées aux catégories de personnel actives dans les missions diplomatiques et consulaires et aux membres de leur famille, en vertu des Conventions de Vienne de 1961 et 1963 et de l'arrêté royal du 30 octobre 1991 relatif aux documents de séjour en Belgique de certains étrangers;

30° la carte d'identité délivrée conformément aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux;

31° le passeport étranger;

32° tout autre document déterminé par le Roi, pour autant que l'arrêté royal soit confirmé par la loi dans les six mois suivant la publication de cet arrêté.

Les opérateurs qui disposent de points de vente permettent à leurs abonnés de s'identifier à l'aide de n'importe lequel des documents d'identification visés à l'alinéa 1er, dans le cadre d'au moins une méthode d'identification de leur choix.

Par dérogation à l'alinéa 2, un opérateur peut refuser d'identifier un abonné sur base d'un document d'identification visé à l'alinéa 1er autre que la carte d'identité électronique belge s'il lui offre la possibilité de s'identifier selon une des manières alternatives visées à l'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 et pour autant que l'abonné soit en mesure de mettre en œuvre cette alternative.

Lorsqu'un opérateur identifie l'abonné à partir d'un document d'identification, il conserve une copie de ce document, sauf lorsqu'il s'agit de la carte d'identité électronique belge.

Les opérateurs prennent les mesures d'ordre technique et organisationnel adéquates et proportionnées pour empêcher que les points de vente ou des tiers ne prennent une copie de la carte d'identité électronique belge, sans préjudice du paragraphe 4, alinéa 3.

§ 7. Sans préjudice de l'article 126, lorsqu'un opérateur identifie l'abonné qui est une personne physique à partir de sa carte d'identité électronique belge, il conserve son numéro de registre national, son nom et son prénom.

Sans préjudice de l'article 126, lorsqu'un opérateur identifie l'abonné à partir d'un autre document que la carte d'identité électronique belge ou au moyen d'une autre méthode

d'identification directe que la présentation d'un document d'identification, il conserve parmi les données suivantes celles qui se trouvent sur le document d'identification présenté ou qui sont traitées lors de la mise en œuvre de la méthode d'identification directe :

1° le nom et le prénom;

2° la nationalité;

3° la date de naissance;

4° l'adresse du domicile, l'adresse e-mail et le numéro de téléphone;

5° le numéro du document d'identification et le pays d'émission du document lorsqu'il s'agit d'un document étranger;

6° le lien entre le nouveau service de communications électroniques auquel l'abonné souscrit et le service pour lequel il a déjà été identifié.

§ 8. Lorsqu'un opérateur fournit à un abonné qui est une personne morale un service de communications électroniques mobile sur la base d'une carte prépayée et qu'il l'identifie par le biais d'une méthode d'identification directe, il collecte et conserve, en respectant les exigences visées aux paragraphes 4 à 7, l'identité civile d'une personne physique qui agit pour le compte de la personne morale.

§ 9. Pour ce qui concerne les méthodes d'identification directe, le Roi peut :

1° déterminer les seules méthodes que les opérateurs peuvent utiliser;

2° prévoir, par méthode, les conditions à respecter, en ce compris soumettre une méthode d'identification proposée par une entreprise à une autorisation préalable du ministre et du ministre de la Justice;

3° imposer des obligations aux opérateurs, aux points de vente, aux entreprises fournissant un service d'identification et aux abonnés, en vue de l'identification de ces derniers.

§ 10. L'opérateur permet aux autorités visées à l'article 127/1, § 3, alinéa 1er, d'identifier ses abonnés par le biais d'une méthode d'identification indirecte :

1° en conservant, en exécution de l'article 126 et pendant les délais prévus par cet article, l'adresse IP ayant servi à la souscription au service de communications électroniques ou à son activation, l'adresse IP à la source de la connexion et les données qui doivent être conservées avec ces adresses, ou;

2° en collectant et conservant le numéro de téléphone de l'abonné attribué dans le cadre d'un service de communications électroniques payant pour lequel un opérateur doit identifier l'abonné conformément au présent article, ou;

3° en cas de paiement en ligne spécifique à la souscription d'un service de communications électroniques, en collectant et conservant :

- la référence de l'opération de paiement, et;

- le nom, le prénom, l'adresse du domicile et la date de naissance déclarés par la personne physique qui est l'abonné de l'opérateur ou qui agit pour le compte d'une personne morale qui est l'abonnée de l'opérateur afin de remplir son obligation en matière d'identification, ou;

4° en cas de carte SIM (' subscriber identity/identification module ') ou toute autre carte équivalente intégrée dans un véhicule, en collectant et conservant le numéro de châssis de ce véhicule ainsi que le lien entre ce numéro et le numéro de cette carte;

5° en cas de souscription d'un abonné qui réside dans un centre fermé ou un lieu d'hébergement au sens des articles 74/8 et 74/9 de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers à un service de communications électroniques mobile fourni au moyen d'une carte prépayée, en collectant et conservant le nom et le prénom de l'abonné, son numéro de sécurité publique, à savoir le numéro de dossier attribué par l'Office des Etrangers et les coordonnées du centre ou du lieu d'hébergement où la souscription a eu lieu, ou;

6° en cas de souscription à un service de communications électroniques par une personne morale au nom et pour le compte d'une personne physique qui rencontre des difficultés à effectuer cette souscription, en collectant et conservant la dénomination précise de cette personne morale et, pour ce qui concerne cette personne physique, au minimum son nom, son prénom, son adresse de résidence, lorsqu'elle en dispose, sa date de naissance et le numéro par lequel elle est identifiée, tel un numéro de registre national, ces informations lui étant transmises par cette personne morale.

Pour l'application de l'alinéa 1er, 6°, la personne morale :

1° doit, avant de pouvoir souscrire à un service de communications électroniques pour la personne physique, obtenir un agrément, délivré par le ministre et le ministre de la Justice, et ayant pour objet de vérifier qu'elle respecte les valeurs démocratiques inscrites dans la Constitution ainsi que le présent article;

2° s'identifie auprès de l'opérateur conformément au présent article;

3° identifie les abonnés à l'aide d'un des documents d'identification visés au paragraphe 6, conformément aux exigences de fiabilité visées au paragraphe 5, ou à l'aide d'une autre méthode autorisée dans l'agrément visé au 1°;

4° conserve une copie du document d'identification des abonnés autre que la carte d'identité électronique belge, sauf dérogation accordée dans l'agrément visé au 1°;

5° conserve une liste actualisée permettant de faire le lien entre le service de communications électroniques et les abonnés, comprenant au minimum le nom, le prénom,

l'adresse de la résidence, lorsque la personne en dispose, la date de naissance et le numéro par lequel elle est identifiée, tel le numéro de registre national.

Le Roi peut :

1° prévoir par méthode visée à l'alinéa 1er les conditions à respecter, une condition pouvant être l'obtention d'une autorisation préalable du ministre et du ministre de la Justice;

2° imposer des obligations aux opérateurs, aux personnes morales visées à l'alinéa 1er, aux entreprises fournissant un service d'identification et aux abonnés, en vue de l'identification de ces derniers.

§ 11. Sauf preuve contraire, la personne identifiée est présumée utiliser elle-même le service de communications électroniques.

Pour les services de communications électroniques mobiles fournis au moyen d'une carte prépayée, le Roi :

1° restreint la possibilité pour l'abonné de permettre à des tiers de bénéficier du service;

2° impose des obligations aux abonnés qui sont des personnes morales afin de déterminer les utilisateurs habituels du service.

L'opérateur qui offre une carte SIM ou toute carte équivalente, destinée à être intégrée dans un véhicule, conserve le numéro de châssis de ce véhicule ainsi que le lien entre ce numéro et le numéro de cette carte. À la demande d'une autorité, l'opérateur ne lui communique que ce numéro de châssis ou le numéro de cette carte.

Le Roi peut fixer les modalités de l'obligation visée à l'alinéa 3 et peut imposer aux entreprises qui disposent du numéro de châssis de le transmettre aux opérateurs.

§ 12. Si un opérateur ne respecte pas les mesures qui lui sont imposées par le présent article ou par le Roi, il lui est interdit de fournir le service pour lequel les mesures en question n'ont pas été prises.

Les opérateurs déconnectent les abonnés qui ne respectent pas les mesures qui leur sont imposées par le présent article ou par le Roi, des réseaux et services auxquels les mesures imposées s'appliquent. Ces abonnés ne sont en aucune manière indemnisés pour la déconnexion.

L'arrêté royal visé dans le présent article est proposé par le ministre de la Justice, le ministre de l'Intérieur, le ministre de la Défense et le ministre, fait l'objet d'un avis de l'Autorité de protection des données et de l'Institut et est délibéré en Conseil des ministres. ' ».

B.51.1. La partie requérante dans l'affaire n° 7930 prend les premier et deuxième moyens de la violation des articles 11, 12, 22 et 29 de la Constitution, de l'article 15, paragraphe 1, et des articles 5, 6 et 9 de la directive 2002/58/CE, lus à la lumière des articles 7, 8, 11, 47 et 52, paragraphe 1, de la Charte, des articles 6, 8, 10, 11 et 18 de la Convention européenne des droits de l'homme et des articles 13 et 54 de la directive (UE) 2016/680, en ce que l'article 12 de la loi du 20 juillet 2022 instaure une obligation généralisée de conservation des données d'identification, sans que cette conservation s'avère nécessaire ni strictement limitée au regard du but poursuivi. En particulier, elle allègue que ce système n'est pas conforme à la jurisprudence de la Cour de justice relative à l'article 15 de la directive 2002/58/CE et aux articles 7, 8 et 52 de la Charte, qui n'autorise une telle conservation qu'aux fins de sauvegarde de la sécurité nationale, de lutte contre la criminalité grave et de prévention des menaces graves contre la sécurité publique.

Il ressort des développements des premier et deuxième moyens relatifs à l'article 12 de la loi du 20 juillet 2022 que les griefs formulés par cette partie requérante doivent être interprétés comme portant uniquement, dans ce cadre, sur la liste des données d'identification visées dans cette disposition et sur leur délai de conservation, en ce que ces mesures ne seraient pas compatibles avec le droit au respect de la vie privée ni avec le droit à la protection des données à caractère personnel, garantis par les dispositions citées en B.11.2.

La partie requérante ne prend aucun grief de la violation des autres normes de référence citées aux premier et deuxième moyens dans le cadre de l'article 12 de la loi du 20 juillet 2022.

B.51.2. Les parties requérantes dans l'affaire n° 7932 prennent un deuxième moyen de la violation des articles 10, 11, 15, 22 et 29 de la Constitution, lus en combinaison ou non avec les articles 5, 6, 8, 9, 10, 11, 14 et 18 de la Convention européenne des droits de l'homme, avec les articles 7, 8, 11, 47 et 52 de la Charte, avec l'article 5, paragraphe 4, du Traité sur l'Union européenne ainsi qu'avec la directive 2002/58/CE, avec la directive (UE) 2016/680 et avec le RGPD.

Les griefs des parties requérantes portent tout d'abord sur l'article 127, § 5, alinéa 3, de la loi du 13 juin 2005 en ce que cet article autoriserait l'utilisation de la technologie de la

reconnaissance faciale, ce qui serait contraire au droit au respect de la vie privée et au droit à la protection des données à caractère personnel (troisième branche). Ensuite, les parties requérantes dénoncent la mesure prévue à l'article 127, § 10, 4°, de la loi du 13 juin 2005 qui prévoit, dans le cas de la carte SIM ou d'une carte équivalente intégrée dans un véhicule, la collecte et la conservation du numéro de châssis de ce véhicule et le lien entre ce numéro et le numéro de la carte. Selon elles, cette mesure serait disproportionnée, notamment par sa combinaison avec la conservation obligatoire des données de localisation sur les autoroutes. Il y a lieu d'interpréter ce grief comme portant sur la compatibilité de la mesure précitée avec le droit au respect de la vie privée (quatrième branche). Enfin, les parties requérantes soutiennent que l'article 127, § 11, de la loi du 13 juin 2005 n'est pas compatible avec le droit à un procès équitable, garanti par l'article 6 de la Convention européenne des droits de l'homme, en ce qu'il instaurerait la présomption qu'un service de communications électroniques est utilisé par la personne qui a été identifiée sur la base de cette disposition (sixième branche).

B.52. La Cour examine d'abord la liste des données conservées en vertu l'article 12 de la loi du 20 juillet 2022 – dont la mesure relative aux cartes SIM ou aux cartes équivalentes – et leur délai de conservation (premier et deuxième moyens dans l'affaire n° 7930, deuxième moyen, quatrième branche, dans l'affaire n° 7932), puis la présomption d'utilisation du service de communications électroniques (deuxième moyen, sixième branche, dans l'affaire n° 7932) et enfin l'utilisation de la technologie de la reconnaissance faciale (deuxième moyen, troisième branche, dans l'affaire n° 7932).

B.53.1. En vertu de l'article 127 de la loi du 13 juin 2005, tel qu'il a été remplacé par l'article 12 de la loi du 20 juillet 2022, il incombe aux « opérateurs qui fournissent en Belgique, aux utilisateurs finaux, un service de communications électroniques » d'identifier les abonnés à ce service (article 127, § 3), et ce, au moyen d'une méthode d'identification directe ou indirecte (article 127, §10).

La méthode d'identification directe constitue la méthode par laquelle l'opérateur collecte et conserve, d'une part, « des données fiables relatives à l'identité civile d'une personne physique, qui est son abonné ou qui agit pour le compte d'une personne morale qui est l'abonnée de l'opérateur afin de remplir l'obligation d'identification de la personne morale »

et, d'autre part, « une copie du document d'identification de cette personne physique », et ce, pour les besoins des autorités visées à l'article 127/1, § 3 , alinéa 1er, de la loi du 13 juin 2005 (article 127, § 2, 3°).

La méthode d'identification indirecte constitue « la méthode par laquelle l'opérateur collecte et conserve des données qui permettent aux autorités visées à l'article 127/1, § 3, alinéa 1er, d'obtenir d'un tiers l'identité de ses abonnés » (article 127, § 2, 4°).

B.53.2.1. Les documents admis pour procéder à l'identification de l'abonné sont ceux qui sont visés à l'article 127, § 6, alinéa 1er, de la loi du 13 juin 2005. Il s'agit de la carte d'identité électronique belge (1°), du passeport belge (2°), du certificat d'inscription au registre des étrangers – séjour temporaire, délivré avant le 11 octobre 2021, en cours de validité (carte A) (3°), du titre de séjour limité (carte A) (4°), du certificat d'inscription au registre des étrangers, délivré avant le 11 octobre 2021, en cours de validité (carte B) (5°), du titre de séjour illimité (carte B) (6°), de la carte d'identité d'étranger, délivrée avant le 11 octobre 2021, en cours de validité (carte C) (7°), du titre d'établissement (carte K) (8°), du titre de séjour de résident de longue durée – UE, délivré avant le 11 octobre 2021, en cours de validité (carte D) (9°), du titre de séjour de résident de longue durée – UE (carte L) (10°), de l'attestation d'enregistrement, délivrée avant le 10 mai 2021, en cours de validité (carte E) (11°), du document d'enregistrement « Art. 8 DIR 2004/38/CE » E (carte EU) (12°), du document attestant de la permanence de séjour, délivré avant le 10 mai 2021, en cours de validité (carte E+) (13°), du document de séjour permanent « Art.19 DIR 2004/38/CE » (carte EU+) (14°), de la carte de séjour de membre de la famille d'un citoyen de l'Union, délivrée avant le 11 octobre 2021, en cours de validité (carte F) (15°), de la carte de séjour de membre de la famille d'un citoyen de l'Union « membre famille UE – Art.10 DIR 2004/38/CE » (carte F) (16°), de la carte de séjour permanent de membre de la famille d'un citoyen de l'Union, délivrée avant le 11 octobre 2021, en cours de validité (carte F+) (17°), de la carte de séjour permanent de membre de la famille d'un citoyen de l'Union « membre famille UE – Art.20 DIR 2004/38/CE » (carte F+) (18°), de la carte bleue européenne (carte H) (19°), du permis pour personne faisant l'objet d'un transfert temporaire intragroupe « ICT » (carte I) (20°), du permis pour mobilité de longue durée « mobile ICT » (carte J) (21°), de la carte de séjour pour bénéficiaires de l'accord de retrait « Art. 50 TUE » (carte M) (22°), de la carte de séjour permanent pour bénéficiaires de l'accord de retrait

« Art. 50 TUE » (carte M) (23°), de la carte pour petit trafic frontalier pour bénéficiaires de l'accord de retrait « Art. 50 TUE – Travailleur frontalier » (carte N) (24°), de l'acte de notoriété (25°), de l'annexe 12 délivrée en application de l'article 6 de l'arrêté royal du 25 mars 2003 « relatif aux cartes d'identité » ou en application de l'article 36*bis* de l'arrêté royal du 8 octobre 1981 « sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers » (26°), de l'attestation d'immatriculation (carte orange) (27°), de la carte d'identité étrangère, lorsqu'un passeport international n'est pas nécessaire pour séjourner en Belgique (28°), des cartes d'identité spéciales délivrées aux catégories de personnel actives dans les missions diplomatiques et consulaires et aux membres de leur famille, en vertu des Conventions de Vienne de 1961 et 1963 et de l'arrêté royal du 30 octobre 1991 « relatif aux documents de séjour en Belgique de certains étrangers » (29°), de la carte d'identité délivrée conformément aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux (30°), du passeport étranger (31°), et, enfin, de tout autre document déterminé par le Roi, pour autant que l'arrêté royal soit confirmé par la loi dans les six mois suivant la publication de cet arrêté (32°).

B.53.2.2. En vertu de l'article 127, § 6, alinéa 2, de la loi du 13 juin 2005, l'opérateur disposant de points de vente permet à son abonné de s'identifier au moyen du document d'identification de son choix parmi ceux qui sont énumérés à l'alinéa 1er. En vertu de l'alinéa 3, l'opérateur peut toutefois refuser d'identifier l'abonné au moyen d'un des documents d'identification précités si l'abonné a la possibilité de s'identifier selon une des autres manières visées dans l'arrêté royal du 27 novembre 2016 « relatif à l'identification de l'utilisateur final de services de communications électroniques accessibles au public mobiles fournis sur la base d'une carte prépayée ». Cette solution n'est pas possible lorsque l'abonné souhaite être identifié au moyen de sa carte d'identité électronique belge.

B.53.2.3. Dans l'hypothèse où l'abonné est identifié au moyen d'un des documents d'identification précités, l'opérateur conserve une copie de ce document, sauf lorsqu'il s'agit de la carte d'identité électronique belge (article 127, § 6, alinéa 4).

B.53.3.1. À la suite de l'identification de l'abonné, il incombe à l'opérateur de conserver certaines données à caractère personnel en vertu de l'application de l'article 127, §§ 7 et 8, de la loi du 13 juin 2005.

B.53.3.2. Lorsque l'abonné est une personne physique et que l'identification est réalisée à partir de la carte d'identité électronique belge, l'opérateur conserve le numéro de registre national, le nom et le prénom de l'abonné (article 127, § 7, alinéa 1er).

B.53.3.3. Lorsque l'abonné est une personne physique et que l'identification est réalisée à partir d'un document autre que la carte d'identité électronique belge, visé à l'article 127, § 6, alinéa 1er, 2° à 32°, ou à partir d'une autre méthode d'identification directe que la présentation d'un document d'identification, l'opérateur conserve parmi les données qui se trouvent sur le document d'identification ou qui sont traitées lors de la mise en œuvre de la méthode d'identification directe les nom et prénom, la nationalité, la date de naissance, l'adresse du domicile, l'adresse e-mail, le numéro de téléphone, le numéro du document d'identification et le pays d'émission du document lorsqu'il s'agit d'un document étranger et, enfin, le lien entre le nouveau service de communications électroniques auquel l'abonné souscrit et le service pour lequel il a déjà été identifié (article 127, § 7, alinéa 2).

B.53.3.4. Lorsque l'abonné est une personne morale, que le service de communication électronique est fourni sur la base d'une carte prépayée et que l'identification est réalisée au moyen d'une méthode d'identification directe, l'opérateur collecte et conserve les données, visées à l'article 127, §§ 4 à 7, de la loi du 13 juin 2005, qui sont relatives à l'identité civile d'une personne physique agissant pour le compte de la personne morale (article 127, § 8).

B.53.4. Enfin, en vertu de l'article 127, § 10, de la loi du 13 juin 2005, il incombe aux opérateurs de permettre aux autorités visées à l'article 127/1, § 3, alinéa 1er, de la même loi d'identifier leurs abonnés au moyen d'une méthode d'identification indirecte.

Pour ce faire, l'article 127, § 10, alinéa 1er, prévoit que les opérateurs conservent, en exécution de l'article 126 de la loi du 13 juin 2005 et pendant les délais prévus par cet article, l'adresse IP ayant servi à la souscription au service de communications électroniques ou à son activation, l'adresse IP à la source de la connexion et les données qui doivent être conservées

avec ces adresses (1°) ou le numéro de téléphone de l'abonné attribué dans le cadre d'un service de communications électroniques payant pour lequel un opérateur doit identifier l'abonné conformément à l'article 127 de la loi du 13 juin 2005 (2°); que les opérateurs collectent et conservent, en cas de paiement en ligne spécifique à la souscription d'un service de communications électroniques, la référence de l'opération de paiement et le nom, le prénom, l'adresse du domicile et la date de naissance déclarés par la personne physique qui est l'abonné de l'opérateur ou qui agit pour le compte d'une personne morale qui est l'abonnée de l'opérateur afin de remplir leur obligation en matière d'identification (3°) ou, dans le cas d'une carte SIM ou de toute autre carte équivalente intégrée dans le véhicule, le numéro de châssis du véhicule et le lien entre ce numéro et le numéro de la carte (4°); que les opérateurs collectent et conservent, en cas de souscription d'un abonné résidant dans un centre fermé ou un lieu d'hébergement au sens des articles 74/8 et 74/9 de la loi du 15 décembre 1980 « sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers » à un service de communications électroniques mobile fourni au moyen d'une carte prépayée, le nom et prénom de l'abonné et le numéro de sécurité publique (5°) ou, dans le cas d'une souscription à un service de communications électroniques par une personne morale au nom et pour le compte d'une personne physique qui rencontre des difficultés à effectuer cette souscription, la dénomination précise de cette personne morale et, pour ce qui concerne cette personne physique, au minimum son nom, son prénom, son adresse de résidence, lorsqu'elle en dispose, sa date de naissance et le numéro par lequel elle est identifiée, tel un numéro de registre national, ces informations leur étant transmises par cette personne morale (6°).

