CONSEIL D'ÉTAT
section de législation

avis 69.381/4
du 28 juin 2021

sur

un avant-projet de loi 'relatif à la collecte et à la conservation des données d'identification, de trafic et de localisation dans le secteur des communications électroniques et à leur accès par les autorités'

RAAD VAN STATE
afdeling Wetgeving

advies 69.381/4
van 28 juni 2021

over

een voorontwerp van wet 'betreffende het verzamelen en het bewaren van de identificatie-, verkeers-en locatiegegevens in de sector van de elektronische communicatie en de toegang daartoe voor de autoriteiten'

‡LW-BEHVMBJEH-GJDIBQW‡

Le 10 mai 2021, le Conseil d'État, section de législation, a été invité par le Vice-Premier Ministre et Ministre de la Justice et de la Mer du Nord à communiquer un avis, dans un délai de trente jours, sur un avant-projet de loi 'relatif à la collecte et à la conservation des données d'identification, de trafic et de localisation dans le secteur des communications électroniques et à leur accès par les autorités'.

L'avant-projet a été examiné par la quatrième chambre le 28 juin 2021. La chambre était composée de Martine BAGUET, président de chambre, Luc CAMBIER et Bernard BLERO, conseillers d'État, Sébastien VAN DROOGHENBROECK et Marianne DONY, assesseurs, et Anne-Catherine VAN GEERSDAELE, greffier.

Le rapport a été présenté par Anne VAGMAN, premier auditeur.

La concordance entre la version française et la version néerlandaise a été vérifiée sous le contrôle de Martine BAGUET.

L'avis, dont le texte suit, a été donné le 28 juin 2021.

*

Op 10 mei 2021 is de Raad van State, afdeling Wetgeving, door de Vice-eersteminister en Minister van Justitie en Noordzee verzocht binnen een termijn van dertig dagen een advies te verstrekken over een voorontwerp van wet 'betreffende het verzamelen en het bewaren van de identificatie-, verkeers-en locatiegegevens in de sector van de elektronische communicatie en de toegang daartoe voor de autoriteiten'.

Het voorontwerp is door de vierde kamer onderzocht op 28 juni 2021. De kamer was samengesteld uit Martine BAGUET, kamervoorzitter, Luc CAMBIER en Bernard BLERO, staatsraden, Sébastien VAN DROOGHENBROECK en Marianne DONY, assessoren, en Anne-Catherine VAN GEERSDAELE, griffier.

Het verslag is uitgebracht door Anne VAGMAN, eerste auditeur.

De overeenstemming tussen de Franse en de Nederlandse tekst van het advies is nagezien onder toezicht van Martine BAGUET.

Het advies, waarvan de tekst hierna volgt, is gegeven op 28 juni 2021.

*

‡LW-BEHVMBJEH-GJDIBQW‡

Comme la demande d'avis est introduite sur la base de l'article 84, § 1er, alinéa 1er, 2°, des lois 'sur le Conseil d'État', coordonnées le 12 janvier 1973, la section de législation limite son examen au fondement juridique de l'avant-projet ‡, à la compétence de l'auteur de l'acte ainsi qu'à l'accomplissement des formalités préalables, conformément à l'article 84, § 3, des lois coordonnées précitées.

Sur ces trois points, l'avant-projet appelle les observations suivantes.

FORMALITÉS PRÉALABLES

L'avant-projet de loi soumis pour avis a été délibéré en Conseil des ministres du 7 mai 2021, où il a été décidé que le texte en projet adopté fera l'objet d'une consultation publique et sera adressé pour avis aux Autorités de protection des données et au Conseil d'État. Les résultats de ces différentes consultations seront alors discutés au sein du Groupe de travail de coordination de la politique concerné et l'avant-projet, le cas échéant adapté, sera ensuite soumis au Comité interministériel des Télécommunications et de la Radiodiffusion et la Télévision, et au Comité de concertation [1].

À la suite de cette concertation, le Groupe de travail se réunira à nouveau et si « des problèmes se posent encore au sein du Groupe de travail, en ce qui concerne les adaptations éventuelles nécessaire », le texte en projet sera à nouveau soumis au Conseil des Ministres. Si par contre, aucun problème de ne se pose au sein du Groupe de travail, l'avant-projet sera soumis à la signature du Roi, en vue de son dépôt à la chambre des représentants.