B.53.5. Les données visées en B.53.2.1 à B.53.4 sont, sauf disposition légale contraire, conservées « à partir de la date d'activation du service jusqu'à douze mois après la fin du service de communications électroniques » (article 127, § 4, alinéa 4).

B.54.1. Les données énumérées à l'article 127 de la loi du 13 juin 2005 ont pour objectif d'identifier les abonnés des opérateurs visés dans cette disposition. Les travaux préparatoires de la loi du 20 juillet 2022 précisent, à cet égard :

« Un principe essentiel est qu'une personne doit rendre compte de ses actes, tant sur le plan civil que pénal. L'anonymat met en péril ce principe. La possibilité d'identifier l'abonné permet de le mettre en œuvre. Il est également essentiel qu'il soit possible pour les autorités (autorités

judiciaires, services de renseignement et de sécurité et autres autorités qui peuvent demander des données de trafic ou d'identification aux opérateurs) de pouvoir retrouver l'identité de l'abonné » (*Doc. parl.*, Chambre, 2021-2022, DOC 55-2572/002, p. 71).

Dans ce cadre, l'objectif est aussi de lutter contre la fraude à l'identité (*ibid.*, pp. 96-97).

B.54.2. Comme il est dit en B.44.2, il y a lieu d'opérer, parmi les données d'identification, une distinction entre, d'une part, les adresses IP à la source et, d'autre part, les données relatives à l'identité civile des utilisateurs de moyens de communications électroniques.

B.55.1. L'article 127, § 10, alinéa 1er, 1°, de la loi du 13 juin 2005 rappelle l'obligation qui incombe aux opérateurs de conserver « l'adresse IP ayant servi à la souscription au service de communication électronique ou à son activation, l'adresse IP à la source de la connexion et les données qui doivent être conservées avec ces adresses », contenue dans l'article 126, § 1er, alinéa 1er, 4° et 15°.

B.55.2. Dès lors que, pour les motifs mentionnés en B.48.1 à B.48.4, l'article 126 de la loi du 13 juin 2005, tel qu'il a été inséré par l'article 8 de la loi du 20 juillet 2022, ne viole pas les normes de référence citées en B.49, et que les griefs présentement examinés sont en substance pris de la violation des mêmes normes de référence, il en va de même en ce qui concerne l'article 127, § 10, alinéa 1er, 1°, de la loi du 13 juin 2005.

B.55.3. Les premier et deuxième moyens dans l'affaire n° 7930 ne sont pas fondés en ce qu'ils portent sur la mesure de conservation des données mentionnées en B.55.1.

B.56. Les autres données d'identification visées à l'article 127, §§ 4, 6 à 8, et 10, de la loi du 13 juin 2005 peuvent être assimilées à des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques dès lors qu'elles ne permettent pas à elles seules de connaître la date, l'heure, la durée et les destinataires d'une communication, ni l'endroit où cette communication a eu lieu ou la fréquence de communication avec certaines personnes pendant une période donnée. La Cour européenne des droits de l'homme et la Cour de justice considèrent en effet que ces données ne fournissent aucune information sur les communications données par ces personnes ni sur leur vie privée. Ces seules données ne permettent pas d'établir

un profil de l'utilisateur ni de suivre ses mouvements (CEDH, 30 janvier 2020, *Breyer c. Allemagne*, ECLI:CE:ECHR:2020:0130JUD005000112, §§ 92-95; CJUE, grande chambre, 2 octobre 2018, C-207/16, *Ministerio Fiscal*, ECLI:EU:C:2018:788, point 62; grande chambre, 6 octobre 2020, C-511/18, C-512/18 et C-520/18, *La Quadrature du Net e.a.*, précité, point 157).

La Cour de justice en déduit que le droit au respect de la vie privée ne s'oppose pas à une collecte, à un traitement et à une conservation généralisés et indifférenciés de données d'identification d'utilisateurs de réseaux de communications électroniques aux fins de la recherche, de la détection et de la poursuite d'infractions pénales ainsi que de la sauvegarde de la sécurité publique. À cet égard, il n'est pas nécessaire qu'il s'agisse d'infractions pénales graves ni de menaces ou d'atteintes graves à la sécurité publique (CJUE, grande chambre, 6 octobre 2020, C-511/18, C-512/18 et C-520/18 précités). Par contre, il y a lieu de démontrer que « ces mesures assurent, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus » (*ibid.*, point 168).

La Cour européenne des droits de l'homme contrôle la collecte, le traitement et la conservation généralisés et indifférenciés de ces données d'identification de manière moins intensive que la collecte, le traitement et la conservation de données relatives au trafic et de données de localisation. Elle vérifie si le délai de conservation est raisonnable, compte tenu de la durée habituelle d'une enquête pénale. La Cour européenne des droits de l'homme n'exige pas qu'une supervision *a priori* soit organisée pour la collecte et la conservation de simples données d'identification : un accès *a posteriori* à une instance judiciaire ou administrative indépendante combiné aux recours de droit commun dont le prévenu dispose au cours d'un procès pénal suffit (CEDH, 30 janvier 2020, *Breyer c. Allemagne*, précité, §§ 96-107).

B.57.1. Les parties requérantes dans l'affaire n° 7932 soutiennent que la mesure prévue à l'article 127, § 10, alinéa 1er, 4°, de la loi du 13 juin 2005 dans le cas d'une carte SIM ou d'une carte équivalente insérée dans un véhicule, qui autorise la collecte et la conservation du numéro de châssis du véhicule et le lien entre ce numéro et le numéro de la carte, permet le traçage permanent de ce véhicule via la connexion internet, notamment par la combinaison de cette

donnée d'identification avec la donnée de localisation sur les autoroutes dont la conservation est autorisée en vertu de l'article 126/3, § 4, *c)*, de la loi du 13 juin 2005.

B.57.2. L'article 127, § 10, alinéa 1er, 4°, de la loi du 13 juin 2005 n'autorise ni la conservation ni la collecte des données relatives à la connexion internet des véhicules visés dans cette disposition.

En outre, il n'est pas possible, à l'aide du numéro de châssis du véhicule, du numéro de la carte SIM ou de la carte équivalente insérée dans le véhicule et du lien entre les numéros précités de suivre les déplacements, les communications, les activités ou les relations sociales d'une personne, ni d'établir un profil personnel permettant de tirer des conclusions précises sur son orientation sexuelle, ses convictions et son état de santé. En soi, les données précitées ne divulguent donc pas d'informations sensibles sur la vie privée.

Enfin, s'il est exact que ces données d'identification peuvent ensuite être associées à d'autres données et contribuer, de cette manière, à la divulgation de telles informations sensibles sur la vie privée d'une personne, ces autres données sont collectées différemment et cette collecte doit aussi s'effectuer dans le respect de la législation applicable et des droits fondamentaux de l'intéressé.

B.57.3. Le deuxième moyen dans l'affaire n° 7932, en sa quatrième branche, n'est pas fondé.

B.58.1. En ce qui concerne les griefs des parties requérantes dans l'affaire n° 7930 développés dans leurs premier et deuxième moyens, il y a lieu d'apprécier la compatibilité des mesures de collecte et de conservation des données prévues à l'article 127, §§ 6 à 8 et 10, alinéa 1er, 2° à 6°, de la loi du 13 juin 2005 avec le droit au respect de la vie privée à l'aide des critères mentionnés en B.56.

B.58.2. Il ressort des travaux préparatoires cités en B.54.1 que, par l'article 127 de la loi du 13 juin 2005, le législateur poursuivait des objectifs de recherche, de détection et de poursuite d'infractions pénales ainsi que de sauvegarde de la sécurité publique au sens de l'article 15 de la directive 2002/58/CE.

B.58.3.1. Les conditions matérielles et procédurales de la collecte, du traitement et de la conservation des données d'identification des abonnés d'un réseau de communications électroniques sont réglées aux articles 127 et 127/3 de la loi du 13 juin 2005.

B.58.3.2. L'article 127, § 1er, alinéa 1er, de la loi du 13 juin 2005 détermine les personnes qui se voient imposer des obligations dans ce cadre, à savoir les opérateurs qui fournissent aux utilisateurs finaux en Belgique un service de communications électroniques. L'article 127/3, § 3, alinéa 2, de la loi du 13 juin 2005 désigne en outre les opérateurs précités comme responsables du traitement de données. L'article 127 de la loi du 13 juin 2005 définit par ailleurs le principe selon lequel tous les abonnés doivent être identifiables et dispose que l'identification doit être effectuée au moyen d'une méthode d'identification directe ou indirecte.

B.58.3.3. L'article 127 de la loi du 13 juin 2005 établit les conditions de conservation des données collectées. Le paragraphe 6 de cette disposition énumère les documents qui sont admis pour procéder à l'identification d'une personne physique, qui agit pour une personne morale, le cas échéant.

Les paragraphes 7 et 8 précisent quelles données d'identification doivent être conservées par les opérateurs. Le paragraphe 10 de la loi du 13 juin 2005, enfin, énumère quelles données d'identification peuvent être collectées et conservées en vue de permettre aux autorités visées à l'article 127/1, § 3, alinéa 1er, d'identifier les abonnés par une méthode d'identification indirecte.

B.58.3.4. L'article 127 fixe le délai de conservation maximal des données d'identification qu'il vise. Le paragraphe 4, alinéa 4, de cette disposition prévoit que celles-ci sont conservées jusqu'à douze mois après la fin du service de communications électroniques, sauf lorsqu'une disposition légale prévoit un autre délai.

B.58.3.5. Par ailleurs, l'article 127 interdit explicitement aux points de vente de conserver des données d'identification ou des copies de documents d'identification, mais il leur incombe d'introduire directement ces données et copies dans leurs systèmes informatiques, étant entendu qu'il appartient aux opérateurs de prendre les mesures d'ordre technique et organisationnel,

adéquates et proportionnées, pour mettre en œuvre l'interdiction précitée, y compris en permettant l'introduction immédiate des données et des copies dans les systèmes informatiques (§ 4, alinéas 1er et 2). Une exception est prévue en cas de défaillance du système informatique rendant impossible l'introduction immédiate précitée. Dans ce cas, les points de vente peuvent temporairement conserver les données et les copies à condition que celles-ci soient détruites au plus tard après l'activation du service de communications électroniques (§ 4, alinéa 3).

B.58.3.6. Enfin, il est prévu que, si l'opérateur ne respecte pas les mesures imposées en vertu de l'article 127 de la loi du 13 juin 2005, il lui est interdit de fournir le service pour lequel les mesures en question n'ont pas été prises (article 127, § 12, alinéa 1er, de la loi du 13 juin 2005).

B.58.3.7. Pour le surplus, s'il est exact que l'article 127 de la loi du 13 juin 2005 ne prévoit pas de contrôle juridictionnel spécifique du traitement des données d'identification collectées et conservées en vertu de cette disposition, il y a toutefois lieu de rappeler, comme il est dit en B.56, que les recours de droit commun suffisent en matière de traitement de simples données d'identification (CEDH, 30 janvier 2020, *Breyer c. Allemagne*, précité, § 106).

Dans le cadre de la procédure pénale, le prévenu dispose à cet égard du droit d'invoquer devant les juridictions d'instruction ou devant la juridiction de jugement la nullité d'un acte d'instruction qui viole son droit au respect de la vie privée ou son droit à un procès équitable.

Par ailleurs, dans le cadre du fonctionnement des services de renseignement et de sécurité, l'intéressé dispose, en vertu de l'article 79 de la loi du 30 juillet 2018 « relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel », du droit de demander au Comité permanent R de faire rectifier ou supprimer ses données à caractère personnel inexactes et de vérifier le respect des dispositions applicables.

En outre, chaque abonné d'un service de communications électroniques dont les données d'identification ont été traitées en violation de l'article 127 de la loi du 13 juin 2005 dispose

d'une action en responsabilité de droit commun contre la personne qui a enfreint cette disposition législative.

Enfin, l'intéressé peut, en vertu de l'article 58 de la loi du 3 décembre 2017 « portant création de l'Autorité de protection des données », déposer sans frais une plainte auprès de l'Autorité de protection des données en cas de traitement illégitime de ses données à caractère personnel.

B.59. Les premier et deuxième moyens dans l'affaire n° 7930 ne sont pas fondés en ce qu'ils portent sur les données visées à l'article 127, §§ 6 à 8 et 10, alinéa 1er, 2° à 6°, de la loi du 13 juin 2005.

B.60. L'article 127, § 11, alinéa 1er, de la loi du 13 juin 2005 dispose que « sauf preuve contraire, la personne identifiée est présumée utiliser elle-même le service de communications électroniques ».

Selon les parties requérantes dans l'affaire n° 7932, cette disposition viole le droit au procès équitable, en particulier la présomption d'innocence, garantie par l'article 6 de la Convention européenne des droits de l'homme, en ce que l'utilisateur final présumé serait dans l'impossibilité de fournir la preuve contraire, en particulier lorsque cet utilisateur autorise l'accès de son réseau wifi au public ou en cas d'accès non autorisé à ce réseau.

B.61.1. Conformément à l'article 6, paragraphe 2, de la Convention européenne des droits de l'homme, toute personne accusée d'une infraction est présumée innocente jusqu'à ce que sa culpabilité ait été légalement établie.

B.61.2. Considérée comme une garantie procédurale en matière pénale, la présomption d'innocence impose des conditions concernant notamment la charge de la preuve, les présomptions légales de fait et de droit, le droit de ne pas contribuer à sa propre incrimination, la publicité pouvant être donnée à l'affaire avant la tenue du procès, la formulation par le juge du fond ou toute autre autorité publique de déclaration prématurée quant à la culpabilité d'un prévenu (CEDH, grande chambre, 12 juillet 2013, *Allen c. Royaume-Uni*, ECLI:CE:ECHR:2013:0712JUD002542409, § 93).

B.61.3. Le droit de toute personne accusée d'une infraction en matière pénale à être présumée innocente et à faire supporter au ministère public la charge de la preuve n'est toutefois pas absolu. Tout système juridique connaît en effet des présomptions de fait ou de droit. De telles présomptions ne sont en principe pas interdites, aussi longtemps qu'elles restent dans des limites raisonnables prenant en compte la gravité de l'enjeu et préservant les droits de la défense. En cas de recours à des présomptions en matière pénale, il convient donc de ménager un juste équilibre entre l'importance de ce qui se trouve en jeu et les droits de la défense. En d'autres termes, les moyens employés doivent être proportionnés au but légitime poursuivi (CEDH, décision, 19 octobre 2004, *Falk c. Pays-Bas*, ECLI:CE:ECHR:2004:1019DEC006627301; 23 juillet 2002, *Västberga Taxi Aktiebolag et Vulic c. Suède*, ECLI:CE:ECHR:2002:0723JUD003698597, § 113).

B.62.1. L'article 127, § 11, alinéa 1er, de la loi du 13 juin 2005 n'établit pas une responsabilité pénale automatique ou une responsabilité objective de l'utilisateur final d'une carte de téléphonie mobile prépayée qui a été identifiée en ce qui concerne l'utilisation qu'en fait un tiers. Il remplit principalement une fonction d'avertissement, étant donné qu'il rappelle la présomption de départ de toute enquête pénale et de toute enquête par les services de renseignement et de sécurité, à savoir la présomption selon laquelle c'est le propriétaire ou l'utilisateur habituel d'un objet qui l'a utilisé pour commettre l'infraction ou pour menacer la sécurité nationale. Les enquêteurs écartent cette présomption dès qu'elle est infirmée par les éléments de preuve recueillis.

B.62.2. La disposition attaquée est donc en rapport avec les objectifs que poursuit le législateur par l'article 127 de la loi du 13 juin 2005, mentionnés en B.54.

B.62.3. En outre, l'utilisateur final présumé dispose de plusieurs possibilités pour se défendre dans le cadre des poursuites pénales qui pourraient découler de l'utilisation du service de communications électroniques faite par un tiers. S'il fait connaître aux enquêteurs l'identité de la personne qui a utilisé ce service, ceux-ci doivent examiner l'implication de cette personne. Dans l'hypothèse où le service de communications électroniques est rendu accessible aux tiers, il appartient à l'utilisateur final présumé d'en faire part aux enquêteurs, qui doivent tenter d'identifier la personne qui a effectivement utilisé le service ainsi que son implication.

Du reste, l'article 127, § 11, alinéa 1er, de la loi du 13 juin 2005 se borne à instaurer une présomption réfragable, que le prévenu peut contester par toutes voies de droit. Il ne lui interdit pas de présenter tous les éléments de fait qui infirment son implication dans les infractions commises ou dans les menaces pour la sécurité nationale qui font l'objet d'une enquête.

Par ailleurs, la disposition précitée n'enlève rien au principe selon lequel il revient au ministère public, dans un procès pénal, de prouver la culpabilité du prévenu. Il appartient au juge répressif d'apprécier la valeur probante de tous les éléments de preuve, en ce compris les explications du prévenu, en respectant son droit à un procès équitable.

B.62.4. L'article 127, § 11, alinéa 1er, de la loi du 13 juin 2005 ne compromet pas la présomption d'innocence.

B.63. Le deuxième moyen dans l'affaire n° 7932, en sa sixième branche, n'est pas fondé.

B.64. L'article 127, § 5, alinéa 4, de la loi du 13 juin 2005 prévoit qu'aux fins d'assurer la fiabilité de l'identification de l'abonné qui est une personne physique et d'éviter les fraudes à l'identité, l'opérateur ou le point de vente peut réaliser, de manière automatique, une comparaison entre les paramètres biométriques présents sur la photo du document d'identification de l'abonné, d'une part, et ceux de son visage, d'autre part.

Selon les parties requérantes dans l'affaire n° 7932, cette disposition autorise le recours à une technologie de reconnaissance faciale qui viole le droit au respect de la vie privée et à la protection des données à caractère personnel, tel qu'il est notamment garanti par le RGPD, en ce que cette mesure ne serait ni nécessaire, ni proportionnée, et ne respecterait pas non plus l'exigence du consentement explicite et informé de l'abonné concerné.

B.65.1. Le droit au respect de la vie privée n'est pas absolu. L'article 22 de la Constitution et l'article 8 de la Convention européenne des droits de l'homme n'excluent pas une ingérence d'une autorité publique dans l'exercice de ce droit, pourvu que cette ingérence soit prévue par une disposition législative suffisamment précise, qu'elle réponde à un besoin social impérieux

dans une société démocratique et qu'elle soit proportionnée à l'objectif légitime qu'elle poursuit.

Le législateur dispose en la matière d'une marge d'appréciation. Cette marge n'est toutefois pas illimitée : pour qu'une norme soit compatible avec le droit au respect de la vie privée, il faut que le législateur ait établi un juste équilibre entre tous les droits et intérêts en cause.

B.65.2. En outre, comme il est dit en B.11.2, les articles 7 et 8 de la Charte ont, en ce qui concerne le traitement des données à caractère personnel, une portée analogue à celle de l'article 8 de la Convention européenne des droits de l'homme.

B.66.1. L'article 5 du RGPD édicte les principes relatifs au traitement des données à caractère personnel :

« 1. Les données à caractère personnel doivent être :

a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence);

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités);

c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données);

d) exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude);

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation);

f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité);

2. Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité) ».

L'article 9 du RGPD concerne le traitement portant sur des catégories particulières de données à caractère personnel :

« 1. Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits.

2. Le paragraphe 1 ne s'applique pas si l'une des conditions suivantes est remplie :

a) la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne concernée;

[...]

g) le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée;

[...] ».

L'article 9 du RGPD doit être lu en combinaison avec l'article 4, point 14), du RGPD, qui dispose :

« Aux fins du présent règlement, on entend par :

[...]

14) ' données biométriques ', les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou

comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques ».

B.66.2. L'article 9, paragraphe 2, *g)*, du RGPD permet le traitement des données à caractère personnel sensibles, telles les données biométriques, lorsqu'il est « nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée ».

B.67.1. Il ressort des travaux préparatoires de l'article 127, § 5, alinéa 4, de la loi du 13 juin 2005 que cette disposition vise à permettre l'identification la plus efficace possible des individus, notamment en vue de renforcer la lutte contre la fraude à l'identité tant de la part des abonnés que des points de vente eux-mêmes (*Doc. parl.*, Chambre, 2021-2022, DOC 55-2572/002, pp. 90-91).

B.67.2. Par l'arrêt n° 2/2021 du 14 janvier 2021 (ECLI:BE:GHCC:2021:ARR.002), la Cour a jugé que les objectifs précités sont légitimes, dès lors qu'ils visent à protéger les droits et les libertés d'autrui, qu'ils constituent par ailleurs des objectifs d'intérêt général reconnus par l'Union européenne et qu'ils peuvent également être considérés comme des motifs d'intérêt public important, au sens de l'article 9, paragraphe 2, *g)*, du RGPD (B.20.2).

B.68. L'article 127, § 5, alinéa 4, de la loi du 13 juin 2005 est pertinent en vue de la réalisation des objectifs poursuivis, dès lors que la comparaison des paramètres biométriques de la photo du document d'identification et de ceux du visage de l'abonné est susceptible, d'une part, de faciliter la tâche des opérateurs de mettre tout en œuvre pour assurer la fiabilité de l'identification de l'abonné qui est une personne physique et, d'autre part, de prévenir l'utilisation frauduleuse des documents d'identification visés.

L'éventuelle non-fiabilité totale du procédé et l'impossibilité corrélative d'exclure la non-détection de certains cas de fraude à la ressemblance ne conduisent pas à une conclusion différente.

B.69. La mesure de comparaison faciale attaquée est par ailleurs prévue par une disposition législative suffisamment précise, dès lors que l'article 127, § 5, alinéa 4, de la loi du 13 juin 2005 détermine les données qui font l'objet de la mesure litigieuse, à savoir les paramètres biométriques sur la photo des documents d'identification visés à l'article 127, § 6, de cette loi et ceux du visage de l'abonné, qu'il est interdit de conserver les données biométriques précitées au-delà du procédé de comparaison, que les données sont lisibles exclusivement de manière électronique et que seuls les opérateurs et les points de vente au sens de l'article 127 précité sont autorisés à lire ces données.

De la sorte, les abonnés visés par cette disposition peuvent connaître de manière suffisamment précise les conditions dans lesquelles les données biométriques précitées sont traitées.

B.70. La Cour examine maintenant la nécessité et la proportionnalité de l'ingérence.

B.71.1. Dans le cadre de l'examen de la nécessité, il y a lieu de vérifier si l'ingérence ne va pas au-delà de ce qui est nécessaire à la réalisation des objectifs poursuivis, et en particulier s'il existe des mesures qui sont moins attentatoires aux droits concernés, tout en contribuant de manière efficace au but de la réglementation en cause (CJUE, 17 octobre 2013, C-291/12, *Schwarz c. Stadt Bochum*, ECLI:EU:C:2013:670, points 46 et 47).

B.71.2. Il ressort des travaux préparatoires de la disposition attaquée que le législateur a estimé que la mesure de comparaison faciale prévue à l'article 127, § 5, alinéa 4, de la loi du 13 juin 2005 était nécessaire à la réalisation des objectifs mentionnés en B.67.1 :

« La méthode de comparaison faciale est une bonne méthode pour atteindre les finalités visées par le gouvernement.

Avec cette méthode de reconnaissance faciale, les opérateurs peuvent réduire l'usurpation d'identité. Cette méthode permet aussi de ne pas faire intervenir les points de vente, qui sont les ' maillons faibles ' en matière de fiabilité de l'identification de l'abonné. Cette augmentation de la fiabilité de l'identification est bénéfique pour les autorités, pour les opérateurs, qui sont victimes des fraudes (d'où l'intérêt de plusieurs opérateurs de mettre en œuvre cette méthode) et pour l'abonné (éviter un détournement de son identité). Même si une personne parvient à s'identifier avec un faux document d'identification, la copie de ce document d'identification autre que la carte d'identité électronique belge comprendra une photo correcte de l'abonné, ce qui pourrait permettre aux autorités de démarrer une enquête.

La méthode de comparaison faciale permet aux opérateurs de répondre à leur obligation d'effectuer une identification fiable de l'abonné et de s'adapter aux besoins des abonnés (voir infra).

Il s'agit d'une méthode acceptable du point de vue de la vie privée, dès lors que les données de biométrie du visage ne sont pas conservées. Comme déjà indiqué, cela permet de ne pas faire intervenir les points de vente, qui sont parfois eux-mêmes à l'origine de fraude (ex. réutilisation frauduleuse de données d'identification d'une personne pour identifier une autre personne).

Cela permet aussi d'augmenter les possibilités pour un abonné de s'identifier et de faciliter son identification, en particulier pour les identifications en ligne. Pour de nombreux utilisateurs qui maîtrisent la technologie, c'est devenu une habitude quotidienne. La comparaison des paramètres biométriques d'un selfie et de la photo sur un document d'identité offre de nouvelles possibilités d'identification fiable. Cette solution en particulier peut fortement faciliter l'identification de clients, surtout en cas d'identification par smartphone, où l'utilisation du lecteur d'eID belge n'est pas possible » (*Doc. parl.*, Chambre, 2021-2022, DOC 55-2572/002, pp. 90-91).

B.71.3. À cet égard, le législateur a souhaité établir un système permettant une réponse appropriée à chaque cas particulier, notamment celui des résidents non belges sans carte d'identité électronique, celui des étrangers en visite en Belgique ou encore celui des personnes moins familiarisées avec le monde numérique. Dans cette perspective, les travaux préparatoires de la loi du 20 juillet 2022 précisent que « l'identification sur la base de la comparaison faciale est complémentaire et constitue un complément nécessaire aux méthodes existantes » (*ibid.*, p. 84).

B.72.1. En ce qui concerne la proportionnalité de la mesure, l'article 127, § 5, alinéa 4, de la loi du 13 juin 2005 établit lui-même plusieurs garanties au profit de l'abonné concerné par la mesure de comparaison faciale.

L'outil de comparaison doit être autorisé par le ministre compétent pour les matières relatives aux communications électroniques et par le ministre de la Justice, après vérification de ce que l'outil assure la fiabilité de l'identification, en tenant compte du risque de fraude à l'identité (1°).

Par ailleurs, l'opérateur propose à l'abonné au moins une autre manière de s'identifier (2°), de sorte que l'abonné ne peut jamais être contraint de recourir à la méthode de reconnaissance faciale afin de souscrire à un service de communications électroniques.

Ensuite, l'abonné doit donner son consentement explicite au sens de l'article 4, point 11), du RGPD (3°), étant entendu que, contrairement à ce que prétendent les parties requérantes, l'article 9, paragraphe 2, *a)*, du RGPD n'exige pas que ce consentement soit écrit.

Enfin, il est interdit aux opérateurs et aux points de vente de communiquer à un tiers les données biométriques traitées ou de les traiter à d'autres fins que l'identification des abonnés (4°).

B.72.2. Pour le surplus, il n'apparaît pas que la mesure attaquée affecterait le contenu essentiel du droit au respect de la vie privée et du droit à la protection des données à caractère personnel.

B.73. Le deuxième moyen dans l'affaire n° 7932, en sa troisième branche, n'est pas fondé.

7. La conservation ciblée des données sur la base d'un critère géographique (articles 9 à 11)

B.74.1. Les premier, deuxième et troisième moyens dans l'affaire n° 7930, le moyen unique dans l'affaire n° 7931 et la troisième branche du premier moyen dans l'affaire n° 7932 portent sur la mesure de conservation ciblée des données de trafic et de localisation, prévue aux articles 9, 10 et 11 de la loi du 20 juillet 2022.

B.74.2. L'article 9 de la loi du 20 juillet 2022 insère, dans la loi du 13 juin 2005, un article 126/1, qui dispose :

« § 1er. Sans préjudice du RGPD et de la loi du 30 juillet 2018, les opérateurs qui offrent aux utilisateurs finaux des services de communications électroniques, ainsi que les opérateurs fournissant les réseaux de communications électroniques sous-jacents, conservent les données visées à l'article 126/2, § 2, pour les zones géographiques visées à l'article 126/3, pendant douze mois à partir de la date de la communication, sauf si une autre durée est fixée dans l'article 126/3.

Chaque opérateur conserve les données qu'il a générées ou traitées dans le cadre de la fourniture des services et réseaux de communications électroniques concernés.

Ces données sont conservées aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave, de la prévention de menaces graves contre la sécurité publique, et de la sauvegarde des intérêts vitaux d'une personne physique.

§ 2. Les métadonnées de communications électroniques, en ce compris les métadonnées pour les appels infructueux, auxquelles s'applique l'obligation de conservation visée au paragraphe 1er, sont énumérées à l'article 126/2, § 2.

§ 3. Les opérateurs conservent les données de trafic pour toutes les communications ou appels infructueux effectués à partir d'une zone géographique visée à l'article 126/3 ou vers une telle zone.

Lorsque, compte tenu de la technologie utilisée par l'opérateur, celui-ci n'est pas en mesure de localiser l'équipement terminal ayant participé à la communication, y compris l'appel infructueux, de façon plus précise que sa localisation sur le territoire national, l'opérateur conserve les données visées à l'article 126/2, § 2, pour la durée la plus courte fixée en exécution du présent article et de l'article 126/3, à la condition qu'en exécution du présent article et de l'article 126/3 l'ensemble du territoire national soit soumis à une obligation de conservation. Lorsque cette condition n'est pas remplie, l'opérateur concerné par le présent alinéa ne conserve pas ces données.

Lorsque l'utilisateur final se déplace pendant une communication électronique, l'opérateur conserve les données de trafic pour autant que l'utilisateur final se trouve à un moment de la communication dans une zone visée à l'article 126/3.

Les opérateurs conservent les données relatives à 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, énumérées à l'article 126/2, § 2, lorsque cet équipement se trouve dans une zone visée à l'article 126/3.

Pour déterminer si l'équipement terminal se trouve dans une zone géographique visée à l'article 126/3, les opérateurs utilisent les données les plus fiables et précises possibles. Ils utilisent, si disponible à cet effet, la localisation satellitaire d'un équipement terminal.

Lorsque la technologie utilisée par l'opérateur ne permet pas de limiter la conservation de données à une zone visée à l'article 126/3, il conserve les données nécessaires pour couvrir la totalité de la zone concernée tout en limitant la conservation de données en dehors de cette zone au strict nécessaire au regard de ses possibilités techniques.

Lorsqu'un point d'agrégation de l'opérateur, telle une antenne, couvre plusieurs zones géographiques visées à l'article 126/3 qui sont soumises à des durées de conservation différentes, l'opérateur conserve les données pour ce point d'agrégation pendant la durée de conservation la plus courte.

Lorsqu'en application du présent article et de l'article 126/3, différentes durées de conservation sont applicables aux mêmes données, les opérateurs conservent les données pendant la durée la plus courte.

§ 4. Le Roi peut fixer, par arrêté délibéré en Conseil des ministres, sur proposition du ministre de la Justice, du ministre de l'Intérieur, du ministre de la Défense, et du ministre, et après avis des autorités de protection des données compétentes et de l'Institut, les éléments suivants :

- les paramètres techniques et les données que les opérateurs utilisent pour limiter la conservation de données aux zones visées à l'article 126/3;

- la liste des différentes autorités compétentes dans les matières visées à l'article 126/3, §§ 2 à 5;

- les modalités de communication des informations par les autorités compétentes au service désigné par le Roi, les modalités de communication des informations par ce service vers les opérateurs concernés, ainsi que le délai dans lequel les opérateurs mettent en œuvre annuellement la conservation visée au paragraphe 1er;

- s'il échet, les zones géographiques additionnelles visées à l'article 126/3, § 3, *m)*, § 4, *g)*, et § 5, *f)*.

L'arrêté royal visé à l'alinéa 1er, quatrième tiret, est renouvelé tous les trois ans. En l'absence de renouvellement, l'obligation de conservation visée au paragraphe 1er en ce qui concerne ces zones géographiques additionnelles cesse de s'appliquer, et ce jusqu'à l'entrée en vigueur d'un nouvel arrêté royal.

§ 5. Le ministre de la Justice, le ministre de l'Intérieur, le ministre de la Défense et le ministre présentent annuellement, après avis préalable du Comité de coordination du Renseignement et de la Sécurité, et de l'Institut et des autorités de protection des données compétentes, un rapport d'évaluation à la Chambre des représentants, sur la mise en œuvre du présent article et, le cas échéant, de l'arrêté royal visé au paragraphe 4, afin de vérifier si des dispositions doivent être adaptées.

Ce rapport d'évaluation examine en particulier si les catégories de zones géographiques énumérées dans la loi et dans l'arrêté royal visé au paragraphe 4 répondent toujours aux critères visés à l'article 126/3, §§ 3 à 5, et s'il est nécessaire de les maintenir ou si d'autres doivent être incluses.

Des catégories de zones géographiques ne peuvent être incluses que dans le but de sauvegarder la sécurité nationale ou s'il peut être établi, sur la base d'éléments objectifs et non discriminatoires, qu'il existe dans ces zones une situation présentant un risque élevé de préparation ou de commission d'actes criminels graves.

Le rapport d'évaluation comprend également le pourcentage du territoire national auquel s'applique l'obligation de conservation des données en vertu du présent article et de l'article 126/3.

Ce rapport d'évaluation est envoyé à l'Organe de contrôle de l'information policière et au Comité permanent R ».

B.74.3. L'article 10 de la loi du 20 juillet 2022 insère, dans la loi du 13 juin 2005, un article 126/2, qui dispose :

« § 1er. Pour l'application du présent article, il y a lieu d'entendre par ' communication ', toute information échangée ou acheminée entre un nombre fini de parties au moyen d'un service de communications électroniques accessible au public, à l'exclusion des informations qui sont acheminées dans le cadre d'un service de radiodiffusion au public par l'intermédiaire d'un réseau de communications électroniques, sauf dans la mesure où un lien peut être établi entre l'information et l'abonné ou utilisateur identifiable qui la reçoit.

§ 2. Les données visées à l'article 126/1, § 2, qui doivent être conservées en exécution des articles 126/1 et 126/3 par les opérateurs qui offrent aux utilisateurs finaux des services de communications électroniques, ainsi que par les opérateurs fournissant les réseaux de communications électroniques sous-jacents qui permettent la fourniture de ces services, sont les suivantes :

1° la description et les caractéristiques techniques du service de communications électroniques utilisé lors de la communication;

2° les données d'identification visées à l'article 126, § 1er, 2°, 10° à 14°, et 16°, du destinataire de la communication;

3° pour les services de communications électroniques à l'exception des services d'accès à Internet, l'adresse IP utilisée par le destinataire de la communication, l'horodatage ainsi que, en cas d'utilisation partagée d'une adresse IP du destinataire, les ports qui lui ont été attribués;

4° en cas d'appel multiple, de déviation ou de renvoi, l'identification de toutes les lignes en ce compris celles vers lesquelles l'appel a été transféré;

5° la date et l'heure exacte du début et de la fin de la session du service de communications électroniques concerné, en ce compris la date et l'heure exacte du début et de la fin de l'appel;

6° les données permettant d'identifier et de localiser les cellules ou d'autres points de terminaison du réseau mobile, qui ont été utilisées pour effectuer la communication, du début

jusqu'à la fin de la communication, ainsi que les dates et heures précises de ces différentes localisations;

7° le volume de données envoyées vers le réseau et téléchargées pendant la durée de la session;

8° pour ce qui concerne les services de communications électroniques mobiles, la date et l'heure de la connexion de l'équipement terminal au réseau en raison du démarrage de cet équipement et le moment de la déconnexion de cet équipement terminal au réseau en raison de l'extinction de cet équipement;

9° pour ce qui concerne les services de communications électroniques mobiles, la localisation de l'équipement terminal et la date et l'heure de cette localisation chaque fois que l'opérateur cherche à connaître quels équipements terminaux sont connectés à son réseau;

10° les autres identifiants relatifs au destinataire de la communication électronique, à son équipement terminal ou à l'équipement le plus proche de cet équipement terminal, qui résultent de l'évolution technologique et qui sont déterminés par le Roi, après avis de l'Autorité de protection des données et de l'Institut, pour autant que cet arrêté soit confirmé par la loi dans les six mois suivant la publication de cet arrêté.

Par dérogation aux articles 126/1 et 126/3, la durée de conservation de la donnée visée à l'alinéa 1er, 8°, est de six mois après avoir été générée ou traitée.

L'arrêté royal visé à l'alinéa 1er, 10°, ne porte pas sur le contenu des communications électroniques.

Le Roi peut, après avis de l'Autorité de protection des données et de l'Institut, préciser les données visées à l'alinéa 1er.

§ 3. La combinaison des données conservées en exécution de l'article 126 et du présent article doit permettre d'établir la relation entre l'origine de la communication et sa destination.

Le Roi peut fixer, par arrêté délibéré en Conseil des ministres, sur proposition du ministre de la Justice, du ministre de l'Intérieur, du ministre de la Défense, et du ministre, après avis des autorités de protection des données compétentes et de l'Institut, les exigences en matière de précision et de fiabilité auxquelles les données visées au présent article doivent répondre ».

B.74.4. L'article 11 de la loi du 20 juillet 2022 insère, dans la loi du 13 juin 2005, un article 126/3, qui dispose :

« § 1er. Les données visées à l'article 126/2, § 2, sont conservées dans la zone géographique composée des :

- arrondissements judiciaires dans lesquels au moins trois infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par 1 000 habitants par an ont été constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;

- zones de police dans lesquelles au moins trois infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par 1 000 habitants par an ont été constatées sur une moyenne des trois années calendriers qui précèdent celle en cours, et situées dans les arrondissements judiciaires dans lesquels pendant l'année calendrier qui précède celle en cours, moins de trois infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par 1 000 habitants par an sur une moyenne de trois années calendriers qui précèdent celle en cours ont été constatées.

Dans l'hypothèse visée à l'alinéa 1er, premier tiret, le délai de conservation des données visées à l'article 126/2, § 2, est de :

a) six mois, s'il y a trois ou quatre infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;

b) neuf mois, s'il y a cinq ou six infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;

c) douze mois, s'il y a sept ou plus de sept infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours.

Dans l'hypothèse visée à l'alinéa 1er, deuxième tiret, le délai de conservation des données visées à l'article 126/2, § 2, est de :

a) six mois, s'il y a trois ou quatre infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;

b) neuf mois, s'il y a cinq ou six infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;

c) douze mois, s'il y a sept ou plus de sept infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours.

Le nombre d'infractions ainsi déterminé est arrondi à l'unité supérieure ou inférieure, selon que le chiffre de la première décimale atteint ou non cinq.

Les statistiques relatives au nombre d'infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours sont issues de la Banque de données Nationale Générale visée à l'article 44/7 de la loi du 5 août 1992 sur la fonction de police.

Les périmètres des arrondissements judiciaires visés à l'alinéa 1er, premier tiret, sont fixés par l'article 4 de l'annexe au Code judiciaire.

Les périmètres des zones de police visées à l'alinéa 1er, deuxième tiret, sont ceux fixés à l'annexe de l'arrêté royal du 24 octobre 2001 portant la dénomination des zones de police.

La direction, visée à l'article 44/11 de la loi du 5 août 1992 sur la fonction de police, envoie les statistiques relatives au nombre d'infractions et la durée de conservation pour chaque arrondissement judiciaire et chaque zone de police à l'Organe de contrôle de l'information policière, qui, dans le mois, après que toutes les données nécessaires à cette fin lui aient été communiquées, procède à leur validation. L'Organe de contrôle peut exercer, aux fins de cette validation, toutes ses compétences octroyées par le titre 7 de la loi du 30 juillet 2018.

Les statistiques et les durées de conservation sont transmises par la direction visée à l'article 44/11 de la loi du 5 août 1992 sur la fonction de police au service désigné par le Roi, uniquement après avoir été informé de leur validation par l'Organe de contrôle.

Sur proposition du service désigné par le Roi, chaque année, les ministres de la Justice et de l'Intérieur adoptent la liste des arrondissements judiciaires et des zones de police soumises à l'obligation de conservation de données ainsi que leur durée de conservation.

Après cette adoption, le service désigné par le Roi transmet la liste des arrondissements judiciaires et des zones de police soumises à l'obligation de conservation de données, ainsi que leur durée de conservation, aux opérateurs.

§ 2. Les données visées à l'article 126/2, § 2, sont conservées dans les zones géographiques déterminées par l'Organe de coordination pour l'analyse de la menace, dont le niveau de la menace, déterminé par l'évaluation visée à l'article 8, 1° et 2°, de la loi du 10 juillet 2006 relative à l'analyse de la menace, est au moins de niveau 3, conformément à l'article 11 de l'arrêté royal du 28 novembre 2006 portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace, et, aussi longtemps que le niveau de la menace d'au moins niveau 3 perdure pour ces zones.

Si le niveau de la menace est au moins de niveau 3 et couvre l'ensemble du territoire, l'Organe de coordination pour l'analyse de la menace informe immédiatement le service désigné par le Roi afin que ce service prenne les mesures nécessaires pour informer les opérateurs et procéder à une conservation générale et indifférenciée des données visées à l'article 126/2, § 2, sur l'ensemble du territoire.

L'obligation de conservation visée à l'alinéa 2 est confirmée par arrêté royal, sur proposition conjointe du ministre de l'Intérieur et du ministre de la Justice. En l'absence de confirmation par arrêté royal, publié dans le mois de la décision visée à l'alinéa 2, la conservation de données prend fin et les opérateurs en sont avertis par le service désigné par le Roi le plus rapidement possible. Après cette notification, les opérateurs suppriment les données qui ont déjà été conservées à cette fin.

§ 3. Les données visées à l'article 126/2, § 2, sont conservées dans les zones particulièrement exposées à des menaces pour la sécurité nationale ou à la commission d'actes de criminalité grave, à savoir :

a) les installations portuaires, les ports et les zones de sûreté portuaire visées à l'article 2.5.2.2, 3° à 5°, du Code de la Navigation belge;

b) les gares au sens de l'article 2, 5°, de la loi du 27 avril 2018 sur la police des chemins de fer;

c) les stations de métro et de pré-métro;

d) les aéroports au sens de l'article 2, point 1), de la directive 2009/12/CE du Parlement européen et du Conseil du 11 mars 2009 sur les redevances aéroportuaires, y compris les aéroports du réseau central énumérés à l'annexe II, section II, du règlement (UE) n° 1315/2013 du Parlement européen et du Conseil du 11 décembre 2013 sur les orientations de l'Union pour le développement du réseau transeuropéen de transport et abrogeant la décision n° 661/2010/UE, et les entités exploitant les installations annexes se trouvant dans les aéroports;

e) les bâtiments affectés à l'administration des douanes et accises;

f) les prisons au sens de l'article 2, 15°, de la loi de principes du 12 janvier 2005 concernant l'administration pénitentiaire ainsi que le statut juridique des détenus, les centres communautaires pour mineurs ayant commis un fait qualifié infraction, visés à l'article 606 du Code d'instruction criminelle, et les centres de psychiatrie légale, visés à l'article 3, 4°, *c)*, de la loi du 5 mai 2014 relative à l'internement;

g) les armuriers et les stands de tir au sens de l'article 2, 1° et 19°, de la loi du 8 juin 2006 réglant des activités économiques et individuelles avec des armes;

h) les établissements visés à l'article 3.1.*a)*, de l'arrêté royal du 20 juillet 2001 portant règlement général de la protection de la population, des travailleurs et de l'environnement contre le danger des rayonnements ionisants;

i) les établissements visés à l'article 2, 1°, de l'accord de coopération du 16 février 2016 entre l'État fédéral, la Région flamande, la Région wallonne et la Région de Bruxelles-Capitale concernant la maîtrise des dangers liés aux accidents majeurs impliquant des substances dangereuses;

j) les communes dans lesquelles il y a un ou plusieurs éléments critiques du réseau ou une ou plusieurs infrastructures critiques, visés dans la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques et ses arrêtés d'exécution; lorsque l'ensemble du réseau a été identifié comme infrastructure critique, seuls les éléments critiques du réseau sont pris en compte pour l'application du présent article;

k) le siège de la SA Astrid et les bâtiments où sont situés ses centres de données centraux et provinciaux ainsi que les bâtiments où sont situés les centres de données centraux et les nœuds de communication du système de communication et d'informations sécurisé et crypté

visé à l'article 11, § 7, de l'arrêté royal du 28 novembre 2006 portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace;

l) les systèmes de réseau et d'information qui soutiennent la fourniture des services essentiels des fournisseurs de service essentiels désignés sur la base de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique;

m) le cas échéant, sans préjudice de l'article 126/1, § 5, alinéa 3, les autres zones particulièrement exposées à des menaces pour la sécurité nationale ou à la commission d'actes de criminalité grave fixées par arrêté royal.