La section de législation relève en outre que l'avis de l'Organe de contrôle de l'information policière a été donné le 21 mai 2021 ; la consultation publique s'est, pour sa part, clôturée le 4 juin 2021 ; enfin, l'avis du Comité Permanent R a été donné le 14 juin 2021. Ces documents ont été transmis à la section de législation postérieurement à l'introduction de la demande d'avis et sont également postérieurs, à fortiori, à la délibération du Conseil des ministres du 7 mai 2021.

Il résulte de ce qui précède que le texte soumis pour avis est encore susceptible de subir des modifications autres que celles qui pourraient découler de l'avis de la section de législation : ainsi il pourrait faire l'objet de modifications à la suite de la consultation publique, des avis des autorités de protection des données, de l'Organe de contrôle de l'information policière et du Comité permanent R et à l'issue de la concertation organisée au sein du Comité interministériel et du Comité de concertation.

Or, et même si la section de législation est tenue de se prononcer sur un avant-projet législatif ou sur un projet réglementaire, même lorsque les formalités préalables obligatoires n'ont pas été accomplies [2], pour que celle-ci puisse accomplir correctement sa

‡ S'agissant d'un avant-projet de loi, on entend par « fondement juridique » la conformité aux normes supérieures.

[1] Ceci ressort également de la lettre de demande d'avis.

[2] Il résulte de l'article 84, § 3, alinéa 2, des lois 'sur le Conseil d'État', coordonnées le 12 janvier 1973, que lorsque l'avis de la section de législation est sollicité dans un délai de trente ou soixante jours, ou de cinq jours ouvrables, l'avis est donné « nonobstant l'inaccomplissement éventuel des formalités prescrites ».

‡LW-BEHVMBJEH-GJDIBQW‡

mission, il y a toutefois lieu de lui soumettre des projets de texte à priori définitifs, non seulement pour éviter qu'elle n'examine inutilement un texte qui fera l'objet de modifications ultérieures, mais également pour qu'un projet ne doive lui être soumis à nouveau pour avis en raison de modifications autres que celles résultant de son avis [3].

Les auteurs de l'avant-projet sont invités à se conformer dorénavant à la règle ainsi rappelée.

PORTÉE ET CONTEXTE DE L'AVANT-PROJET

A. DROIT ET JURISPRUDENCE EUROPÉENS ET JURISPRUDENCE INTERNE

1.1. Par un arrêt du 8 avril 2014, rendu en grande chambre en réponse aux questions préjudicielles de la Haute Cour d'Irlande et de la Cour constitutionnelle d'Autriche [4], la Cour de Justice de l'Union européenne (ci-après « La Cour de Justice ») a invalidé la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 'sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications électroniques, et modifiant la directive 2002/58/CE'.

À la suite de cet arrêt de la Cour de Justice, l'arrêt 84/2015 du 11 juin 2015 de la Cour constitutionnelle a annulé 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', laquelle avait pour objet d'assurer la transposition partielle de la directive 2006/24/CE.

L'arrêt de la Cour constitutionnelle repose sur la motivation suivante :

> « B.10.1. Comme la Cour de justice l'a relevé aux points 56 et 57 de son arrêt, la directive impose la conservation de toutes les données relatives au trafic concernant la téléphonie fixe, la téléphonie mobile, l'accès à l'internet, le courrier électronique par internet ainsi que la téléphonie par l'internet, couvrant de manière généralisée toute personne et tous les moyens de communication électronique sans distinction en fonction de l'objectif de lutte contre les infractions graves que le législateur de l'Union entendait poursuivre.
>
> La loi attaquée ne se distingue nullement de la directive sur ce point. En effet, ainsi qu'il est dit en B.8, les catégories de données qui doivent être conservées sont identiques à celles énumérées par la directive tandis qu'aucune distinction n'est opérée quant aux personnes concernées ou aux règles particulières à prévoir en fonction de l'objectif de lutte contre les infractions décrites à l'article 126, § 2, de la loi du 13 juin 2005 remplacé par la loi attaquée. Tout comme la Cour de justice l'a constaté à propos de la directive (point 58), la loi s'applique donc également à des personnes pour lesquelles il

[3] Voir, en ce sens l'avis n° 39.690/3 donné le 8 février 2006 sur un avant-projet devenu la loi du 20 juillet 2006 'relative à la création et au fonctionnement de l'Agence fédérale des médicaments et des produits de santé', http://www.raadvst-consetat.be/dbx/avis/39690.pdf.