§ 4. Les données visées à l'article 126/2, § 2, sont conservées dans les zones où il y a une menace grave potentielle pour les intérêts vitaux du pays ou pour les besoins essentiels de la population, à savoir :

a) en matière d'ordre public, les zones neutres au sens de l'article 3 de la loi du 2 mars 1954 tendant à prévenir et réprimer les atteintes au libre exercice des pouvoirs souverains établis par la Constitution, et les organes stratégiques ministériels;

b) pour ce qui concerne le potentiel scientifique et économique, les bâtiments affectés aux personnes morales dont le potentiel économique et/ou scientifique doit être protégé et repris sur une liste établie annuellement par la Sûreté de l'État et le Service général du Renseignement et de la Sécurité sur proposition du ministre de la Justice et du ministre de la Défense et approuvée par le Conseil national de sécurité;

c) pour le transport, les autoroutes et les parkings publics attenants;

d) pour ce qui concerne la souveraineté nationale et les institutions établies par la Constitution et les lois, les décrets ou les ordonnances :

i) les assemblées législatives visées à l'article 1er de la loi du 2 mars 1954 tendant à prévenir et réprimer les atteintes au libre exercice des pouvoirs souverains établis par la Constitution;

ii) les maisons communales et les hôtels de ville;

iii) le palais royal;

iv) les domaines royaux;

v) les bâtiments affectés aux institutions visées au titre III, chapitres 5 à 7, de la Constitution;

vi) les communes dans lesquelles se trouvent des domaines militaires;

vii) les bâtiments affectés à la police locale, à la police fédérale, ainsi qu'à la Sûreté de l'État;

e) pour ce qui concerne l'intégrité du territoire national, les communes frontalières;

f) pour ce qui concerne les intérêts économiques ou financiers importants, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale :

i) les hôpitaux visés à l'article 2 de la loi coordonnée du 10 juillet 2008 sur les hôpitaux et autres établissements de soins;

ii) la Banque nationale de Belgique;

g) le cas échéant, et sans préjudice de l'article 126/1, § 5, alinéa 3, les autres zones où il y a une menace grave potentielle pour les intérêts vitaux du pays ou pour les besoins essentiels de la population fixées par arrêté royal.

§ 5. Les données visées à l'article 126/2, § 2, sont conservées dans les zones où il y a une menace potentielle grave pour les intérêts des institutions internationales établies sur le territoire national, à savoir :

a) les ambassades et les représentations diplomatiques;

b) les bâtiments affectés à l'Union européenne;

c) les bâtiments et infrastructures affectés à l'OTAN;

d) les institutions de l'Espace économique européen;

e) les institutions des Nations Unies;

f) le cas échéant, et sans préjudice de l'article 126/1, § 5, alinéa 3, les autres zones où il y a une menace potentielle grave pour les intérêts des institutions internationales établies sur le territoire national fixées par arrêté royal.

§ 6. Pour chaque catégorie de zone visée aux paragraphes 3 à 5, le Roi détermine l'étendue du périmètre de la zone.

Chaque autorité compétente dans l'une des matières visées aux paragraphes 3 à 5, transmet chaque année à la date déterminée par le Roi, uniquement au service désigné par le Roi, les informations nécessaires à la détermination concrète des zones géographiques.

Ces autorités informent sans délai uniquement ce service lorsqu'une zone géographique ne correspond plus au critère concerné afin qu'il soit mis fin le plus rapidement possible à l'obligation de conservation visée à l'article 126/1, § 1er, dans cette zone.

À l'exception de la liste des lieux visés au paragraphe 4, *b)*, mise exclusivement à la disposition du Comité permanent R par les services de renseignement et de sécurité, le service désigné par le Roi tient à la disposition de l'Organe de contrôle de l'information policière et du Comité permanent R, chacun dans le cadre de ses compétences, la liste actualisée des zones visées aux paragraphes 3 à 5, où une conservation de données est obligatoire.

L'Organe de contrôle de l'information policière et le Comité permanent R peuvent, chacun dans le cadre de ses compétences, formuler des recommandations à l'égard de cette liste ou ordonner de manière motivée que certaines zones géographiques visées aux paragraphes 3 à 5 soient retirées de la liste.

Sur proposition du service désigné par le Roi, chaque année et lors de chaque modification visée à l'alinéa 5, le ministre de la Défense, le ministre de la Justice et le ministre de l'Intérieur adoptent la liste des zones géographiques soumises à l'obligation de conservation des données ainsi que leur durée de conservation.

L'arrêté ministériel visé à l'alinéa 6 est publié par voie de mention au *Moniteur belge*.

Après cette approbation, le service désigné par le Roi transmet la liste des zones géographiques soumises à l'obligation de conservation des données, ainsi que leur durée de conservation, aux opérateurs.

Toute personne qui, du chef de sa fonction, a connaissance des données communiquées par les autorités compétentes au service désigné par le Roi ou de la liste des zones géographiques soumises à l'obligation de conservation des données, ou prête son concours à la mise en œuvre du présent article, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal ».

B.75.1. La partie requérante dans l'affaire n° 7930 prend les premier, deuxième et troisième moyens de la violation des articles 11, 12, 22 et 29 de la Constitution, de l'article 15, paragraphe 1, et des articles 5, 6 et 9 de la directive 2002/58/CE, lus à la lumière des articles 7, 8, 11, 47 et 52, paragraphe 1, de la Charte, des articles 6, 8, 10, 11 et 18 de la Convention européenne des droits de l'homme et des articles 13 et 54 de la directive (UE) 2016/680. Selon elle, les articles 9 à 11 de la loi du 20 juillet 2022 instaurent une obligation généralisée de conservation des données de communication, sans que cette conservation s'avère nécessaire ni strictement limitée au regard du but poursuivi. Elle soutient que l'article 9 se contredit en ce qui concerne les finalités de conservation qu'il énumère. Par ailleurs, en ce qui concerne l'article 11, elle affirme que cette disposition autorise *de facto* une conservation sur l'ensemble du territoire belge, que la conservation des données dans le cadre de la sécurité nationale sur la base du niveau de la menace déterminé par l'OCAM ne fait pas l'objet d'un contrôle indépendant et que ce niveau n'atteint pas le seuil exigé par la Cour de justice, que les délais de conservation prévus ne sont pas limités au strict nécessaire, que le système de zones déterminées sur la base du taux d'infractions n'est ni pertinent ni proportionné, notamment en ce qui concerne la notion de « criminalité grave » et le système de statistique retenu, et, enfin, que les zones spécifiques visées couvrent en réalité l'ensemble du territoire belge. La partie

requérante dénonce aussi la circonstance que le périmètre des zones est fixé par le Roi, ce qui violerait le principe de la légalité formelle.

B.75.2. La partie requérante dans l'affaire n° 7931 prend un moyen unique de la violation des articles 11, 12, 22 et 29 de la Constitution, lus en combinaison ou non avec les articles 7, 8, 11, 47 et 52, paragraphe 1, de la Charte, avec l'article 8 de la Convention européenne des droits de l'homme, avec les articles 5, 6 et 15 de la directive 2002/58/CE et avec les articles 13 et 54 de la directive (UE) 2016/680.

En ce qui concerne les zones caractérisées par un taux important de criminalité grave, la partie requérante soutient que les articles 9 à 11 de la loi du 20 juillet 2022 prévoient la conservation des données durant une période qui ne satisfait pas au principe de nécessité et qu'ils visent certaines infractions qui relèvent de la criminalité ordinaire. À titre subsidiaire, la partie requérante demande de poser une question préjudicielle à ce sujet à la Cour de justice. Elle ajoute que les statistiques retenues renvoient à la qualification des faits en début d'enquête et non aux infractions aboutissant à une condamnation pénale, ce qui ne serait pas pertinent, et qu'il revient au Roi de fixer le périmètre de la zone, ce qui ne serait pas compatible avec le principe de la légalité formelle.

En ce qui concerne les zones caractérisées par une menace pour la sécurité nationale, la partie requérante conteste le niveau de menace retenu, qui ne serait pas conforme aux exigences de la Cour de justice, et la circonstance que des données puissent être conservées à d'autres fins que celles de la sauvegarde de la sécurité nationale. La partie requérante dénonce également l'absence de contrôle effectif exercé par une autorité indépendante ainsi que la possibilité, pour le Roi, de fixer le périmètre des zones et de compléter la liste des zones, ce qui ne serait pas compatible avec le principe de la légalité formelle.

En ce qui concerne les mesures qui peuvent être prises par les opérateurs, la partie requérante estime que l'article 9 de la loi du 20 juillet 2022 autorise une conservation plus étendue des données lorsque l'opérateur n'est pas en mesure de déterminer la localisation des utilisateurs ou de limiter la conservation à la zone concernée, ce qui ne serait pas proportionné.

B.75.3. Les parties requérantes dans l'affaire n° 7932 prennent le premier moyen de la violation des articles 10, 11, 13, 15, 22, 23 et 29 de la Constitution, lus en combinaison ou non avec les articles 5, 6, 8, 9, 10, 11, 14 et 18 de la Convention européenne des droits de l'homme, avec les articles 7, 8, 11, 47 et 52 de la Charte, avec l'article 5, paragraphe 4, du Traité sur l'Union européenne, ainsi qu'avec l'article 6 de la directive 2002/58/CE, avec la directive (UE) 2016/680 et avec le RGPD.

Dans la troisième branche de ce moyen, les parties requérantes soutiennent que les mesures de conservation des données prévues aux articles 9, 10 et 11 de la loi du 20 juillet 2022 entraînent *de facto* la conservation indifférenciée des données. À cet égard, elles relèvent que ces dispositions n'opèrent pas une distinction entre les finalités qu'elles poursuivent, contrairement à ce qui est exigé par la Cour de justice. Les parties requérantes soutiennent par ailleurs que le délai de conservation des données prévu dans les dispositions attaquées est disproportionné et que ces dispositions autorisent une conservation en dehors de la zone géographique concernée. En outre, elles affirment que les différentes zones géographiques énumérées à l'article 11 de la loi du 20 juillet 2022 sont trop larges et ne respectent pas le principe de nécessité. Elles dénoncent également l'absence de recours effectif organisé contre la mesure de conservation prévue aux articles 9 à 11 de la loi du 20 juillet 2022 ainsi que l'habilitation faite au Roi de déterminer le périmètre des zones. Enfin, selon les parties requérantes, les obligations supplémentaires de conservation prévues à l'article 9 de la loi du 20 juillet 2022 pour les services OTT ne sont pas proportionnées.

B.76. Les griefs des parties requérantes sont principalement pris de la violation du droit au respect de la vie privée et du droit à la protection des données à caractère personnel, garantis par l'article 22 de la Constitution, par l'article 8 de la Convention européenne des droits de l'homme, par les articles 7, 8 et 52, paragraphe 1, de la Charte, par la directive 2002/58/CE, par la directive (UE) 2016/680 et par le RGPD.

B.77. La Cour de justice a jugé, par l'arrêt du 6 octobre 2020 précité, que l'obligation de conservation des données relatives aux communications électroniques doit être l'exception et non la règle.

B.78.1. Les articles 126/1 à 126/3 de la loi du 13 juin 2005, tels qu'ils ont été insérés par les articles 9 à 11 de la loi du 20 juillet 2022, obligent les opérateurs qu'ils visent à conserver une série de données (article 126/2) à des fins de sauvegarde de la sécurité nationale, de lutte contre la criminalité grave, de prévention de menaces graves contre la sécurité publique et de sauvegarde des intérêts vitaux d'une personne physique (article 126/1), dans cinq types de zones géographiques, à savoir, premièrement, celles qui sont caractérisées par un taux d'au moins trois infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par 1 000 habitants par an (article 126/3, § 1er), deuxièmement, celles dont le niveau de menace est au moins de 3, tel qu'il a été déterminé dans le cadre de l'évaluation visée à l'article 8, 1° et 2°, de la loi du 10 juillet 2006 « relative à l'analyse de la menace », conformément à l'article 11 de l'arrêté royal du 28 novembre 2006 « portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace » (article 126/3, § 2), troisièmement, celles qui sont particulièrement exposées à des menaces pour la sécurité nationale ou à la commission d'actes de criminalité grave, composées d'une série de lieux limitativement énumérés (article 126/3, § 3), quatrièmement, celles qui sont caractérisées par une menace grave potentielle pour les intérêts vitaux du pays ou pour les besoins essentiels de la population, composées d'une série de lieux limitativement énumérés (article 126/3, § 4), et, cinquièmement, celles qui sont caractérisées par une menace potentielle grave pour les intérêts des institutions internationales établies sur le territoire national, composées d'une série de lieux limitativement énumérés (article 126/3, § 5).

B.78.2. Dans le dispositif de l'arrêt du 6 octobre 2020 précité, la Cour de justice a dit pour droit 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, s'oppose à des mesures législatives prévoyant, aux fins visées dans cet article 15, paragraphe 1, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation.

Dans ce même dispositif, la Cour de justice a dit pour droit 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, ne s'oppose toutefois pas à des mesures législatives :

- prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une

conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période limitée au strict nécessaire mais renouvelable;

- prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période limitée au strict nécessaire;

- prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité et de la sauvegarde de la sécurité publique, une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques.

Les mesures législatives précitées doivent toutefois garantir, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect de conditions matérielles et procédurales et que les personnes concernées disposent de garanties effectives contre les risques d'abus.

B.79.1. Les données visées à l'article 126/2 de la loi du 13 juin 2005 peuvent, en principe, faire l'objet d'une conservation préventive ciblée en vue des finalités de sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention de menaces graves contre la sécurité publique, visées à l'article 126/1, § 1er, alinéa 3, de la loi du 13 juin 2005.

Comme la section de législation du Conseil d'État l'a observé dans son avis sur l'avant-projet de loi qui est à l'origine de la loi du 20 juillet 2022, la finalité de « sauvegarde des intérêts vitaux d'une personne physique », également visée à l'article 126/1, § 1er, alinéa 3, de la loi du 13 juin 2005, peut être considérée comme relevant de la finalité de sauvegarde de la sécurité publique (*Doc. parl.*, Chambre, 2021-2022, DOC 55-2572/001, p. 279).

B.79.2. Il appartient à la Cour de vérifier, au regard desdites normes de référence citées en B.76, si les articles 126/1 à 126/3 de la loi du 13 juin 2005 prévoient des règles claires et précises concernant la portée et l'application de la mesure de conservation des données prévues et imposent des exigences minimales. L'ingérence doit se limiter au strict nécessaire et répondre à des critères objectifs, établissant un rapport entre les données conservées et l'objectif poursuivi. Il revient au législateur d'opérer les distinctions qui s'imposent entre les différents types de données soumises à conservation, de sorte à garantir que, pour chaque type de donnée, l'ingérence soit limitée au strict nécessaire.

B.80.1. En ce qui concerne la mesure de conservation des données à des fins de sécurité nationale, la Cour de justice a jugé, dans l'arrêt du 6 octobre 2020 précité :

« 148. S'agissant de la délimitation dont doit faire l'objet une telle mesure de conservation des données, celle-ci peut, notamment, être fixée en fonction des catégories de personnes concernées, dès lors que l'article 15, paragraphe 1, de la directive 2002/58 ne s'oppose pas à une réglementation fondée sur des éléments objectifs, permettant de viser les personnes dont les données relatives au trafic et les données de localisation 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 ou encore un risque pour la sécurité nationale (voir, en ce sens, arrêt du 21 décembre 2016, *Tele2*, C-203/15 et C-698/15, EU:C:2016:970, point 111).

149. À cet égard, il convient de préciser que les personnes ainsi visées peuvent notamment être celles ayant été préalablement identifiées, dans le cadre des procédures nationales applicables et sur la base d'éléments objectifs, comme présentant une menace pour la sécurité publique ou la sécurité nationale de l'État membre concerné.

150. La délimitation d'une mesure prévoyant la conservation des données relatives au trafic et des données de localisation peut également être fondée sur un critère géographique lorsque les autorités nationales compétentes considèrent, sur la base d'éléments objectifs et non discriminatoires, qu'il existe, dans une ou plusieurs zones géographiques, une situation caractérisée par un risque élevé de préparation ou de commission d'actes de criminalité grave (voir, en ce sens, arrêt du 21 décembre 2016, *Tele2*, C-203/15 et C-698/15, EU:C:2016:970, point 111). Ces zones peuvent être, notamment, des lieux caractérisés par un nombre élevé d'actes de criminalité grave, des lieux particulièrement exposés à la commission d'actes de criminalité grave, tels que des lieux ou infrastructures fréquentés régulièrement par un nombre très élevé de personnes, ou encore des lieux stratégiques, tels que des aéroports, des gares ou des zones de péages.

151. Afin d'assurer que l'ingérence que comportent les mesures de conservation ciblée décrites aux points 147 à 150 du présent arrêt soit conforme au principe de proportionnalité, leur durée ne saurait dépasser celle qui est strictement nécessaire au regard de l'objectif poursuivi ainsi que des circonstances les justifiant, sans préjudice d'un renouvellement éventuel

en raison de la persistance de la nécessité de procéder à une telle conservation » (CJUE, 6 octobre 2020, C-511/18, C-512/18 et C-520/18 précités).

B.80.2. Il ressort des travaux préparatoires des dispositions attaquées que le législateur a souhaité, par les articles 126/1 à 126/3 de la loi du 13 juin 2005, mettre en œuvre la possibilité de délimiter une mesure de conservation des données sur la base d'un critère géographique, possibilité mise en évidence par l'arrêt de la Cour de justice du 6 octobre 2020 précité (*Doc. parl.*, Chambre, 2021-2022, Doc 55-2572/001, pp. 45-49).

B.80.3.1. La mise en œuvre du critère géographique précité doit toutefois s'avérer pertinente et proportionnée au regard des finalités poursuivies.

B.80.3.2. Comme la section de législation du Conseil d'État l'a observé dans son avis sur l'avant-projet de loi qui est à l'origine de la loi du 20 juillet 2022, le nombre et la variété des zones visées à l'article 126/3 de la loi du 13 juin 2005 sont considérables et leur addition aboutit à couvrir une partie assez importante du territoire (*ibid.*, p. 283).

B.80.3.3. Il ressort de l'exposé des motifs du projet à l'origine de la loi du 20 juillet 2022 que le législateur estime que le terme « zones géographiques » visé au point 150 de l'arrêt de la Cour de justice du 6 octobre 2020 précité, « peut à l'issue de l'examen des statistiques de chaque arrondissement porter sur l'ensemble du territoire national s'il y a dans chacun de ces arrondissements un taux de criminalité élevé » (*ibid.*, p. 65).

En ce qui concerne la première catégorie de zones géographiques, définie à l'article 126/3, § 1er, de la loi du 13 juin 2005, lequel prévoit la conservation des données visées à l'article 126/2, § 2, de la loi du 13 juin 2005 sur la base de lieux caractérisés par un nombre élevé de faits de criminalité grave (critère statistique), le législateur reconnaît qu'« on ne peut dès lors nier qu'il existe une possibilité, sur base de données statistiques, qui sont par définition dynamiques et évolutives, que des données doivent être conservées, dans tous les arrondissements judiciaires et donc pour l'ensemble du territoire » (*ibid.*, p. 66).

Le législateur relève également que « les groupes d'auteurs sont, par ailleurs, très mobiles et se déplacent et que le crime organisé est par essence polycriminel. Se limiter d'office à certains lieux très ciblés au niveau local pour ce type de criminalité n'est pas approprié » (*ibid.*, pp. 63-64).

Lors de l'examen du projet de loi au sein de la commission compétente de la Chambre des représentants, le ministre de la Justice a observé, en ce qui concerne les zones stratégiques énumérées à l'article 126/3, §§ 3 à 5, de la loi du 13 juin 2005, qu'« au total, environ 30 % du territoire constituera une zone stratégique, ce qui montre avant tout que la Belgique est un pays de petite taille densément peuplé » (*Doc. parl.*, Chambre, 2021-2022, DOC 55-2572/003, p. 104).

B.80.3.4. Le simple constat que la mesure de conservation des données visée aux articles 126/1 à 126/3 peut cibler l'ensemble du territoire dans certaines circonstances ne signifie toutefois pas que celle-ci doive s'assimiler à une mesure généralisée de conservation des données visant de manière indifférenciée l'ensemble des utilisateurs des moyens de communications électroniques.

En effet, ceci ne correspond pas à l'objectif du législateur, mais uniquement à une conséquence possible de données statistiques de zones géographiques décrites et délimitées en détail à l'article 126/3. Les statistiques relatives au nombre d'infractions dans ces zones géographiques déterminent avec objectivité et pertinence la règle applicable en matière de conservation et de traitement de données.

Par conséquent, la loi répond à l'exigence, citée au point 150 de l'arrêt de la Cour de justice du 6 octobre 2020, précité, de ce que « les autorités nationales compétentes considèrent, sur la base d'éléments objectifs et non discriminatoires, qu'il existe, dans une ou plusieurs zones géographiques, une situation caractérisée par un risque élevé de préparation ou de commission d'actes de criminalité grave ».

B.81. Par conséquent, par la mesure de conservation des données prévue aux articles 9 à 11 de la loi du 20 juillet 2022, le législateur s'est limité au strict nécessaire.

B.82. Les premier, deuxième et troisième moyens dans l'affaire n° 7930, le moyen unique dans l'affaire n° 7931 et le premier moyen dans l'affaire n° 7932, en sa troisième branche, ne sont pas fondés en ce qu'ils sont pris de la violation de l'article 22 de la Constitution, lu en combinaison avec l'article 8 de la Convention européenne des droits de l'homme, avec les articles 7, 8 et 52, paragraphe 1, de la Charte et avec l'article 15, paragraphe 1, de la directive 2002/58/CE.

8. L'énumération des autorités compétentes et des finalités dans le cadre de l'accès aux données (article 13)

B.83. Les premier et quatrième moyens dans l'affaire n° 7930, le moyen unique dans l'affaire n° 7931, ainsi que les première et deuxième branches du troisième moyen dans l'affaire n° 7932 portent sur l'article 13 de la loi du 20 juillet 2022.

Cette disposition insère, dans la loi du 13 juin 2005, un article 127/1, qui dispose :

« § 1er. Pour l'application du présent article, la criminalité grave comprend notamment les faits pour lesquels il existe des indices sérieux :

1° qu'ils sont de nature à entraîner la peine minimale d'emprisonnement correctionnel principal visée à l'article 88*bis*, § 1er, alinéa 1er, du Code d'instruction criminelle;

2° qu'ils sont de nature à entraîner une sanction de niveau 5 ou 6 visée à l'article XV.70 du Code de droit économique;

3° qu'ils pourraient constituer une infraction aux articles 14 ou 15 du règlement (UE) n° 596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché (règlement relatif aux abus de marché) et abrogeant la directive 2003/6/CE du Parlement européen et du Conseil et les directives 2003/124/CE, 2003/125/CE et 2004/72/CE de la Commission ou aux dispositions prises sur la base ou en exécution de ces articles.

§ 2. Seules les autorités suivantes peuvent obtenir d'un opérateur des données conservées en vertu des articles 122 et 123, pour les finalités ci-dessous, pour autant que prévu par et aux conditions fixées dans une norme législative formelle :

1° les services de renseignement et de sécurité, afin d'accomplir les missions qui leur sont attribuées par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité;

2° les autorités compétentes aux fins de la prévention de menaces graves pour la sécurité publique;

3° les autorités chargées de la sauvegarde des intérêts vitaux de personnes physiques;

4° les autorités compétentes pour l'examen d'une défaillance de la sécurité du réseau ou du service de communications électroniques ou des systèmes d'information;

5° les autorités administratives ou judiciaires compétentes pour la prévention, la recherche, la détection ou la poursuite d'une infraction commise en ligne ou par le biais d'un réseau ou service de communications électroniques;

6° les autorités administratives ou judiciaires compétentes pour la prévention, la recherche, la détection ou la poursuite d'un fait qui relève de la criminalité grave;

7° les autorités administratives chargées de préserver un intérêt économique ou financier important de l'Union européenne ou de la Belgique, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale;

8° les autorités administratives ou judiciaires compétentes pour la prévention, la recherche, la détection ou la poursuite d'un fait qui constitue une infraction pénale mais qui ne relève pas de la criminalité grave;

9° l'Institut dans le cadre du contrôle de la présente loi et les autorités compétentes pour la protection des données dans le cadre de leurs missions de contrôle;

10° les autorités qui sont légalement habilitées à réutiliser des données à des fins de recherche scientifique ou historique ou à des fins statistiques.

§ 3. Les données conservées en vertu des articles 126 et 127 le sont pour les autorités et les finalités visées au paragraphe 2, 1° à 8°.

Seules les autorités visées au paragraphe 2 peuvent obtenir d'un opérateur des données conservées en vertu des articles 126 et 127, pour les finalités prévues dans ce même paragraphe, pour autant que prévu par et aux conditions fixées dans une norme législative formelle.

Par dérogation à l'alinéa 2, les autorités visées au paragraphe 2, 10°, ne peuvent pas obtenir d'un opérateur des adresses IP attribuées à la source de la connexion.

Par dérogation à l'alinéa 2, une demande d'une autorité d'obtenir d'un opérateur des adresses IP attribuées à la source d'une connexion n'est autorisée qu'aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave, de la prévention des menaces graves contre la sécurité publique et de la sauvegarde des intérêts vitaux d'une personne physique, lorsque cette autorité serait en mesure, à l'aide des informations en sa possession et des adresses IP attribuées à la source de la connexion obtenues de l'opérateur, de tracer le parcours de navigation d'un utilisateur final sur Internet.

§ 4. Les données conservées en vertu des articles 126/1 et 126/3 le sont pour les autorités et finalités visées au paragraphe 2, 1° à 3° et 6°.

Seules les autorités visées au paragraphe 2, 1° à 3°, 6° et 9°, peuvent obtenir d'un opérateur, pour les finalités visées dans ce même paragraphe, des données conservées en vertu des articles 126/1 et 126/3, pour autant que prévu par et aux conditions fixées dans une norme législative formelle.

§ 5. La norme législative formelle de droit belge visée aux paragraphes 2 à 4 précise :

- la ou les catégories d'entreprises auxquelles l'autorité peut demander des données;

- les catégories de données qui peuvent être demandées;

- les finalités poursuivies;

- les mécanismes de contrôle de la demande de données, qui est effectué en interne ou, le cas échéant, par une juridiction ou une autorité administrative indépendante.

Le ministre fait publier au *Moniteur belge* une circulaire qui comprend une liste des autorités belges qui sont habilitées à obtenir d'un opérateur des données conservées en vertu des articles 122, 123, 126, 126/1, 126/3 et 127.

À la demande du ministre ou de l'Institut, les autorités belges visées aux paragraphes 2 à 4 fournissent les informations nécessaires pour la rédaction de cette circulaire.

§ 6. Les demandes que les autorités adressent aux opérateurs afin d'obtenir certaines données conservées en vertu des articles 122, 123, 126, 126/1, 126/3 ou 127 comprennent les mentions minimales suivantes :

1° l'identité de l'autorité demanderesse, ou, lorsque la demande est envoyée à l'opérateur par un service central pour le compte de cette autorité, l'identité de ce service;

2° la fonction de la personne de contact auprès de l'autorité demanderesse, ou, lorsque la demande est envoyée à l'opérateur par un service central pour le compte de l'autorité, la fonction de la personne de contact auprès de ce service central;

3° la base juridique sur laquelle se fonde la demande, sauf lorsque la demande est envoyée à l'opérateur par le biais d'un service central pour le compte d'une autre autorité;

4° le délai de réponse souhaité.

§ 7. L'Institut transmet annuellement au ministre et au ministre de la Justice des statistiques sur la fourniture aux autorités de données conservées en vertu des articles 122, 123,

126, 126/1, 126/3 et 127. Ces ministres les transmettent annuellement à la Chambre des représentants.

Ces statistiques comprennent notamment :

1° les cas dans lesquels des données conservées 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 conservées n'ont pu être satisfaites.

Ces statistiques ne peuvent comprendre des données à caractère personnel ou de l'information confidentielle.

Les données qui concernent l'application de l'alinéa 2, 1°, sont également jointes au rapport que le ministre de la Justice fait au Parlement conformément à l'article 90*decies* du Code d'instruction criminelle.

L'Institut demande aux opérateurs et au service désigné par le Roi les informations qui lui permettent de remplir l'obligation visée à l'alinéa 1er ».

B.84.1. La partie requérante dans l'affaire n° 7930 prend les premier et quatrième moyens de la violation des articles 11, 12, 22 et 29 de la Constitution, de l'article 15, paragraphe 1, et des articles 5, 6 et 9 de la directive 2002/58/CE, lus à la lumière des articles 7, 8, 11, 47 et 52, paragraphe 1, de la Charte, des articles 6, 8, 10, 11 et 18 de la Convention européenne des droits de l'homme et des articles 13 et 54 de la directive (UE) 2016/680, en ce que l'article 13 de la loi du 20 juillet 2022 autorise un accès très large aux données concernées, qui font elles-mêmes l'objet d'une obligation de conservation généralisée. En particulier, elle soutient que les autorités visées sortent du cadre des finalités énumérées à l'article 15, paragraphe 1, de la directive 2002/58/CE, qu'aucune hiérarchie entre les finalités n'est établie, que la notion de « criminalité grave » retenue n'est pas conforme à la jurisprudence de la Cour de justice et qu'il appartient au ministre compétent de déterminer les autorités qui peuvent accéder aux données, ce qui n'est pas compatible avec le principe de la légalité formelle.

B.84.2. La partie requérante dans l'affaire n° 7931 prend un moyen unique de la violation des articles 11, 12, 22 et 29 de la Constitution, lus en combinaison ou non avec les articles 7, 8, 11, 47 et 52, paragraphe 1, de la Charte, avec l'article 8 de la Convention européenne des droits de l'homme, avec les articles 5, 6 et 15 de la directive 2002/58/CE et avec les articles 13 et 54 de la directive (UE) 2016/680. La partie requérante affirme que l'article 13 de la loi du

20 juillet 2022 autorise le ministre compétent à énumérer les autorités habilitées à accéder aux données visées, ce qui viole le principe de la légalité formelle, que cette disposition n'exige pas que la demande d'accès soit motivée par rapport à la finalité poursuivie et que la manière dont la « criminalité grave » est définie n'est pas conforme à la jurisprudence de la Cour de justice.

B.84.3. Les parties requérantes dans l'affaire n° 7932 prennent un troisième moyen de la violation des articles 10, 11, 15, 22 et 29 de la Constitution, lus en combinaison ou non avec les articles 5, 6, 8, 9, 10, 11, 14 et 18 de la Convention européenne des droits de l'homme, avec les articles 7, 8, 11, 47 et 52 de la Charte, avec l'article 5, paragraphe 4, du Traité sur l'Union européenne, avec la directive 2002/58/CE, avec la directive (UE) 2016/680 et avec le RGPD.

Dans une première branche, les parties requérantes soutiennent que l'article 13 de la loi du 20 juillet 2022 ne respecte pas la hiérarchie des finalités imposée par la jurisprudence de la Cour de justice, que la définition de la « criminalité grave » retenue n'est pas conforme à cette jurisprudence, que les autorités visées sont trop nombreuses et que celles-ci sortent du cadre des finalités énumérées par l'article 15, paragraphe 1, de la directive 2002/58/CE.

Dans une deuxième branche, les parties requérantes soutiennent que les griefs dirigés contre l'article 13 de la loi du 20 juillet 2022 valent aussi pour les modalités spécifiques d'accès aux données, prévues aux chapitres 3 à 10 de la loi du 20 juillet 2022, qui, par ailleurs, ne prévoient pas systématiquement les garanties procédurales nécessaires ainsi qu'un contrôle indépendant lors de l'accès à des données sensibles. À cet égard, les parties requérantes citent les articles 21, 24, 26, 27, 28, 33, 34, 35, 37, 40, 41, 42 et 44 de la loi du 20 juillet 2022.

B.85. Les griefs des parties requérantes sont principalement pris de la violation du droit au respect de la vie privée et du droit à la protection des données à caractère personnel, garantis par l'article 22 de la Constitution, par l'article 8 de la Convention européenne des droits de l'homme, par les articles 7, 8 et 52, paragraphe 1, de la Charte, par la directive 2002/58/CE, par

la directive (UE) 2016/680 et par le RGPD. Elles ne formulent explicitement aucun grief de violation des autres normes de référence citées en B.84.1 à B.84.3.

B.86. L'article 127/1 de la loi du 13 juin 2005 porte sur l'accès aux données conservées en vertu des articles 122, 123, 126, 126/1, 126/3 et 127 de cette loi.

B.87.1. Il ressort du libellé de l'article 127/1 de la loi du 13 juin 2005 ainsi que de ses travaux préparatoires que cette disposition ne règle pas l'accès aux données visées aux articles 122, 123, 126, 126/1, 126/3 et 127 de la loi du 13 juin 2005 (*Doc. parl.*, Chambre, 2021-2022, DOC 55-2572/001, pp. 96-97).

B.87.2. En effet, l'article 127/1 de la loi du 13 juin 2005 se limite à énumérer les autorités et les finalités qui peuvent permettre l'accès aux données conservées sur la base des articles 122, 123, 126, 126/1, 126/3 et 127 de la loi du 13 juin 2005. Si l'article 127/1 s'oppose à ce qu'une autre autorité soit désignée ou à ce qu'une autre finalité soit invoquée en vue d'accéder aux données précitées, il n'autorise pas non plus lui-même l'ensemble des autorités et des finalités qu'il énumère à y avoir accès, comme l'a observé la section de législation du Conseil d'État dans son avis sur l'avant-projet de loi qui est à l'origine de la loi du 20 juillet 2022 (*ibid.*, pp. 309-311).

B.87.3. Les conditions prévues à l'article 127/1 de la loi du 13 juin 2005 ne sont pas suffisantes pour permettre l'accès aux données concernées. Il est en effet exigé qu'une « norme législative formelle » spécifique soit adoptée (article 127/1, §§ 2 et 3) et que celle-ci précise « la ou les catégories d'entreprises auxquelles l'autorité peut demander des données », « les catégories de données qui peuvent être demandées », « les finalités poursuivies » et « les mécanismes de contrôle de la demande de données, qui est effectuée en interne ou, le cas échéant, par une juridiction ou une autorité administrative indépendante » (article 127/1, § 5).

C’est à travers les différentes « normes législatives formelles » visées à l’article 127/1 qu’il appartient au législateur d’opérer les distinctions qui s’imposent entre les différents types de données conservées, de manière à garantir que, pour chaque type de données, l’ingérence soit limitée au strict nécessaire.

B.88. Partant, en ce qu’ils portent sur l’accès aux données dont la conservation est autorisée par la loi du 13 juin 2005, les griefs des parties requérantes ne sauraient être imputables à l’article 127/1 de cette loi, mais aux « normes législatives formelles », visées dans cette disposition, qui déterminent les données ciblées, les autorités qui peuvent en demander l’accès, les finalités précises qui sont poursuivies, ainsi que les mécanismes éventuels de contrôle.

Dans ce cadre, le troisième moyen, en sa deuxième branche, des parties requérantes dans l’affaire n° 7932 ne saurait être considéré comme portant sur de telles normes législatives formelles, dès lors que ces parties se limitent à citer les articles 21, 24, 26, 27, 28, 33, 34, 35, 37, 40, 41, 42 et 44 de la loi du 20 juillet 2022, sans démontrer en quoi ceux-ci constitueraient des applications de l’article 127/1 de la loi du 13 juin 2005, et qu’elles n’étayent pas davantage en quoi ces dispositions violeraient concrètement les normes de référence citées en B.85.

B.89. Enfin, en ce qui concerne la compatibilité de l’article 127/1, § 5, alinéa 2, de la loi du 13 juin 2005 avec le principe de la légalité formelle, en ce que cette disposition prévoit que le ministre compétent fait publier au *Moniteur belge* une circulaire comprenant la liste des autorités belges habilitées à obtenir d’un opérateur l’accès aux données conservées en vertu des articles 122, 123, 126, 126/1, 126/3 et 127 de la loi du 13 juin 2005, cette disposition vise uniquement à permettre au ministre précité d’énumérer, dans une circulaire, l’ensemble des autorités ciblées dans les « normes législatives formelles » dont il est question à l’article 127/1 de la loi du 13 juin 2005.

L’article 127/1, § 5, alinéa 2, n’habilite pas un ministre à déterminer les autorités compétentes pour accéder aux données visées aux articles 122, 123, 126, 126/1, 126/3 et 127 de la loi du 13 juin 2005.

B.90. Les premier et quatrième moyens dans l'affaire n° 7930, le moyen unique dans l'affaire n° 7931 ainsi que le troisième moyen dans l'affaire n° 7932, en ses première et deuxième branches, ne sont pas fondés en ce qu'ils portent sur l'article 13 de la loi du 20 juillet 2022.

B.91.1. Dans son moyen unique, la partie requérante dans l'affaire n° 7931 dénonce également la non-information de la personne dont les données font l'objet d'un accès et l'absence de voies de recours en cas d'accès illégal à ces données. En ce qui concerne l'absence d'information précitée, elle demande à titre subsidiaire qu'une question préjudicielle soit posée à la Cour de justice.

B.91.2. Les parties requérantes dans l'affaire n° 7932 prennent un quatrième moyen de la violation des articles 10, 11, 13 et 22 de la Constitution, lus en combinaison ou non avec les articles 5, 6, 8, 9, 10, 11, 14 et 18 de la Convention européenne des droits de l'homme, avec les articles 7, 8, 11, 47 et 52 de la Charte, avec l'article 5, paragraphe 4, du Traité sur l'Union européenne, avec la directive 2002/58/CE, avec la directive (UE) 2016/680 et avec le RGPD. Dans ce moyen, les parties requérantes dénoncent de manière générale la non-notification à l'utilisateur de l'accès aux données par les autorités compétentes, ce qui serait contraire au droit d'accès à la justice et au droit à un recours effectif, sans toutefois viser une disposition particulière de la loi du 20 juillet 2022.

B.91.3. Si ces moyens peuvent être considérés comme portant sur l'article 127/1 de la loi du 13 juin 2005, il y a lieu de rappeler, comme il est dit en B.87.1, que cette disposition n'autorise pas en soi l'accès aux données concernées. Partant, la demande de poser une question préjudicielle faite par la partie requérante dans l'affaire n° 7931 n'est pas pertinente dans le cadre de l'article 127/1 de la loi du 13 juin 2005.

Par ailleurs, en ce que le quatrième moyen dans l'affaire n° 7932 porterait sur les « normes législatives formelles » spécifiques visées à l'article 127/1 de la loi du 13 juin 2005, les parties requérantes ne visent aucune disposition législative particulière à l'appui de leurs griefs, ni n'expliquent en quoi ces normes législatives formelles spécifiques violeraient les normes de référence citées en B.85.

B.91.4. Le moyen unique dans l'affaire n° 7931, en ce qu'il porte sur les griefs mentionnés en B.91.1, et le quatrième moyen dans l'affaire n° 7932 ne sont pas fondés.

9. Les compétences des officiers de police judiciaire de l'IBPT (article 24)

B.92. Le moyen unique dans l'affaire n° 7931 porte sur l'article 24 de la loi du 20 juillet 2022. Cette disposition insère, dans la loi du 17 janvier 2003 « relative au statut du régulateur des secteurs des postes et des télécommunications belges » (ci-après : la loi du 17 janvier 2003), un article 25/1, qui dispose :

« § 1er. Afin de rechercher, de constater ou de poursuivre une infraction visée à l'article 145, § 3 ou § 3*bis*, de la loi du 13 juin 2005 relative aux communications électroniques ou à l'article 24, § 1er, 2°, un officier de police judiciaire de l'Institut peut, par écrit :

1° exiger d'un opérateur de répondre à une demande de données d'identification qui est nécessaire à ces fins;

2° requérir la collaboration des personnes et institutions visées à l'article 46*quater*, § 1er, du Code d'instruction criminelle et d'associations les représentant, sur la base de la référence de paiement en ligne spécifique à un service de communications électroniques qui a préalablement été communiquée par un opérateur conformément au 1°, afin d'identifier la personne qui a payé le service;

3° requérir la collaboration des centres fermés ou des lieux d'hébergement au sens des articles 74/8 et 74/9 de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers, où la souscription de l'abonné à un service de communications électroniques a été effectué, sur la base des coordonnées du centre ou du lieu d'hébergement qui ont préalablement été communiquées par un opérateur conformément au 1°, afin d'identifier l'abonné;

4° requérir la collaboration de toute autre personne morale qui est l'abonnée d'un opérateur ou qui souscrit à un service de communications électroniques au nom et pour le compte de personnes physiques, sur la base des données qui ont préalablement été communiquées par un opérateur conformément au 1°, afin d'identifier l'abonné ou l'utilisateur habituel du service.

Une demande visée à l'alinéa 1er ne peut être transmise à un acteur visé à l'alinéa 1er qu'après autorisation écrite d'un officier de police judiciaire visé à l'article 24, § 2. Cette autorisation ne peut être octroyée que sur demande écrite et motivée adressée à cet officier conformément au paragraphe 5.

§ 2. Pour les besoins de l'accomplissement de ses missions, un officier de police judiciaire de l'Institut peut exiger d'un opérateur, par écrit, de répondre à une demande de métadonnées,

qui est nécessaire afin de rechercher, de constater ou de poursuivre une infraction visée à l'article 145, § 3, ou § 3*bis*, de la loi du 13 juin 2005 relative aux communications électroniques ou à l'article 24, § 1er, 2°.

Sauf en cas d'urgence dûment justifiée, l'officier de police judiciaire de l'Institut ne peut adresser la demande à l'opérateur qu'après avoir soumis une demande écrite et motivée au juge d'instruction et après autorisation écrite de ce dernier.

En cas d'urgence dûment justifiée visée à l'alinéa 2, l'officier de police judiciaire de l'Institut communique au juge d'instruction, sans délai après l'envoi de la demande à l'opérateur, une copie de cette demande, la motivation de la demande et la justification de l'urgence. Un contrôle ultérieur est effectué par le juge d'instruction.

Lorsqu'à la suite de ce contrôle ultérieur, le juge d'instruction refuse de confirmer la validité de la demande envoyée par l'officier de police judiciaire de l'Institut à l'opérateur, cet officier le notifie sans délai à l'opérateur concerné et supprime les métadonnées reçues.

§ 3. Par dérogation aux paragraphes 1er et 2, afin de contrôler le respect des articles 126, 126/1, 126/2, 126/3 ou 127 de la loi du 13 juin 2005 relative aux communications électroniques et de leurs arrêtés d'exécution et à la demande écrite et motivée d'un officier de police judiciaire de l'Institut, un opérateur fournit, dans le délai fixé dans le réquisitoire, un accès permettant de consulter ses bases de données qui mettent en œuvre un de ces articles ou un de ces arrêtés d'exécution.

Une demande visée à l'alinéa 1er ne peut être transmise à un opérateur qu'après autorisation écrite d'un officier de police judiciaire de l'Institut visé à l'article 24, § 2. Cette autorisation ne peut être octroyée que sur demande écrite et motivée conformément au paragraphe 5.

La demande adressée à l'opérateur précise les noms des officiers de police judiciaire de l'Institut qui peuvent consulter la base de données.

Ces officiers ne peuvent prendre une copie des données et documents consultés dans le cadre de l'alinéa 1er que dans le but de constater des infractions commises par l'opérateur.

§ 4. Pour l'application des paragraphes 1er et 2, les acteurs visés au paragraphe 1er, alinéa 1er, auxquels un officier de police judiciaire de l'Institut a demandé des données, lui communiquent ces données en temps réel ou, le cas échéant, au moment précisé dans le réquisitoire.

Pour l'application des paragraphes 1er à 3, toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

Toute personne qui refuse de communiquer les données ou qui ne les communique pas en temps réel ou, le cas échéant, au moment précisé dans le réquisitoire est punie d'une amende de vingt-six euros à dix mille euros.

Toute personne qui refuse de permettre la consultation de la base de données conformément au paragraphe 3 ou qui ne permet pas cette consultation dans le délai fixé dans le réquisitoire est punie d'une amende de vingt-six euros à dix mille euros.

§ 5. Pour l'application des paragraphes 1er à 3, la motivation de la demande adressée à l'officier de police judiciaire visé à l'article 24, § 2, ou au juge d'instruction doit être développée au regard des circonstances de l'enquête.

Pour l'application des paragraphes 1er et 2, cette motivation indique :

1° le lien entre les données demandées et l'objectif de recherche, de constat ou de poursuite de l'infraction spécifique qui justifie la demande;

2° le caractère strictement nécessaire des données demandées dans le cadre de l'enquête.