[4] C.J.(gde ch.), arrêt *Digital Rights Ireland Ltd c. Minister for communications, Marine and Natural Resouces e.a.*, 8 avril 2014, C-293/12, ECLI:EU:C:2014:238 et C.J. (gde ch.), arrêt *Kärntner Landesregierung e.a. c. Autriche*, C-594/12, ECLI:EU:C:2014:238, ci-après, l'arrêt « *Digital Rights* »).

‡LW-BEHVMBJEH-GJDIBQW‡

n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec les infractions énumérées par la loi attaquée. De même, la loi s'applique sans aucune exception, également à des personnes dont les communications sont soumises au secret professionnel.

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

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

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

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

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

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

1.2. Faisant suite à ces deux décisions, le législateur a adopté la loi du 29 mai 2016 'relative à la collecte et à la conservation des données dans le secteur des communications électroniques' [5].

Cette loi a fait l'objet de quatre recours en annulation auprès de la Cour constitutionnelle, qui a posé, par son arrêt n° 96/2018 du 19 juillet 2018, les questions préjudicielles suivantes à la Cour de Justice :

« 1. L'article 15, paragraphe 1, de la directive 2002/58/CE, lu en combinaison avec le droit à la sécurité, garanti par l'article 6 de la Charte des droits fondamentaux de l'Union européenne, et le droit au respect des données personnelles, tel que garanti par les articles 7, 8 et 52, § 1er [lire : paragraphe 1], de la Charte des droits fondamentaux de l'Union européenne, doit-il être interprété en ce sens qu'il s'oppose à une réglementation nationale telle que celle en cause, qui prévoit une obligation générale pour les opérateurs et fournisseurs de services de communications électroniques de conserver les données de trafic et de localisation au sens de la directive 2002/58/CE, générées ou traitées par eux

[5] La section de législation a, le 7 décembre 2015, donné un avis n° 58.449/4 sur un avant-projet devenu cette loi du 29 mai 2016, http://www.raadvst-consetat.be/dbx/avis/58449.pdf.

‡LW-BEHVMBJEH-GJDIBQW‡

dans le cadre de la fourniture de ces services, réglementation nationale qui n'a pas seulement pour objectif la recherche, la détection et la poursuite de faits de criminalité grave, mais également la garantie de la sécurité nationale, de la défense du territoire et de la sécurité publique, la recherche, la détection et la poursuite d'autres faits que ceux de criminalité grave ou la prévention d'un usage interdit des systèmes de communication électronique, ou la réalisation d'un autre objectif identifié par l'article 23, paragraphe 1, du règlement (UE) 2016/679 et qui est en outre sujette à des garanties précisées dans cette réglementation sur le plan de la conservation des données et de l'accès à celles-ci ?

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

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

Dans ce même arrêt, la Cour constitutionnelle a décidé de

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

1.3.1. La Cour de Justice a répondu à ces questions préjudicielles, ainsi qu'à d'autres questions posées par le Conseil d'État de France, dans un arrêt du 6 octobre 2020, rendu en grande chambre [6] (ci-après l'arrêt « *La Quadrature du Net* »).

1.3.2. Concernant les deux premières questions préjudicielles posées par la Cour constitutionnelle, l'arrêt de la Cour de Justice a motivé sa réponse comme suit :

« 108. S'agissant, en particulier, du traitement et du stockage des données relatives au trafic par les fournisseurs de services de communications électroniques, il ressort de l'article 6 ainsi que des considérants 22 et 26 de la directive 2002/58 qu'un tel traitement n'est autorisé que dans la mesure et pour la durée nécessaires à la commercialisation des services, à la facturation de ceux-ci et à la fourniture de services à valeur ajoutée. Une fois cette durée expirée, les données ayant été traitées et stockées doivent être effacées ou

[6] C.J. (gde ch.), arrêt *La Quadrature du Net et autres c. Premier ministre e.a.,* 6 octobre 2020, C-511/18, ECLI:EU:C:2020:791 et C.J. (gde ch.), arrêt *French Data network e.a*., C-512/18 et C.J. (gde ch.), arrêt *Ordre des barreaux francophones et germanophone et autres*, C-520/18.