§ 6. Les officiers de police judiciaire de l'Institut consignent dans un registre :

1° l'ensemble des demandes visées aux paragraphes 1er, 2 et 3;

2° la motivation de la demande et la justification de l'urgence communiquées au juge d'instruction conformément au paragraphe 2, alinéa 3;

3° les autorisations prévues aux paragraphes 1er, 2 et 3 ».

B.93. La partie requérante dans l'affaire n° 7931 prend un moyen unique de la violation des articles 11, 12, 22 et 29 de la Constitution, lus en combinaison ou non avec les articles 7, 8, 11, 47 et 52, paragraphe 1, de la Charte, avec l'article 8 de la Convention européenne des droits de l'homme, avec les articles 5, 6 et 15 de la directive 2002/58/CE et avec les articles 13 et 54 de la directive (UE) 2016/680. Elle soutient que l'article 25/1 de la loi du 17 janvier 2003 viole les normes de référence précitées en ce qu'il autorise l'accès aux données, dans le cadre d'une procédure pénale, par un officier de police judiciaire, qui n'est pas une autorité indépendante, et en ce qu'il n'impose pas de contrôle judiciaire préalable à cet accès. Par ailleurs, elle dénonce également le fait que la personne dont les données font l'objet de l'accès n'en soit pas prévenue, ainsi que l'absence de voies de recours en cas d'accès illégal aux données. En ce qui concerne la non-information précitée, elle demande à titre subsidiaire qu'une question préjudicielle soit posée à la Cour de justice.

B.94. Les griefs de la partie requérante sont uniquement pris de la violation du droit au respect de la vie privée et du droit à la protection des données à caractère personnel, garantis par l'article 22 de la Constitution, par l'article 8 de la Convention européenne des droits de l'homme, par les articles 7, 8 et 52, paragraphe 1, de la Charte, par la directive 2002/58/CE, par la directive (UE) 2016/680 et par le RGPD.

B.95. Dans le cadre d'une procédure pénale, l'article 25/1 de la loi du 17 janvier 2003 autorise un officier de police judiciaire de l'IBPT à accéder aux données dans deux hypothèses. Premièrement, l'officier de police judiciaire peut accéder à des données d'identification afin de rechercher, de constater ou de poursuivre les infractions visées à l'article 145, §§ 3 et 3*bis*, de la loi du 13 juin 2005 et à l'article 24, § 1er, 2°, de la loi du 17 janvier 2003 (article 25/1, § 1er). Deuxièmement, l'officier de police judiciaire peut accéder, pour les besoins de l'accomplissement de ses missions, aux métadonnées nécessaires afin de rechercher, de constater ou de poursuivre les infractions précitées (article 25/1, § 2).

B.96. Au regard de ce qui précède, la Cour limite son examen à l'article 25/1, §§ 1 et 2, de la loi du 17 janvier 2003.

B.97. Étant donné que la disposition attaquée renvoie aux dispositions à propos desquelles la Cour a posé des questions préjudicielles à la Cour de justice, il convient de surseoir à statuer sur l'examen de ces moyens, dans l'attente de la réponse de la Cour de justice à ces questions préjudicielles.

10. Les compétences du procureur du Roi (articles 25 et 26)

B.98.1. Le moyen unique dans l'affaire n° 7931 porte, notamment, sur les articles 25 et 26 de la loi du 20 juillet 2022.

B.98.2. L'article 25 de la loi du 20 juillet 2022 insère, dans le Code d'instruction criminelle, un article 39*quinquies* , qui dispose :

« § 1er. Lors de la recherche de crimes et délits, le procureur du Roi peut, s'il existe des indices sérieux que les infractions peuvent donner lieu à un emprisonnement correctionnel principal d'un an ou à une peine plus lourde, ordonner, par une décision écrite et motivée, à un ou plusieurs acteurs visés à l'alinéa 2, de conserver les données visées à l'article 88*bis*, § 1, alinéa 1er, générées ou traitées par eux dans le cadre de la fourniture des services de communications concernés, qu'il juge nécessaires.

L'ordre visé à l'alinéa 1er peut être donné, directement ou par l'intermédiaire du service de police désigné par le Roi, à :

- l'opérateur d'un réseau de communications électroniques; et

- toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.

La décision écrite et motivée mentionne :

- le nom du procureur du Roi qui ordonne la conservation;

- l'infraction qui fait l'objet de l'ordre;

- les circonstances de fait de la cause qui justifient la conservation;

- l'indication précise d'un ou de plusieurs des éléments suivants : la personne ou les personnes, les moyens de communication ou les lieux qui font l'objet de la conservation;

- le cas échéant, les catégories de données de trafic et de localisation qui doivent être conservées;

- la durée de la mesure, qui ne peut excéder deux mois à compter de la date de l'ordre, sans préjudice de renouvellement;

- la durée de conservation des données, qui ne peut excéder six mois. Ce délai peut être prolongé par écrit.

En cas d'urgence, la conservation peut être ordonnée verbalement. L'ordre doit être confirmé dans les plus brefs délais dans la forme prévue à l'alinéa 3.

§ 2. Les acteurs visés au paragraphe 1er, alinéa 2, veillent à ce que l'intégrité, la qualité et la disponibilité des données soit garantie et à ce que les données soient conservées de manière sécurisée.

§ 3. Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

Toute personne qui refuse de coopérer, ou qui fait disparaître, détruit ou modifie les données conservées, est punie d'un emprisonnement de six mois à un an ou d'une amende de vingt-six euros à vingt mille euros ou d'une de ces peines seulement.

§ 4. L'accès aux données conservées conformément à cet article n'est possible qu'en application de l'article 88*bis* ».

B.98.3. L'article 26 de la loi du 20 juillet 2022 modifie l'article 46*bis* du Code d'instruction criminelle comme suit :

« 1° dans le paragraphe 1er, un alinéa rédigé comme suit est inséré entre les alinéas 2 et 3 :

' Pour procéder à l'identification de l'abonné ou de l'utilisateur habituel d'un service visé à l'alinéa 2, deuxième tiret, il peut également requérir, directement ou par l'intermédiaire du service de police désigné par le Roi, la collaboration :

- des personnes et institutions visées à l'article 46*quater*, § 1er, sur la base de la référence d'une transaction bancaire électronique qui a préalablement été communiquée par un des acteurs visés à l'alinéa 2, premier et deuxième tirets, en application de l'alinéa 1er;

- des centres fermés ou des lieux d'hébergement au sens des articles 74/8 et 74/9 de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers, sur la base des coordonnées du centre ou du lieu d'hébergement où la souscription de l'abonné à un service de communications électroniques mobiles a été effectué, et qui ont préalablement été communiquées par un des acteurs visés à l'alinéa 2, premier et deuxième tirets, en application de l'alinéa 1er;

- des autres personnes morales qui sont l'abonné d'un des acteurs visés à l'alinéa 2, premier ou deuxième tiret, ou qui souscrivent à un service de communications électroniques au nom et pour le compte de personnes physiques, sur la base des données qui ont préalablement été communiquées par un des acteurs visés à l'alinéa 2, premier et deuxième tirets, en application de l'alinéa 1er. ';

2° dans le paragraphe 2, les alinéas 3 et 4 sont abrogés;

3° l'article est complété par les paragraphes 3 et 4, rédigés comme suit :

' § 3. Les acteurs visés au paragraphe 1er, alinéa 3, premier à troisième tiret, requis de communiquer l'identification de l'abonné ou de l'utilisateur habituel d'un service visé au paragraphe 1er, alinéa 2, deuxième tiret, communiquent au procureur du Roi ou à l'officier de police judiciaire les données en temps réel ou, le cas échéant, au moment précisé dans la réquisition.

§ 4. Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

Toute personne qui refuse de communiquer les données ou qui ne les communique pas en temps réel ou, le cas échéant, au moment précisé dans la réquisition est punie d'une amende de vingt-six euros à dix mille euros. ' ».

B.99.1. La partie requérante dans l'affaire n° 7931 prend un moyen unique de la violation des articles 11, 12, 22 et 29 de la Constitution, lus en combinaison ou non avec les articles 7, 8, 11, 47 et 52, paragraphe 1, de la Charte, avec l'article 8 de la Convention européenne des droits de l'homme, avec les articles 5, 6 et 15 de la directive 2002/58/CE et avec les articles 13 et 54 de la directive (UE) 2016/680.

La partie requérante dans l'affaire n° 7931 soutient que l'article 39*quinquies* du Code d'instruction criminelle vise la criminalité « en général », alors que la Cour de justice se limite aux cas de criminalité « grave », d'une part, et que cette disposition prévoit une durée de conservation disproportionnée, d'autre part.

En ce qui concerne les modifications apportées à l'article 46*bis* du Code d'instruction criminelle, la partie requérante allègue tout d'abord que cette disposition permet au procureur du Roi ou, en cas d'extrême urgence, à un officier de police judiciaire, d'accéder à des données d'identification sans que cet accès soit subordonné à un contrôle préalable et indépendant, comme l'exige la Cour de justice. À titre subsidiaire, elle demande qu'une question préjudicielle soit posée à la Cour de justice. En outre, la partie requérante allègue que l'article 46*bis* du Code d'instruction criminelle, tel qu'il a été modifié, autorise le procureur du Roi, en cas d'urgence, à accéder aux données de trafic et de localisation à des fins de lutte contre la criminalité en général, ce qui n'est pas non plus compatible avec les exigences de la Cour de justice. À titre subsidiaire, elle demande qu'une question préjudicielle à ce sujet soit posée à cette juridiction. Par ailleurs, la partie requérante allègue que la collaboration des centres fermés et des lieux d'hébergement visés à l'article 46*bis* du Code d'instruction criminelle n'est pas justifiée au regard de la lutte contre la criminalité. Enfin, elle allègue que l'article 46*bis* du Code d'instruction criminelle ne prévoit pas que la personne soit informée de l'accès aux données ni

de l'existence d'une voie de recours spécifique. En ce qui concerne la non-information précitée, elle demande qu'une question préjudicielle soit posée à la Cour de justice.

B.99.2. Les griefs de la partie requérante dirigés contre les articles 39*quinquies* et 46*bis* du Code d'instruction criminelle sont uniquement pris de la violation du droit au respect de la vie privée et du droit à la protection des données à caractère personnel, tels qu'ils sont garantis par l'article 22 de la Constitution, par l'article 8 de la Convention européenne des droits de l'homme, par les articles 7, 8 et 52, paragraphe 1, de la Charte, par la directive 2002/58/CE et par la directive (UE) 2016/680.

B.100. La Cour examine d'abord les griefs dirigés contre l'article 39*quinquies* du Code d'instruction criminelle, puis les griefs relatifs à l'article 46*bis* du même Code.

B.101.1. Dans le dispositif de son arrêt du 6 octobre 2020 précité, la Cour de justice a dit pour droit que 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, ne s'oppose pas à une mesure « permettant, aux fins de la lutte contre la criminalité grave et, *a fortiori*, de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques, par le biais d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont disposent ces fournisseurs de services ».

B.101.2. Dans sa jurisprudence, la Cour de justice ne définit pas la notion de « criminalité grave ». Comme il ressort des conclusions de l'avocat général précédant l'arrêt de la Cour de justice du 2 octobre 2018 rendu en grande chambre en cause de *Ministerio Fiscal*, précité, cette notion relève en principe de la compétence des États membres, même s'il appartient à la Cour de justice de veiller au respect de toutes les exigences résultant du droit de l'Union européenne, et notamment d'assurer une application cohérente de la protection offerte par les dispositions de la Charte. En effet, la qualification juridique d'une infraction est susceptible non seulement de varier d'un État membre à un autre, en fonction des traditions suivies et des priorités définies par chacun d'eux, mais également de fluctuer dans le temps, en fonction des orientations qui sont données à la politique pénale, vers plus ou moins de sévérité, pour tenir compte de

l'évolution de la criminalité, ainsi que, plus généralement, des transformations de la société et des besoins existants, notamment en matière de répression pénale, sur le plan national. Par ailleurs, en ce qui concerne l'importance de la peine, le fait qu'un État membre prévoie une peine d'emprisonnement peu élevée voire une peine alternative à l'emprisonnement ne préjuge pas pour autant de la gravité intrinsèque du type d'infraction concerné (conclusions de l'avocat général Henrik Saugmandsgaard Øe précédant CJUE, grande chambre, 2 octobre 2018, C-207/16, précité, points 93-100).

À cet égard, la Cour de justice a souligné que la définition donnée, en droit national, aux « infractions graves » susceptibles de permettre d'accéder aux données conservées par les fournisseurs de services de communications électroniques et de tirer des conclusions précises sur la vie privée des personnes concernées ne doit pas être large au point que l'accès à ces données devienne la règle plutôt que l'exception. Ainsi, elle ne saurait couvrir la grande majorité des infractions pénales, ce qui serait le cas si le seuil au-delà duquel la peine de réclusion maximale dont est punie une infraction justifie que celle-ci soit qualifiée d'infraction grave était fixé à un niveau excessivement bas (CJUE, grande chambre, 30 avril 2024, C-178/22, *Procura della Repubblica presso il Tribunale di Bolzano*, ECLI:EU:C:2024:371, point 55).

B.101.3. En ce qui concerne la proportionnalité de la durée de la conservation des données précitées, la Cour de justice, par l'arrêt du 6 octobre 2020 précité, a jugé que « la durée de conservation des données doit être limitée au strict nécessaire, celle-ci pouvant néanmoins être prolongée lorsque les circonstances et l'objectif poursuivi par ladite mesure le justifient » (point 164).

B.102.1. En l'espèce, la partie requérante ne démontre pas en quoi le législateur aurait excédé la marge d'appréciation nationale en définissant, à l'article 39*quinquies*, § 1er, alinéa 1er, du Code d'instruction criminelle, la notion de « criminalité grave » par référence aux infractions susceptibles de « donner lieu à un emprisonnement correctionnel principal d'un an ou à une peine plus lourde ». L'on n'aperçoit pas non plus en quoi cette définition violerait les normes de référence citées en B.99.2. À cet égard, la section de législation du Conseil d'État a précisément observé, dans son avis sur l'avant-projet de loi qui est à l'origine de la loi du 20 juillet 2022, que « concernant le ministère public par exemple, le respect du critère de ' criminalité grave ', résulte également de l'article 39*quinquies* en projet, du Code d'instruction

criminelle » (*Doc. parl.*, Chambre, 2021-2022, DOC 55-2572/001, p. 310). Du reste, le rattachement d'une infraction pénale à la criminalité grave doit s'apprécier de façon concrète, sous le contrôle du juge pénal, au regard de la nature de l'infraction commise et de l'ensemble des faits de l'espèce.

Le juge pénal doit en particulier être en mesure de refuser l'accès aux données concernées lorsque cet accès est sollicité dans le cadre de poursuites pour une infraction qui n'est manifestement pas grave (CJUE, grande chambre, 30 avril 2024, C-178/22, précité, ECLI:EU:C:2024:371, point 62).

B.102.2. En ce qui concerne la durée de conservation des données visées, l'article 39*quinquies* du Code d'instruction criminelle prévoit un délai qui ne peut excéder six mois, mais qui peut être prolongé par écrit (article 39*quinquies*, § 1er, alinéa 3). La durée précise de la conservation doit être, sauf en cas d'urgence, écrite et motivée, de sorte qu'il appartient au procureur du Roi de démontrer, sous le contrôle du juge pénal, que le délai de conservation qu'il impose est limité au strict nécessaire et, en cas de prolongation, les circonstances et les objectifs qui justifient une telle mesure.

B.103.1. L'article 46*bis* du Code d'instruction criminelle, tel qu'il a été modifié par la loi du 20 juillet 2022, vise à permettre au Procureur du Roi de procéder à l'identification de l'abonné ou de l'utilisateur habituel d'un service visé à l'alinéa 2 de cette disposition, à savoir le service fourni par « l'opérateur d'un réseau de communications électroniques » et « toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques », définition qui comprend également « le fournisseur d'un service de communications électroniques ».

B.103.2. Il ressort des travaux préparatoires de la loi du 20 juillet 2022 que l'article 46*bis* du Code d'instruction criminelle, tel qu'il a été modifié par cette loi, a vocation à porter sur les données d'identification visées à l'article 127 de la loi du 13 juin 2005 (*Doc. parl.*, Chambre, 2021-2022, DOC 55-2572/002, pp. 148-151)

B.103.3. Dès lors que, pour les motifs mentionnés en B.48.1 à B.48.4, l'article 126 de la loi du 13 juin 2005, tel qu'il a été inséré par l'article 8 de la loi du 20 juillet 2022, ne viole pas les normes de référence citées en B.49, il en va de même en ce qui concerne l'article 46*bis* du Code d'instruction criminelle, tel qu'il a été modifié par la loi du 20 juillet 2022.

B.103.4. La Cour de justice et la Cour européenne des droits de l'homme n'exigent ni la mise en place d'un contrôle judiciaire ou administratif préalable, ni l'information de la personne concernée quant à un accès à des données d'identification, ni qu'un recours spécifique soit prévu. Partant, il ne saurait être reproché au législateur de ne pas avoir prévu, à l'article 46*bis* du Code d'instruction criminelle, tel qu'il a été modifié par la loi du 20 juillet 2022, de telles modalités, dès lors que cette disposition vise uniquement des données d'identification. Partant, il n'est pas nécessaire de poser les questions préjudicielles suggérées par la partie requérante à ce sujet.

B.103.5. En ce que la partie requérante allègue que l'article 46*bis* du Code d'instruction criminelle autorise le procureur du Roi, en cas d'urgence, à accéder aux données de trafic et de localisation à des fins de lutte contre la criminalité en général, le moyen unique manque en fait, puisque, comme il est dit en B.103.2, l'article 26 de la loi du 20 juillet 2022, qui modifie l'article 46*bis* précité, ne porte que sur les données d'identification et non sur les données de trafic et de localisation. Partant, il n'y a pas lieu de poser la question préjudicielle demandée par la partie requérante à ce sujet.

B.103.6. Enfin, en ce qui concerne la possibilité dont dispose le procureur du Roi de requérir la collaboration des centres fermés et des lieux d'hébergement visés à l'article 46*bis*, § 1er, alinéa 2, deuxième tiret, du Code d'instruction criminelle, la partie requérante ne développe aucun élément concret qui soit de nature à démontrer l'absence du caractère nécessaire de la mesure.

B.103.7. Le moyen unique dans l'affaire n° 7931 n'est pas fondé en ce qu'il porte sur les articles 25 et 26 de la loi du 20 juillet 2022.

11. Les compétences du juge d'instruction (article 27)

B.104. Le cinquième moyen dans l'affaire n° 7930 et le moyen unique dans l'affaire n° 7931 portent sur l'article 27 de la loi du 20 juillet 2022, qui dispose :

« A l'article 88*bis* du [Code d'instruction criminelle], inséré par la loi du 11 février 1991, remplacé par la loi du 10 juin 1998 et modifié en dernier lieu par la loi du 5 mai 2019, les modifications suivantes sont apportées :

1° le paragraphe 2, remplacé par l'article 9 de la loi du 29 mai 2016, annulé lui-même par l'arrêt n° 57/2021 de la Cour constitutionnelle, 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 des articles 126/1 et 126/3 de la loi du 13 juin 2005 relative aux communications électroniques, les dispositions suivantes s'appliquent :

- pour une infraction visée au livre II, titre Iter, 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. ';

2° à la place du paragraphe 3, inséré par l'article 9 de la loi du 29 mai 2016, annulé lui-même par l'arrêt n° 57/2021 de la Cour constitutionnelle, il est inséré 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. Ces personnes sont tenues au secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal. ' ».

B.105.1. La partie requérante dans l'affaire n° 7930 prend un cinquième moyen de la violation des articles 11, 12, 22 et 29 de la Constitution, lus en combinaison ou non avec l'article 15, paragraphe 1, avec les articles 5, 6 et 9 de la directive 2002/58/CE, avec les articles 6, 8, 10, 11 et 18 de la Convention européenne des droits de l'homme et avec les articles 13 et 54 de la directive (UE) 2016/680. Elle soutient que l'article 88*bis*, § 3, du Code d'instruction criminelle, tel qu'il a été modifié par la loi du 20 juillet 2022, prévoit en ce qui concerne l'accès aux données des avocats et des médecins une mesure spécifique qui ne permet pas de pallier l'inconstitutionnalité de la conservation généralisée de données en tant que telle, et que cette mesure ne concerne que le juge d'instruction et non les autres autorités qui peuvent également demander l'accès aux données des avocats, des médecins et des journalistes.

B.105.2. La partie requérante dans l'affaire n° 7931 prend un moyen unique de la violation des articles 11, 12, 22 et 29 de la Constitution, lus en combinaison ou non avec les articles 7, 8, 11, 47 et 52, paragraphe 1, de la Charte, avec l'article 8 de la Convention européenne des droits de l'homme, avec les articles 5, 6 et 15 de la directive 2002/58/CE et avec les articles 13 et 54 de la directive (UE) 2016/680. Elle soutient que l'article 88*bis*, § 2, du Code d'instruction criminelle, tel qu'il a été modifié par la loi du 20 juillet 2022, autorise un accès aux données lorsqu'existent des indices sérieux de la commission d'une infraction de nature à entraîner un emprisonnement correctionnel principal d'un an ou d'une peine plus lourde, ce qui vise en réalité la grande majorité des infractions et ne se limite pas au cas de la criminalité grave. À titre subsidiaire, la partie requérante demande qu'une question préjudicielle soit posée à la Cour de justice sur ce point. Par ailleurs, la partie requérante dénonce également la non-information de la personne dont les données font l'objet de l'accès et l'absence de voies de recours en cas d'accès illégal aux données. En ce qui concerne la non-information précitée, elle demande à titre subsidiaire qu'une question préjudicielle soit posée à la Cour de justice.

B.106.1. Les griefs des parties requérantes dirigés contre l'article 88*bis* du Code d'instruction criminelle sont uniquement pris de la violation du droit au respect de la vie privée et du droit à la protection des données à caractère personnel, garantis par l'article 22 de la Constitution, par l'article 8 de la Convention européenne des droits de l'homme, par les

articles 7, 8 et 52, paragraphe 1, de la Charte, par la directive 2002/58/CE et par la directive (UE) 2016/680.

B.106.2. La Cour examine d'abord les griefs dirigés contre le paragraphe 2 de l'article 88*bis* du Code d'instruction criminelle, puis les griefs relatifs au paragraphe 3 de cette disposition.