‡LW-BEHVMBJEH-GJDIBQW‡

rendues anonymes. Quant aux données de localisation autres que les données relatives au trafic, l'article 9, paragraphe 1, de ladite directive prévoit que ces données ne peuvent être traitées que sous certaines conditions et après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés (arrêt du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, point 86 et jurisprudence citée).

109. Ainsi, en adoptant cette directive, le législateur de l'Union a concrétisé les droits consacrés aux articles 7 et 8 de la Charte, de telle sorte que les utilisateurs des moyens de communications électroniques sont en droit de s'attendre, en principe, à ce que leurs communications et les données y afférentes restent, en l'absence de leur consentement, anonymes et ne puissent pas faire l'objet d'un enregistrement.

110.Toutefois, l'article 15, paragraphe 1, de la directive 2002/58 permet aux États membres d'introduire des exceptions à l'obligation de principe, énoncée à l'article 5, paragraphe 1, de cette directive, de garantir la confidentialité des données à caractère personnel ainsi qu'aux obligations correspondantes, mentionnées notamment aux articles 6 et 9 de ladite directive, lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale, la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques. 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 l'un de ces motifs.

111. Cela étant, la faculté de déroger aux droits et aux obligations prévus aux articles 5, 6 et 9 de la directive 2002/58 ne saurait justifier que la dérogation à l'obligation de principe de garantir la confidentialité des communications électroniques et des données y afférentes et, en particulier, à l'interdiction de stocker ces données, explicitement prévue à l'article 5 de cette directive, devienne la règle (voir, en ce sens, arrêt du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, points 89 et 104).

112. Quant aux objectifs susceptibles de justifier une limitation des droits et des obligations prévus, notamment, aux articles 5, 6 et 9 de la directive 2002/58, la Cour a déjà jugé que l'énumération des objectifs figurant à l'article 15, paragraphe 1, première phrase, de cette directive revêt un caractère exhaustif, de telle sorte qu'une mesure législative adoptée au titre de cette disposition doit répondre effectivement et strictement à l'un de ces objectifs (voir, en ce sens, arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, point 52 et jurisprudence citée).

113. En outre, il ressort de l'article 15, paragraphe 1, troisième phrase, de la directive 2002/58 que les États membres ne sont autorisés à prendre des mesures législatives visant à limiter la portée des droits et des obligations visés aux articles 5, 6 et 9 de cette directive que dans le respect des principes généraux du droit de l'Union, parmi lesquels figure le principe de proportionnalité, et des droits fondamentaux garantis par la Charte. À cet égard, la Cour a déjà jugé que l'obligation imposée par un État membre aux fournisseurs de services de communications électroniques, par une réglementation nationale, de conserver les données relatives au trafic aux fins de les rendre, le cas échéant, accessibles aux autorités nationales compétentes soulève des questions relatives au respect non seulement des articles 7 et 8 de la Charte, relatifs, respectivement à la protection de la vie privée ainsi qu'à la protection des données à caractère personnel, mais également de l'article 11 de la Charte, relatif à la liberté d'expression (voir, en ce sens, arrêts du 8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, points 25 et 70, ainsi que du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, points 91 et 92 ainsi que jurisprudence citée).

‡LW-BEHVMBJEH-GJDIBQW‡

114. Ainsi, l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58 doit tenir compte de l'importance tant du droit au respect de la vie privée, garanti à l'article 7 de la Charte, que du droit à la protection des données à caractère personnel, garanti à l'article 8 de celle-ci, telle qu'elle ressort de la jurisprudence de la Cour, ainsi que du droit à la liberté d'expression, ce droit fondamental, garanti à l'article 11 de la Charte, constituant l'un des fondements essentiels d'une société démocratique et pluraliste et faisant partie des valeurs sur lesquelles est, conformément à l'article 2 TUE, fondée l'Union (voir, en ce sens, arrêts du 6 mars 2001, Connolly/Commission, C-274/99P, EU:C:2001:127, point 39, ainsi que du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, point 93 et jurisprudence citée).

115. Il y a lieu de préciser, à cet égard, que la conservation des données relatives au trafic et des données de localisation constitue, par elle-même, d'une part, une dérogation à l'interdiction, prévue à l'article 5, paragraphe 1, de la directive 2002/58, faite à toute autre personne que les utilisateurs de stocker ces données et, d'autre part, une ingérence dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, consacrés aux articles 7 et 8 de la Charte, sans qu'il importe de savoir si les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou si les intéressés ont ou non subi d'éventuels inconvénients en raison de cette ingérence [voir, en ce sens, avis 1/15 (Accord PNRUE-Canada), du 26 juillet 2017, EU:C:2017:592, points 124 et 126 ainsi que jurisprudence citée ; voir, par analogie, en ce qui concerne l'article 8 de la CEDH, Cour EDH, 30 janvier 2020, Breyer c. Allemagne, CE:ECHR:2020:0130 JUD005000 112, § 81].

116. Il est également sans pertinence que les données conservées soient ou non utilisées par la suite (voir, par analogie, en ce qui concerne l'article 8 de la CEDH, Cour EDH, 16 février 2000, Amann c. Suisse, CE:ECHR:2000:0216JUD002779895, § 69, ainsi que 13 février 2020, Trjakovski et Chipovskic Macédoine du Nord, CE:ECHR:2020:0213JUD005320513, § 51), l'accès à de telles données constituant, quelle que soit l'utilisation qui en est faite ultérieurement, une ingérence distincte dans les droits fondamentaux visés au point précédent [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 124 et 126].

117. Cette conclusion apparaît d'autant plus justifiée que les données relatives au trafic et les données de localisation sont susceptibles de révéler des informations sur un nombre important d'aspects de la vie privée des personnes concernées, y compris des informations sensibles, telles que l'orientation sexuelle, les opinions politiques, les convictions religieuses, philosophiques, sociétales ou autres ainsi que l'état de santé, alors que de telles données jouissent, par ailleurs, d'une protection particulière en droit de l'Union. Prises dans leur ensemble, lesdites données peuvent permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci. En particulier, ces données fournissent les moyens d'établir le profil des personnes concernées, information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications (voir, en ce sens, arrêts du 8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, point 27, ainsi que du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, point 99).

118. Dès lors, d'une part, la conservation des données relatives au trafic et des données de localisation à des fins policières est susceptible, à elle seule, de porter atteinte au droit au respect des communications, consacré à l'article 7 de la Charte, et d'entraîner 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 celle-ci (voir, en ce

‡LW-BEHVMBJEH-GJDIBQW‡

sens, arrêts du 8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, point 28, ainsi que du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, point 101). Or, de tels effets dissuasifs peuvent affecter en particulier les personnes dont les communications sont soumises, selon les règles nationales, au secret professionnel ainsi que les lanceurs d'alerte dont les activités sont protégées par la directive (UE) 2019/1937 du Parlement européen et du Conseil, du 23 octobre 2019, sur la protection des personnes qui signalent des violations du droit de l'Union (JO 2019, L 305, p. 17). En outre, ces effets sont d'autant plus graves que le nombre et la variété des données conservées sont élevés.

119. D'autre part, compte tenu de la quantité importante de données relatives au trafic et de données de localisation susceptibles d'être conservées de manière continue par une mesure de conservation généralisée et indifférenciée ainsi que du caractère sensible des informations que ces données peuvent fournir, la seule conservation desdites données par les fournisseurs de services de communications électroniques comporte des risques d'abus et d'accès illicite.

120. Cela étant, en ce qu'il permet aux États membres d'introduire les dérogations visées au point 110 du présent arrêt, l'article 15, paragraphe 1, de la directive 2002/58 reflète la circonstance que les droits consacrés aux articles 7, 8 et 11 de la Charte n'apparaissent pas comme étant des prérogatives absolues, mais doivent être pris en considération par rapport à leur fonction dans la société (voir, en ce sens, arrêt du 16 juillet 2020, Facebook Ireland et Schrems, C-311/18, EU:C:2020:559, point 172 ainsi que jurisprudence citée).

121. En effet, ainsi qu'il ressort de l'article 52, paragraphe 1, de la Charte, celle-ci admet des limitations à l'exercice de ces droits, pour autant que ces limitations soient prévues par la loi, qu'elles respectent le contenu essentiel desdits droits et que, dans le respect du principe de proportionnalité, elles soient nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui.