B.107.1. L'article 88*bis*, § 2, du Code d'instruction criminelle porte sur l'accès du juge d'instruction aux données conservées en vertu des articles 126/1 et 126/3 de la loi du 13 juin 2005, soit aux données de trafic et de localisation (voy. *Doc. parl.*, Chambre, 2021-2022, DOC 55-2572/001, p. 145).

B.107.2. En ce qui concerne les finalités, l'article 88*bis*, § 2, du Code d'instruction criminelle, tel qu'il a été modifié par l'article 27 de la loi du 20 juillet 2022, autorise le juge d'instruction à accéder aux données conservées lorsqu'existent des indices sérieux de la commission d'une infraction de nature à entraîner un emprisonnement correctionnel principal d'un an ou d'une peine plus lourde.

Comme il est dit en B.102.1, la partie requérante ne démontre pas en quoi le législateur aurait excédé sa marge d'appréciation en définissant, à l'article 88*bis*, § 2, du Code d'instruction criminelle, la notion de « criminalité grave » par référence aux infractions susceptibles de « donner lieu à un emprisonnement correctionnel principal d'un an ou à une peine plus lourde ». Cette définition ne viole pas les normes de référence citées en B.105.2. Du reste, le rattachement d'une infraction pénale à la criminalité grave doit s'apprécier *in concreto*, sous le contrôle du juge pénal, au regard de la nature de l'infraction commise et de l'ensemble des faits de l'espèce.

B.107.3. Les parties requérantes dénoncent également la non-information de la personne dont les données font l'objet de l'accès et l'absence de voies de recours en cas d'accès illégal aux données.

S'il est exact que l'article 88*bis*, § 2, du Code d'instruction criminelle ne prévoit pas de contrôle juridictionnel spécifique en ce qui concerne l'accès du juge d'instruction aux données conservées en vertu des articles 126/1 et 126/3, il importe de relever que le juge d'instruction

est un magistrat indépendant et impartial dont l'intervention est une garantie essentielle du respect des conditions auxquelles est subordonnée une atteinte au droit au respect de la vie privée. Même si les décisions qu'il prend ne sont pas revêtues de l'autorité de la chose jugée, elles participent de l'exercice de la fonction juridictionnelle et s'inscrivent dans le cadre d'une procédure judiciaire.

Par ailleurs, les recours de droit commun dirigés contre une ordonnance du juge d'instruction suffisent en la matière. Il convient de relever, notamment, que, dans le cadre de la procédure pénale, le prévenu dispose à cet égard du droit d'invoquer devant les juridictions d'instruction ou devant la juridiction de jugement la nullité d'un acte d'instruction qui viole son droit au respect de la vie privée ou son droit à un procès équitable. Par ailleurs, l'intéressé peut, en vertu de l'article 58 de la loi du 3 décembre 2017 « portant création de l'Autorité de protection des données », déposer sans frais une plainte auprès de l'Autorité de protection des données en cas de traitement illicite de ses données à caractère personnel.

Quant à l'information de la personne concernée, elle se fait conformément aux règles du Code d'instruction criminelle applicables à l'instruction.

B.107.4. Le moyen unique dans l'affaire n° 7931 n'est pas fondé en ce qu'il porte sur l'article 88*bis*, § 2, du Code d'instruction criminelle.

B.108.1. En ce qui concerne l'article 88*bis*, § 3, du Code d'instruction criminelle, les griefs de la partie requérante dans l'affaire n° 7930 ne portent en réalité pas sur cette disposition. En effet, « la mesure de conservation généralisée des données en tant que telle », que vise la partie requérante, n'est pas réglée à l'article 88*bis*, § 3 et, par ailleurs, la circonstance que le système prévu par cette disposition n'est pas étendu aux « autres autorités » qui peuvent demander l'accès aux données des avocats, des médecins et des journalistes ne saurait être imputable à l'article 88*bis*, puisque celui-ci se borne à délimiter les pouvoirs du juge d'instruction et, en cas de flagrant délit, du procureur du Roi (paragraphe 1er, alinéa 1er).

B.108.2. Le cinquième moyen dans l'affaire n° 7930 n'est pas fondé en ce qu'il est pris de la violation de l'article 20, 2°, de la loi du 20 juillet 2022.

12. Les compétences des services de renseignement et de sécurité (articles 33, 34 et 37)

B.109.1. Le premier moyen dans l'affaire n° 7932 porte notamment sur les articles 33, 34 et 37 de la loi du 20 juillet 2022.

B.109.2. L'article 33 de la loi du 20 juillet 2022 modifie la loi du 30 novembre 1998, en y insérant un article 13/6, qui dispose :

« § 1er. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, requérir le concours d'un opérateur de réseaux de communications électroniques ou d'un fournisseur de services de communications électroniques pour procéder à :

1° la conservation des données de trafic et de localisation de moyens de communications électroniques qui sont à sa disposition au moment de la réquisition;

2° la conservation des données de trafic et de localisation qu'il génère et traite à partir de la réquisition.

La réquisition visée à l'alinéa 1er repose sur une décision écrite et motivée du dirigeant du service ou de son délégué.

§ 2. La réquisition visée au paragraphe 1er, alinéa 1er, mentionne :

1° la nature des données de trafic et de localisation à conserver;

2° les personnes, les groupements, les zones géographiques, les moyens de communication et/ou le mode d'utilisation dont les données de trafic et de localisation doivent être conservées;

3° pour la mesure visée au paragraphe 1er, alinéa 1er, 1°, le délai de conservation des données, qui ne peut excéder six mois à compter de la date de la réquisition, sans préjudice de la possibilité de prolongation en suivant la même procédure;

4° pour la mesure visée au paragraphe 1er, alinéa 1er, 2° :

- la durée de la mesure, qui ne peut excéder six mois à compter de la date de la réquisition, sans préjudice de la possibilité de prolongation en suivant la même procédure;

- le délai de conservation des données, qui ne peut excéder six mois à compter de la date de la communication, sans préjudice de la possibilité de prolongation en suivant la même procédure;

5° la date de la réquisition;

6° la signature du dirigeant du service ou de son délégué.

§ 3. En cas d'extrême urgence, le dirigeant du service ou son délégué peut requérir la conservation verbalement. Cette réquisition verbale est confirmée par écrit au plus tard le premier jour ouvrable qui suit.

§ 4. Les services de renseignement et de sécurité tiennent un registre de toutes les réquisitions de conservation.

Chaque décision de réquisition est notifiée avec sa motivation au Comité permanent R. Lorsqu'il constate une illégalité, le Comité permanent R met fin à la réquisition.

Lorsqu'il est mis fin prématurément à la réquisition, l'opérateur d'un réseau de communications électroniques ou le fournisseur d'un service de communications électroniques requis en est averti le plus rapidement possible.

§ 5. Pour l'exécution de la réquisition, le dirigeant du service ou son délégué peut requérir le concours de l'Institut visé à l'article 2, 1°, de la loi du 13 juin 2005 relative aux communications électroniques, ainsi que des personnes dont il présume qu'elles ont une expertise technique utile. Cette réquisition est écrite et mentionne la base légale.

§ 6. Toute personne qui refuse de prêter son concours aux réquisitions visées aux paragraphes 1er et 5 est punie d'une amende de vingt-six euros à vingt mille euros.

§ 7. Le Roi peut déterminer, sur proposition du ministre de la Justice, du ministre de la Défense et du ministre qui a les Communications électroniques dans ses attributions, les modalités de collaboration des opérateurs d'un réseau de communications électroniques ou des fournisseurs d'un service de communications électroniques ».

L'article 34 de la loi du 20 juillet 2022 modifie la loi du 30 novembre 1998 en y insérant un article 13/7, qui dispose :

« § 1er. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions et lorsqu'il existe une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, requérir le concours des opérateurs d'un réseau de communications électroniques et des fournisseurs d'un service de communications électroniques afin de procéder à la conservation généralisée et indifférenciée des données de trafic et de localisation de moyens de communications électroniques générées et traitées par eux.

§ 2. La réquisition visée au paragraphe 1er ne peut avoir lieu qu'avec l'accord écrit préalable de la commission. La commission donne son accord dans les quatre jours suivant la réception de la demande écrite et motivée du dirigeant du service.

§ 3. La demande du dirigeant du service de requérir la conservation mentionne, sous peine d'illégalité :

1° la menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible;

2° les circonstances de fait qui justifient la conservation généralisée et indifférenciée des données de trafic et de localisation;

3° la nature des données de trafic et de localisation à conserver;

4° la durée de la mesure de conservation, qui ne peut excéder six mois à compter de la date de la réquisition. Elle peut être prolongée en suivant la même procédure;

5° le délai de conservation des données, qui ne peut excéder six mois à compter de la date de la communication. Il peut être prolongé en suivant la même procédure;

6° le cas échéant, les motifs qui justifient l'extrême urgence visée au paragraphe 5;

7° la date de la demande;

8° la signature du dirigeant du service.

§ 4. La réquisition visée au paragraphe 1er mentionne :

1° la date de l'accord de la commission;

2° la nature des données de trafic et de localisation à conserver;

3° la durée de la mesure et le délai de conservation des données;

4° la date de la réquisition;

5° la signature du dirigeant du service ou de son délégué.

§ 5. En cas d'extrême urgence, le dirigeant du service demande l'accord verbal préalable du président de la commission ou, en cas d'indisponibilité, d'un autre membre de la commission. L'auteur de l'accord en informe immédiatement les autres membres de la commission. Le dirigeant du service confirme sa demande par écrit dans les vingt-quatre heures suivant l'accord. Le président ou le membre contacté confirme également son accord par écrit le plus rapidement possible. Cet accord est valable cinq jours.

§ 6. La réquisition de conservation généralisée et indifférenciée est confirmée par arrêté royal.

L'arrêté royal ne mentionne que :

1° la date de l'accord de la commission;

2° la date de la réquisition;

3° la nature des données de trafic et de localisation à conserver;

4° la durée de la mesure et le délai de conservation des données.

En l'absence de confirmation par arrêté royal dans le mois de la réquisition, cette réquisition prend fin.

Les opérateurs d'un réseau de communications électroniques et les fournisseurs d'un service de communications électroniques requis en sont avertis le plus rapidement possible.

§ 7. Pour l'exécution de la réquisition, le dirigeant du service peut requérir le concours de l'Institut visé à l'article 2, 1°, de la loi du 13 juin 2005 relative aux communications électroniques, ainsi que des personnes dont il présume qu'elles ont une expertise technique utile. Cette réquisition est écrite et mentionne la base légale et l'accord de la commission.

§ 8. Toute personne qui refuse de prêter son concours aux réquisitions visées aux paragraphes 1er et 7 est punie d'une amende de vingt-six euros à vingt mille euros.

§ 9. La commission transmet sans délai la demande du dirigeant du service et son accord au Comité permanent R.

§ 10. Le service de renseignement et de sécurité fait rapport à la commission toutes les deux semaines sur l'évolution de la menace. Ce rapport met en évidence les éléments qui justifient soit le maintien de la conservation généralisée et indifférenciée, soit la fin de celle-ci.

§ 11. Le dirigeant du service met fin à la réquisition, nonobstant la confirmation par arrêté royal, lorsque la conservation n'est plus utile pour lutter contre la menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, lorsque cette menace a disparu ou lorsqu'il constate une illégalité.

Lorsque la commission ou le Comité permanent R constate une illégalité, il est mis fin à la réquisition nonobstant la confirmation par arrêté royal.

Lorsqu'il est mis fin prématurément à la réquisition, les opérateurs d'un réseau de communications électroniques ou les fournisseurs d'un service de communications électroniques requis en sont avertis le plus rapidement possible.

§ 12. Le Roi détermine, sur proposition du ministre de la Justice, du ministre de la Défense et du ministre qui a les Communications électroniques dans ses attributions, les modalités de collaboration des opérateurs d'un réseau de communications électroniques ou des fournisseurs d'un service de communications électroniques ».

L'article 37 de la loi du 20 juillet 2022 remplace l'article 18/8 de la loi du 30 novembre 1998, qui dispose désormais :

« § 1er. 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 communications électroniques ou du fournisseur d'un service de communications électroniques, 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.

Dans les cas visés à l'alinéa 1er et pour chaque moyen de communication électronique dont les données de trafic sont repérées ou dont l'origine ou la destination de la communication électronique est localisée, le jour, l'heure et la durée ainsi que, si nécessaire, le lieu de la communication électronique sont indiqués et consignés dans un rapport.

La nature de la décision est communiquée à l'opérateur requis du réseau de communications électroniques ou au fournisseur du service de communications électroniques qui est requis.

§ 2. [...]

§ 3. Tout opérateur d'un réseau de communications électroniques et tout fournisseur d'un service de communications électroniques qui est requis de communiquer les données visées au paragraphe 1er donne au dirigeant du service les données qui ont été demandées dans un délai et selon les modalités à fixer par un arrêté royal pris sur la proposition du ministre de la Justice, du ministre de la Défense et du ministre qui a les Communications électroniques dans ses attributions.

Toute personne visée à l'alinéa 1er qui refuse de prêter son concours technique aux réquisitions visées au présent article est punie d'une amende de vingt-six euros à vingt mille euros.

§ 4. […] ».

B.109.3. Le premier moyen dans l'affaire n° 7932 est pris de la violation des articles 10, 11, 13, 15, 22, 23 et 29 de la Constitution, lus en combinaison ou non avec les articles 5, 6, 8, 9, 10, 11, 14 et 18 de la Convention européenne des droits de l'homme, avec les articles 7, 8, 11, 47 et 52 de la Charte, avec l'article 5, paragraphe 4, du Traité sur l'Union européenne, avec l'article 6 de la directive 2002/58/CE, avec la directive (UE) 2016/680 et avec le RGPD.

Dans une quatrième branche, les parties requérantes soutiennent que l'article 13/6 de la loi du 30 novembre 1998 viole le principe de prévisibilité garanti par l'article 22 de la Constitution, en ce qu'il ne décrit pas avec précision les données de trafic et de localisation qu'il vise. Par ailleurs, elles affirment que l'article 13/6 n'est pas conforme à la jurisprudence de la Cour de justice en ce qu'il prévoit une obligation de conservation qui excède ce qui est strictement nécessaire et qui équivaut en réalité à une obligation de conservation généralisée et indifférenciée de données, d'une part, et en ce qu'il n'établit ni une voie de recours, ni la notification de la conservation de données, ni l'intervention d'un juge, ni, lorsqu'il est mis prématurément fin à la réquisition par le Comité permanent R en raison d'une illégalité, l'effacement des données collectées, d'autre part.

Dans une cinquième branche, les parties requérantes soutiennent que l'article 13/7 de la loi du 30 novembre 1998 ne respecte pas le critère de prévisibilité qui découle de l'article 22 de la Constitution et de la jurisprudence de la Cour de justice, en ce qu'il ne définit pas la notion de « données de trafic et de localisation » qu'il vise. Par ailleurs, elles affirment qu'aucune notification n'est prévue à l'égard des personnes concernées, ce qui entrave la possibilité de contester l'ingérence dans le droit au respect de la vie privée. Enfin, elles allèguent que l'article 13/7 ne prévoit pas un effacement des données conservées en cas d'illégalité de la mesure, contrairement à ce qu'exige la Cour de justice.

Dans une sixième branche, les parties requérantes soutiennent que l'article 18/8 de la loi du 30 novembre 1998 ne définit pas la notion de « données de trafic et de localisation » qu'il vise, ni la durée de la mesure de conservation, ce qui viole le principe de prévisibilité, garanti par l'article 22 de la Constitution et par la jurisprudence de la Cour de justice. Par ailleurs, les parties requérantes allèguent que l'article 18/8 ne prévoit pas de contrôle quant à la nécessité de la mesure, contrairement à ce qu'exige la Cour de justice.

B.109.4. Eu égard à leur connexité, ces branches sont examinées conjointement.

B.110. Il ressort de ce qui est dit en B.109.2 que les griefs des parties requérantes dirigés contre les articles 13/6, 13/7 et 18/8 de la loi du 30 novembre 1998 portent en substance sur la compatibilité de ces dispositions avec le droit au respect de la vie privée et avec le droit à la protection des données à caractère personnel.

B.111.1. En vertu de l'article 1er, paragraphe 3, de la directive 2002/58/CE, cette dernière « ne s'applique pas aux activités qui ne relèvent pas du Traité instituant la Communauté européenne, telles celles qui sont visées dans les titres V et VI du Traité sur l'Union européenne et, en tout état de cause, aux activités concernant la sécurité publique, la défense, la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) ou aux activités de l'État dans des domaines relevant du droit pénal ».

En vertu de l'article 2, paragraphe 2, *a)*, du RGPD, ce règlement « ne s'applique pas au traitement de données à caractère personnel effectué dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union ». En vertu de l'article 2, paragraphe 2, *d)*, du RGPD, il ne s'applique pas non plus au traitement des données à caractère personnel effectué par les autorités compétentes à des fins de protection et de prévention des menaces pour la sécurité publique.

En vertu de l'article 2, paragraphe 3, *a)*, de la directive (UE) 2016/680, cette dernière ne s'applique pas au traitement de données à caractère personnel effectué « dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union ».

Par l'arrêt du 6 octobre 2020 précité, la Cour de justice a jugé :

« À cet égard, il convient de relever, d'emblée, que l'article 4, paragraphe 2, TUE énonce que la sécurité nationale reste de la seule responsabilité de chaque État membre. Cette responsabilité correspond à l'intérêt primordial de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société et inclut la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'État en tant que tel, telles que notamment des activités de terrorisme » (point 135).

B.111.2. En vertu des articles 13/6, 13/7 et 18/8 de la loi du 30 novembre 1998, les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions,

requérir le concours d'un opérateur de réseaux de communications électroniques ou d'un fournisseur de services de communications électroniques pour procéder à la conservation et à la communication de données de trafic et de localisation.

B.111.3. Étant donné que les articles 13/6, 13/7 et 18/8 de la loi du 30 novembre 1998 ne sont applicables que dans le cadre des missions des services de renseignement et de sécurité, ils ne relèvent pas du champ d'application du droit de l'Union européenne. Le moyen est dès lors irrecevable en ce qu'il est pris de la violation des dispositions invoquées du Traité sur l'Union européenne, de la Charte, du RGPD, de la directive (UE) 2016/680 ou de la directive 2002/58/CE, tels qu'ils sont interprétés par la Cour de justice dans sa jurisprudence.

B.112.1. Les autres griefs des parties requérantes relatifs aux articles 13/6, 13/7 et 18/8 de la loi du 30 novembre 1998 sont pris de la violation de l'article 22 de la Constitution.

B.112.2. Comme il est dit en B.11.3, le Constituant a recherché la plus grande concordance possible entre l'article 22 de la Constitution et l'article 8 de la Convention européenne des droits de l'homme (*Doc. parl.*, Chambre, 1992-1993, n° 997/5, p. 2).

La portée de cet article 8 est analogue à celle de la disposition constitutionnelle précitée, de sorte que les garanties que fournissent ces deux dispositions forment un tout indissociable.

B.112.3. Par ailleurs, comme il est rappelé en B.24.1 et B.24.2, l'article 22 de la Constitution réserve au législateur compétent le pouvoir de fixer dans quels cas et à quelles conditions il peut être porté atteinte au droit au respect de la vie privée. Il garantit ainsi à tout citoyen qu'aucune ingérence dans l'exercice de ce droit ne peut avoir lieu qu'en vertu de règles adoptées par une assemblée délibérante, démocratiquement élue. À cet égard, les éléments essentiels du traitement des données à caractère personnel doivent être fixés dans la loi, le décret ou l'ordonnance même. À cet égard, quelle que soit la matière concernée, les éléments suivants constituent, en principe, des éléments essentiels : (1°) la catégorie de données traitées; (2°) la catégorie de personnes concernées; (3°) la finalité poursuivie par le traitement; (4°) la catégorie

de personnes ayant accès aux données traitées; (5°) le délai maximal de conservation des données.

Outre l'exigence de légalité formelle, l'article 22 de la Constitution, lu en combinaison avec l'article 8 de la Convention européenne des droits de l'homme, impose que l'ingérence dans l'exercice du droit au respect de la vie privée et du droit à la protection des données à caractère personnel soit définie en des termes clairs et suffisamment précis qui permettent d'appréhender de manière prévisible les hypothèses dans lesquelles le législateur autorise pareille ingérence. En matière de protection des données, cette exigence de prévisibilité implique qu'il doit être prévu de manière suffisamment précise dans quelles circonstances les traitements de données à caractère personnel sont autorisés. Toute personne doit dès lors pouvoir avoir une idée suffisamment claire des données traitées, des personnes concernées par un traitement de données déterminé et des conditions et finalités dudit traitement.

B.113.1. Les articles 13/6, 13/7 et 18/8 de la loi du 30 novembre 1998 prévoient que les services de renseignement peuvent, dans l'intérêt de l'exercice de leurs missions, requérir le concours d'un opérateur de réseaux de communications électroniques ou d'un fournisseur de service de communications électroniques pour procéder à la conservation et à la communication de « données de trafic et de localisation ». Ce faisant, le législateur a respecté le principe de légalité formelle garanti par l'article 22 de la Constitution, dès lors qu'il a précisé les catégories de données traitées.

B.113.2. De surcroît, les articles 13/6, 13/7 et 18/8 de la loi du 30 novembre 1998 exposent de manière claire et détaillée les données de trafic et de localisation que les services de renseignement peuvent conserver et traiter, ainsi que les conditions et modalités de ces activités, ce qui permet aux personnes concernées d'appréhender de manière suffisamment prévisible les hypothèses dans lesquelles le législateur autorise une ingérence dans le droit au respect de la vie privée et dans le droit à la protection des données à caractère personnel.

B.114. Enfin, la mesure prévue à l'article 18/8 de la loi du 30 novembre 1998 concerne le repérage ou la localisation de données et non leur conservation.

En effet, le commentaire des articles précise, sur ce point :

« Cet article 18/8 porte sur l'accès aux données de communications électroniques par les services de renseignement et de sécurité et non sur la conservation de ces données. [...].

[...]

[...] [I]l convient de préciser qu'aucune modification n'est apportée à l'accès par les services de renseignement et de sécurité aux données de communications électroniques, ni à ses modalités.

La seule modification de l'article 18/8 consiste en la suppression du paragraphe 2 annulé par la Cour constitutionnelle.

L'accès aux données par les services de renseignement et de sécurité visé à l'article 18/8 porte bien entendu sur toutes les données conservées par les opérateurs, peu importe pour quelle finalité.

[...]

En réponse à un commentaire du Comité permanent R (points 16-18), les auteurs du projet souhaitent souligner qu'il n'y a plus de raison de moduler l'accès aux données, puisque l'accès dépendra de la durée de conservation effective et modulée. En outre, l'accès devra toujours être motivé de sorte que la Commission et le Comité permanent R puissent vérifier la proportionnalité, la subsidiarité et la légalité de l'historique demandé. Cette obligation de motivation a en effet été réintroduite, à la demande du Comité, à l'article 18/3, 2, 12° » (*Doc. parl.*, Chambre, 2021-2022, DOC 55-2572/001, pp. 163-164).

Il s'ensuit que le premier moyen dans l'affaire n° 7932, qui porte sur la conservation des données, en sa sixième branche, n'est pas fondé.

B.115. Le premier moyen dans l'affaire n° 7932, en ses quatrième, cinquième et sixième branches, n'est pas fondé.

13. L'entrée en vigueur (article 45)

B.116.1. Le troisième moyen dans l'affaire n° 7930 porte sur l'article 45 de la loi du 20 juillet 2022, qui dispose :

« La conservation ciblée des données sur la base des critères visés à l'article 126/3, §§ 3 à 5, de la loi du 13 juin 2005 relative aux communications électroniques, entre en vigueur à la date fixée par le Roi par arrêté délibéré en Conseil des ministres, et au plus tard le 1er janvier 2027.

Pour la première application de l'article 126/3, §§ 3 à 5, de la loi du 13 juin 2005 relative aux communications électroniques, les autorités compétentes visées à l'article 126/3, § 6, alinéa 2, de la même loi, transmettent les informations nécessaires au service désigné par le Roi à une date fixée par l'arrêté royal visé à l'alinéa 1er et au plus tard le 1er janvier 2026 ».

B.116.2. Le troisième moyen dans l'affaire n° 7930 est pris de la violation des articles 11, 12, 22 et 29 de la Constitution, de l'article 15, paragraphe 1, et des articles 5, 6 et 9 de la directive 2002/58/CE, lus à la lumière des articles 7, 8, 11, 47 et 52, paragraphe 1, de la Charte, des articles 6, 8, 10, 11 et 18 de la Convention européenne des droits de l'homme et des articles 13 et 54 de la directive (UE) 2016/680. La partie requérante soutient que l'entrée en vigueur réglée à l'article 45 viole le principe de légalité garanti par l'article 22 de la Constitution.

B.116.3. L'exposé du moyen ne montre pas en quoi le principe de légalité précité serait violé. Le moyen n'est pas fondé.

14. La protection du secret professionnel

B.117.1. Le moyen unique dans l'affaire n° 7907, le moyen unique dans l'affaire n° 7929, les deuxième et cinquième moyens dans l'affaire n° 7930, ainsi que la septième branche du premier moyen et la troisième branche du troisième moyen dans l'affaire n° 7932 portent sur la non-protection des informations couvertes par le secret professionnel.

B.117.2.1. Le moyen unique dans l'affaire n° 7907, pris de la violation des articles 10 et 11 de la Constitution, lus en combinaison ou non avec les articles 6 et 8 de la Convention européenne des droits de l'homme et avec les articles 7, 8 et 47 de la Charte, porte sur les articles 5, 4° et 6°, 8 à 11, 13 à 15, 19, 21, 22, 24 à 42 et 44 de la loi du 20 juillet 2022.

En particulier, la partie requérante soutient que les dispositions attaquées ne différencient pas, ou à tout le moins pas suffisamment, les utilisateurs titulaires du secret professionnel par rapport aux autres utilisateurs, d'une part, et les données couvertes par le secret professionnel par rapport aux autres données, d'autre part. En ce qui concerne, en particulier, l'article 27 de la loi du 20 juillet 2022, la partie requérante allègue que cette disposition ne vise que les communications qui émanent d'un avocat ou d'un médecin, mais pas celles qui émanent du client ou du patient, ce qui ne permet pas de réserver un traitement spécifique adéquat aux dépositaires du secret professionnel (première et deuxième branches). Par ailleurs, la partie requérante soutient que les dispositions attaquées créent une surveillance généralisée de l'ensemble des citoyens (troisième branche) et qu'elles ne sont pas proportionnées au but poursuivi (quatrième branche).

B.117.2.2. Le moyen unique dans l'affaire n° 7929 est pris de la violation des articles 10 et 11 de la Constitution, lus en combinaison ou non avec les articles 6 et 8 de la Convention européenne des droits de l'homme et avec les articles 7, 8, 11 et 47 de la Charte, et porte sur les articles 2 à 17 de la loi du 20 juillet 2022.

En substance, les parties requérantes soutiennent que les dispositions attaquées traitent de la même manière les utilisateurs de services de télécommunications ou de communications électroniques soumis au secret professionnel, notamment les professionnels comptables et fiscaux, d'une part, et les autres utilisateurs de ces services, d'autre part, sans qu'il soit tenu compte du caractère fondamental du secret professionnel.

B.117.2.3. Le deuxième moyen dans l'affaire n° 7930, qui est pris de la violation des articles 10, 11, 22 et 29 de la Constitution, lus en combinaison ou non avec l'article 15, paragraphe 1, 5, 6 et 9 de la directive 2002/58/CE, lus à la lumière des articles 7, 8, 11, 47 et 52, paragraphe 1, de la Charte, avec les articles 6, 8, 10, 11 et 18 de la Convention européenne des droits de l'homme et avec les articles 13 et 54 de la directive (UE) 2016/680, porte sur les articles 5, 6, 8, 9, 10 et 12 de la loi du 20 juillet 2022, en ce que ces dispositions ne prévoient pas d'exception, en ce qui concerne la conservation des données et l'accès à celles-ci, au bénéfice des médecins, des avocats ou des journalistes.

Le cinquième moyen dans l'affaire n° 7930, qui est pris de la violation des articles 10, 11, 22 et 29 de la Constitution, lus en combinaison ou non avec l'article 15, paragraphe 1, 5, 6 et 9

de la directive 2002/58/CE, lus à la lumière des articles 7, 8, 11, 47 et 52, paragraphe 1, de la Charte, avec les articles 6, 8, 10, 11 et 18 de la Convention européenne des droits de l'homme et avec les articles 13 et 54 de la directive (UE) 2016/680, porte sur la loi du 20 juillet 2022 dans son intégralité en ce qu'elle ne prévoit aucun mécanisme de contrôle pertinent permettant aux bénéficiaires du secret professionnel de s'opposer à la collecte, à la conservation ou à la prise de connaissance de leurs données.

B.117.2.4. La septième branche du premier moyen dans l'affaire n° 7932, lequel est pris de la violation des articles 10, 11, 13, 15, 22, 23 et 29 de la Constitution, lus en combinaison ou non avec les articles 5, 6, 8, 9, 10, 11, 14 et 18 de la Convention européenne des droits de l'homme, avec les articles 7, 8, 11, 47 et 52 de la Charte, avec l'article 5, paragraphe 4, du Traité sur l'Union européenne, ainsi qu'avec l'article 6 de la directive 2002/58/CE, avec la directive (UE) 2016/680 et avec le RGPD, porte sur la loi du 20 juillet 2022 en ce qu'elle ne prévoit aucun traitement particulier pour la conservation des données de trafic et de localisation des avocats, des médecins et des journalistes, alors qu'il s'agit de données sensibles, qui relèvent du secret professionnel.

La troisième branche du troisième moyen dans cette affaire, lequel est pris de la violation des articles 10, 11, 13, 15, 22, 23 et 29 de la Constitution, lus en combinaison ou non avec les articles 5, 6, 8, 9, 10, 11, 14 et 18 de la Convention européenne des droits de l'homme, avec les articles 7, 8, 11, 47 et 52 de la Charte, avec l'article 5, paragraphe 4, du Traité sur l'Union européenne, ainsi qu'avec l'article 6 de la directive 2002/58/CE, avec la directive (UE) 2016/680 et avec le RGPD, porte sur la loi du 20 juillet 2022 en ce qu'elle ne prévoit pas de protection particulière en ce qui concerne l'accès aux données des avocats, des médecins et des journalistes. Les parties requérantes soutiennent par ailleurs que les données précitées sont traitées différemment selon que l'accès aux données se fait ou non sur la base de l'article 27 de la loi du 20 juillet 2022.

B.117.3. Eu égard à leur connexité, la Cour examine les moyens et branches précitées conjointement.

B.118. L'article 88*bis* du Code d'instruction criminelle, tel qu'il a été modifié par la loi attaquée dispose :

« § 1er. 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 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.

Si nécessaire, il peut pour ce faire requérir, directement ou par l'intermédiaire du service de police désigné par le Roi, la collaboration :

- de l'opérateur d'un réseau de communications électroniques; et

- de toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.

Dans les cas visés à l'alinéa 1er, pour chaque moyen de communication électronique dont les données de trafic sont repérées ou dont l'origine ou la destination de la communication électronique est localisée, le jour, l'heure, la durée et, si nécessaire, le lieu de la communication électronique sont indiqués et consignés dans un procès-verbal.

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.

Il précise également la durée durant laquelle la mesure 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.

En cas de flagrant délit, le procureur du Roi peut ordonner la mesure pour les infractions visées à l'article 90*ter*, §§ 2, 3 et 4. Dans ce cas, la mesure doit être confirmée dans les vingt-quatre heures par le juge d'instruction.

S'il s'agit toutefois de l'infraction visée à l'article 137, 347*bis*, 434 ou 470 du Code pénal, à l'exception de l'infraction visée à l'article 137, § 3, 6°, du même Code, le procureur du Roi peut ordonner la mesure tant que la situation de flagrant délit perdure, sans qu'une confirmation par le juge d'instruction ne soit nécessaire.

S'il s'agit de l'infraction visée à l'article 137 du Code pénal, à l'exception de l'infraction visée à l'article 137, § 3, 6°, du même Code, le procureur du Roi peut en outre ordonner la

mesure dans les septante-deux heures suivant la découverte de cette infraction, sans qu'une confirmation par le juge d'instruction soit nécessaire.

Toutefois, le procureur du Roi peut ordonner la mesure si le plaignant le sollicite, lorsque cette mesure s'avère indispensable à l'établissement d'une infraction visée à l'article 145, § 3 et § 3*bis* de la loi du 13 juin 2005 relative aux communications électroniques.

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 4 et 5.

§ 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 des articles 126/1 et 126/3 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.

§ 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. Ces personnes sont tenues au secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

§ 4. Les acteurs visés au § 1er, alinéa 2, communiquent les informations demandées en temps réel ou, le cas échéant, au moment précisé dans la réquisition, selon les modalités fixées par le Roi, sur la proposition du ministre de la Justice et du ministre compétent pour les Télécommunications.

Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

Toute personne qui refuse de prêter son concours technique aux réquisitions visées au présent article, concours dont les modalités sont fixées par le Roi, sur la proposition du ministre de la Justice et du ministre compétent pour les Télécommunications, ou ne le prête pas en temps réel ou, le cas échéant, au moment précisé dans la réquisition, est punie d'une amende de cent euros à trente mille euros ».

B.119. En dehors de l'hypothèse visée à l'article 88*bis*, § 3, du Code d'instruction criminelle, la loi du 20 juillet 2022 ne prévoit pas expressément une protection particulière pour les données protégées par le secret professionnel.

Le libellé même de l'article 88*bis*, § 3, du Code d'instruction criminelle, tel qu'il a été remplacé par l'article 27 de la loi du 20 juillet 2022, prévoit une protection particulière pour les moyens de communications électroniques des avocats et des médecins, c'est-à-dire tant pour les communications qui proviennent de l'avocat et du médecin que pour celles qui émanent des clients et patients (*Doc. parl.*, Chambre, 2021-2022, DOC 55-2572/003, p. 48).

B.120. Le secret professionnel auquel sont astreintes les personnes visées à l'article 458 du Code pénal, notamment les avocats et les médecins, ne vise pas à leur conférer un quelconque privilège, mais principalement à protéger le droit fondamental au respect de la vie privée de la personne qui se confie à eux, parfois dans ce qu'elle a de plus intime. En outre, les informations confidentielles confiées à un avocat, dans l'exercice de sa profession et en raison de cette qualité, bénéficient aussi, dans certaines hypothèses, de la protection découlant, pour le justiciable, des garanties inscrites à l'article 6 de la Convention européenne des droits de l'homme, dès lors que la règle du secret professionnel imposée à l'avocat est un élément fondamental des droits de la défense du justiciable qui se confie à lui.

L'effectivité des droits de la défense de tout justiciable suppose nécessairement qu'une relation de confiance puisse être établie entre lui et l'avocat qui le conseille et le défend. Cette nécessaire relation de confiance ne peut être établie et maintenue que si le justiciable a la

garantie que ce qu'il confiera à son avocat ne sera pas divulgué par celui-ci. Il en découle que la règle du secret professionnel imposée à l'avocat est un élément fondamental des droits de la défense.

Comme l'observe la Cour de cassation, « le secret professionnel auquel sont tenus les membres du barreau repose sur la nécessité d'assurer une entière sécurité à ceux qui se confient à eux » (Cass., 13 juillet 2010, ECLI:BE:CASS:2010:ARR.20100713.1; voy. aussi Cass., 9 juin 2004, ECLI:BE:CASS:2004:ARR.20040609.10).

Même s'il n'est « pas intangible », le secret professionnel de l'avocat constitue dès lors « l'un des principes fondamentaux sur lesquels repose l'organisation de la justice dans une société démocratique » (CEDH, 6 décembre 2012, *Michaud c. France*, ECLI:CE:ECHR:2012:1206JUD001232311, § 123).

B.121.1. Dans ce contexte, la loi du 20 juillet 2022 doit recevoir une interprétation conforme à la Constitution, compte tenu de ce que le secret professionnel de l'avocat est un principe général qui participe du respect des droits fondamentaux. Ainsi, les règles qui y dérogent ne peuvent être que de stricte interprétation, compte tenu de la manière dont est organisée la profession d'avocat dans l'ordre juridique interne.

Les travaux préparatoires relatifs à cette disposition indiquent :

« Le point 2° de l'article 21 [devenu 27] réintègre l'ancien § 3 qui protège les données de communications des médecins et des avocats. La mesure ne peut porter sur leurs moyens de communications électronique que dans le cadre de certaines situations très spécifiques. Ce paragraphe est une reprise des articles 39*bis*, § 9, 56*bis*, 88*bis*, § 3 et 90*octies* CIC » (*Doc. parl.*, Chambre, 2021-2022, DOC 55-2572/001, p. 145).

À propos de cet article 39*bis*, § 9, du Code d'instruction criminelle, la Cour, par l'arrêt n° 66/2021 du 29 avril 2021 (ECLI:BE:GHCC:2021:ARR.066), a jugé :

« B.11.1. L'article 39*bis*, § 9, alinéa 2, du Code d'instruction criminelle prévoit que la mesure ne peut être exécutée sans que le bâtonnier ou le représentant du conseil provincial de l'Ordre des médecins, selon le cas, en soit averti, et que ces personnes seront informées par le procureur du Roi des éléments dont celui-ci estime qu'ils relèvent du secret professionnel.

B.11.2. Cette disposition n'établit pas la manière dont l'intervention du représentant de l'ordre concerné doit concrètement avoir lieu. À cet égard, il convient d'interpréter l'article 39*bis*, § 9, du Code d'instruction criminelle de manière à ce qu'il ait un effet utile à la lumière de sa *ration legis*, qui est de protéger le secret professionnel de l'avocat et du médecin. Aussi, l'article 39*bis*, § 9, alinéa 2, du Code d'instruction criminelle doit être interprété comme obligeant le procureur du Roi à avertir le bâtonnier ou le représentant du conseil provincial de l'Ordre des médecins préalablement à la réalisation de la mesure, de sorte que celui-ci puisse y assister et qu'il soit en mesure d'examiner préalablement les documents, fichiers ou éléments que le procureur du Roi souhaite consulter et d'aviser celui-ci de ce qui, selon lui, relève du secret professionnel. Le représentant de l'ordre concerné peut par ailleurs recommander les mesures adéquates permettant de consulter certaines pièces, couvertes par le secret professionnel, sans compromettre ce secret.

C'est au procureur du Roi qu'il appartient de statuer sur le caractère confidentiel ou non des éléments qu'il souhaite consulter, après avoir recueilli l'avis, selon le cas, du bâtonnier ou du représentant du conseil provincial de l'Ordre des médecins. En cas de désaccord, le représentant de l'ordre concerné peut faire acter ses réserves dans le procès-verbal.

B.11.3. Dès lors que cette prérogative du procureur du Roi est le corollaire de sa compétence d'ordonner des recherches non secrètes dans un système informatique, comme il est dit en B.9.3, il n'est pas sans justification raisonnable que le procureur du Roi statue lui-même sur le caractère confidentiel ou non des éléments qu'il souhaite consulter, moyennant l'avis du représentant de l'ordre concerné et sans préjudice du contrôle de la chambre des mises en accusation et des juridictions de jugement. En effet, le procureur du Roi et légalement responsable du bon déroulement de l'information, qui consiste à rechercher les infractions, leurs auteurs et les preuves, et à rassembler les éléments utiles à l'exercice de l'action publique (article 28*bis*, § 1er, alinéas 1er et 3, du Code d'instruction criminelle).

B.11.4. En vertu de l'article 39*bis*, § 9, alinéa 2, du Code d'instruction criminelle, les éléments dont le procureur du Roi estime qu'ils relèvent du secret professionnel ne sont pas consignés au procès-verbal et le représentant de l'ordre concerné est tenu au secret.

[...]

B.14. Sous réserve de l'interprétation mentionnée en B.11.2, les deux moyens ne sont pas fondés ».

La même réserve d'interprétation s'applique à l'article 88*bis*, § 3, attaqué, du Code d'instruction criminelle.

B.121.2. Cette même interprétation doit s'imposer *mutatis mutandis* de manière générale pour toutes les données relevant du champ d'application de l'article 458 du Code pénal et, par conséquent, pour d'autres catégories de professionnels, selon les modalités et dans les conditions prévues par le législateur. Ainsi la règle du secret professionnel ne doit-elle céder, dans chaque cas concret où un juge d'instruction ou une autre autorité a accès aux données conservées, que si cela peut se justifier par un motif impérieux d'intérêt général et si la levée du secret est strictement proportionnée, eu égard à cet objectif.

B.122. Compte tenu de l'interprétation mentionnée en B.121, la loi du 20 juillet 2022 ne porte pas une atteinte discriminatoire au secret professionnel.

B.123. Le moyen unique dans l'affaire n° 7907, le moyen unique dans l'affaire n° 7929, les deuxième et cinquième moyens dans l'affaire n° 7930, ainsi que le premier moyen dans l'affaire n° 7932, en sa septième branche, et le troisième moyen dans l'affaire n° 7932, en sa troisième branche, ne sont pas fondés.

Par ces motifs,

la Cour

- avant de statuer sur les griefs relatifs aux articles 5, 6 et 24 de la loi du 20 juillet 2022 « relative à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités », 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 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) », lu en combinaison avec les articles 7, 8 et 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, doit-il être interprété en ce sens :

a) qu'il s'oppose à une législation nationale qui prévoit une obligation pour les opérateurs de services de communications électroniques de conserver et de traiter les données de trafic visées dans cette législation dans le cadre de la fourniture de ce réseau ou de ce service, pendant une période de quatre ou douze mois, selon le cas, afin qu'ils prennent les mesures appropriées, proportionnées, préventives et curatives de manière à éviter les fraudes et les utilisations malveillantes sur leurs réseaux et à empêcher que les utilisateurs finaux subissent un préjudice ou soient importunés, ainsi qu'à établir les fraudes ou les utilisations malveillantes du réseau ou du service ou à pouvoir en identifier les auteurs et l'origine;

b) qu'il s'oppose à une législation nationale qui permet à ces opérateurs de conserver et de traiter les données de trafic concernées au-delà des délais précités, en cas de fraude spécifique identifiée ou d'utilisation malveillante du réseau spécifique identifiée, le temps nécessaire à son analyse et à sa résolution ou le temps nécessaire au traitement de cette utilisation malveillante;

c) qu'il s'oppose à une législation nationale qui, sans prévoir l'obligation de solliciter un avis préalable ou de notifier à une autorité indépendante, permet à ces opérateurs de conserver et de traiter d'autres données que celles visées dans la loi, en vue de permettre d'établir la fraude ou l'utilisation malveillante du réseau ou du service, ou d'identifier son auteur et son origine;

d) qu'il s'oppose à une législation nationale qui, sans prévoir l'obligation de solliciter un avis préalable ou de notifier à une autorité indépendante, permet à ces opérateurs de conserver et de traiter pour une durée de douze mois les données de trafic qu'ils estiment nécessaires pour garantir la sécurité et le bon fonctionnement de leurs réseaux et services de communications électroniques, et en particulier pour détecter et analyser une atteinte potentielle ou réelle à cette sécurité, en ce compris pour identifier l'origine de cette atteinte et, en cas d'atteinte spécifique à la sécurité du réseau, pendant la durée nécessaire pour la traiter ?

2. L'article 15, paragraphe 1, de la directive 2002/58/CE, lu en combinaison avec les articles 7, 8 et 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, doit-il être interprété en ce sens :

a) qu'il s'oppose à une législation nationale qui permet aux opérateurs de réseaux mobiles de conserver et de traiter les données de localisation, sans que la législation décrive précisément quelles données sont visées, dans le cadre de la fourniture de ce réseau ou de ce service, pendant une période de quatre ou douze mois, selon le cas, lorsque cela est nécessaire pour le bon fonctionnement et la sécurité du réseau ou du service, ou pour détecter ou analyser les fraudes ou l'utilisation malveillante du réseau;

b) qu'il s'oppose à une législation nationale qui permet à ces opérateurs de conserver et de traiter les données de localisation au-delà des délais précités, en cas d'atteinte spécifique, de fraude spécifique ou d'utilisation malveillante spécifique ?

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 certaines dispositions de la loi du 20 juillet 2022 « relative à la collecte et à la conservation des données

d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités » violent une ou plusieurs des obligations découlant des dispositions mentionnées dans ces questions, pourrait-elle maintenir provisoirement les effets des dispositions précitées de la loi du 20 juillet 2022 afin d'éviter une insécurité juridique et de permettre que les données collectées et conservées précédemment puissent encore être utilisées pour les objectifs visés dans la loi ?

- Sous réserve de l'interprétation mentionnée en B.121, rejette les autres griefs.

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 26 septembre 2024.

Le greffier, Le président,

Nicolas Dupont Pierre Nihoul