122. Ainsi, l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58 à la lumière de la Charte requiert de tenir compte également de l'importance des droits consacrés aux articles 3, 4, 6 et 7 de la Charte et de celle que revêtent les objectifs de protection de la sécurité nationale et de lutte contre la criminalité grave en contribuant à la protection des droits et des libertés d'autrui.

123. À cet égard, l'article 6 de la Charte, auquel se réfèrent le Conseil d'État et la Cour constitutionnelle, consacre le droit de toute personne non seulement à la liberté mais également à la sûreté et garantit des droits correspondant à ceux qui le sont à l'article 5 de la CEDH (voir, en ce sens, arrêts du 15 février 2016, N., C-601/15PPU, EU:C:2016:84, point 47 ; du 28 juillet 2016, JZ, C-294/16PPU, EU:C:2016:610, point 48, ainsi que du 19 septembre 2019, Rayonna prokuratura Lom, C-467/18, EU:C:2019:765, point 42 et jurisprudence citée).

124. En outre, il y a lieu de rappeler que l'article 52, paragraphe 3, de la Charte vise à assurer la cohérence nécessaire entre les droits contenus dans cette dernière et les droits correspondants garantis par la CEDH, sans porter atteinte à l'autonomie du droit de l'Union et de la Cour de justice de l'Union européenne. Il convient donc de tenir compte des droits correspondants de la CEDH en vue de l'interprétation de la Charte, en tant que seuil de protection minimale [voir, en ce sens, arrêts du 12 février 2019, TC, C-492/18PPU, EU:C:2019:108, point 57, ainsi que du 21 mai 2019, Commission/Hongrie (Usufruits sur terres agricoles), C-235/17, EU:C:2019:432, point 72 et jurisprudence citée].

‡LW-BEHVMBJEH-GJDIBQW‡

125. S'agissant de l'article 5 de la CEDH, qui consacre le 'droit à la liberté' et le 'droit à la sûreté', celui-ci vise, selon la jurisprudence de la Cour européenne des droits de l'homme, à protéger l'individu contre toute privation de liberté arbitraire ou injustifiée (voir, en ce sens, Cour EDH, 18 mars 2008, Ladent c. Pologne, CE:ECHR:2008:0318JUD001103603, §§ 45 et 46 ; 29 mars 2010, Medvedyev et autres c. France, CE:ECHR:2010:0329JUD000339403, §§ 76 et 77, ainsi que 13 décembre 2012, El-Masri v. 'The former Yugoslav Republic of Macedonia', CE:ECHR:2012:1213JUD003963009, § 239). Toutefois, dans la mesure où cette disposition vise une privation de liberté commise par une autorité publique, l'article 6 de la Charte ne saurait être interprété comme imposant aux pouvoirs publics une obligation d'adopter des mesures spécifiques en vue de réprimer certaines infractions pénales.

126. En revanche, en ce qui concerne, en particulier, la lutte effective contre les infractions pénales dont sont victimes, notamment, les mineurs et les autres personnes vulnérables, évoquée par la Cour constitutionnelle, il convient de souligner que des obligations positives à la charge des pouvoirs publics peuvent résulter de l'article 7 de la Charte, en vue de l'adoption de mesures juridiques visant à protéger la vie privée et familiale [voir, en ce sens, arrêt du 18 juin 2020, Commission/Hongrie (Transparence associative), C-78/18, EU:C:2020:476, point 123 et jurisprudence citée de la Cour européenne des droits de l'homme]. De telles obligations sont également susceptibles de découler dudit article 7 en ce qui concerne la protection du domicile et des communications, ainsi que des articles 3 et 4 s'agissant de la protection de l'intégrité physique et psychique des personnes ainsi que de l'interdiction de la torture et des traitements inhumains et dégradants.

127. Or, face à ces différentes obligations positives, il convient de procéder à une conciliation nécessaire des différents intérêts et droits en cause.

128. En effet, la Cour européenne des droits de l'homme a jugé que les obligations positives découlant des articles 3 et 8 de la CEDH, dont les garanties correspondantes figurent aux articles 4 et 7 de la Charte, impliquent, notamment, l'adoption de dispositions matérielles et procédurales ainsi que de mesures d'ordre pratique permettant une lutte efficace à l'encontre des infractions contre les personnes à travers une enquête et des poursuites effectives, cette obligation étant d'autant plus importante lorsque le bien-être physique et moral d'un enfant est menacé. Cela étant, les mesures qu'il appartient aux autorités compétentes de prendre doivent pleinement respecter les voies légales et les autres garanties qui sont de nature à limiter l'étendue des pouvoirs d'investigations pénales ainsi que les autres libertés et droits. En particulier, selon cette juridiction, il convient d'instaurer un cadre légal permettant de concilier les différentes intérêts et droits à protéger (Cour EDH, 28 octobre 1998, Osman c. Royaume-Uni, CE:ECHR:1998:1028JUD002345294, §§ 115 et 116 ; 4 mars 2004, M.C. c. Bulgarie, CE:ECHR:2003:1204JUD003927298, § 151 ; 24 juin 2004, Von Hannover c. Allemagne, CE:ECHR:2004:0624JUD005932000, §§ 57 et 58, ainsi que 2 décembre 2008, K.U. c. Finlande, CE:ECHR:2008:1202JUD000287202, §§ 46, 48 et 49).

129. En ce qui concerne le respect du principe de proportionnalité, l'article 15, paragraphe 1, première phrase, de la directive 2002/58 dispose que les États membres peuvent adopter une mesure dérogeant au principe de confidentialité des communications et des données relatives au trafic y afférentes lorsqu'une telle mesure est 'nécessaire, appropriée et proportionnée, au sein d'une société démocratique', au regard des objectifs que cette disposition énonce. Le considérant 11 de cette directive précise qu'une mesure de cette nature doit être 'rigoureusement' proportionnée au but poursuivi.

‡LW-BEHVMBJEH-GJDIBQW‡

130. À cet égard, il convient de rappeler que la protection du droit fondamental au respect de la vie privée exige, conformément à la jurisprudence constante de la Cour, que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire. En outre, un objectif d'intérêt général ne saurait être poursuivi sans tenir compte du fait qu'il doit être concilié avec les droits fondamentaux concernés par la mesure, ce en effectuant une pondération équilibrée entre, d'une part, l'objectif d'intérêt général et, d'autre part, les droits en cause [voir, en ce sens, arrêts du 16 décembre 2008, Satakunnan Markkinapörssi et Satamedia, C-73/07, EU:C:2008:727, point 56 ; du 9 novembre 2010, Volker und Markus Schecke et Eifert, C-92/09 et C-93/09, EU:C:2010:662, points 76, 77 et 86, ainsi que du 8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, point 52 ; avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 140].

131. Plus particulièrement, il découle de la jurisprudence de la Cour que la possibilité pour les États membres de justifier une limitation aux droits et aux obligations prévus, notamment, aux articles 5, 6 et 9 de la directive 2002/58 doit être appréciée en mesurant la gravité de l'ingérence que comporte une telle limitation et en vérifiant que l'importance de l'objectif d'intérêt général poursuivi par cette limitation est en relation avec cette gravité (voir, en ce sens, arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, point 55 et jurisprudence citée).

132. Pour satisfaire à l'exigence de proportionnalité, une réglementation doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de telle sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus. Cette réglementation doit être légalement contraignante en droit interne et, en particulier, indiquer en quelles circonstances et sous quelles conditions une mesure prévoyant le traitement de telles données peut être prise, garantissant ainsi que l'ingérence soit limitée au strict nécessaire. La nécessité de disposer de telles garanties est d'autant plus importante lorsque les données à caractère personnel sont soumises à un traitement automatisé, notamment lorsqu'il existe un risque important d'accès illicite à ces données. Ces considérations valent en particulier lorsqu'est en jeu la protection de cette catégorie particulière de données à caractère personnel que sont les données sensibles [voir, en ce sens, arrêts du 8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, points 54 et 55, ainsi que du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, point 117 ; avis 1/15(Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 141].

133. Ainsi, une réglementation prévoyant une conservation des données à caractère personnel doit toujours répondre à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 191 et jurisprudence citée, ainsi que arrêt du 3 octobre 2019, A e.a., C-70/18, EU:C:2019:823, point 63].

- Sur les mesures législatives prévoyant la conservation préventive des données relatives au trafic et des données de localisation aux fins de la sauvegarde de la sécurité national.

134. Il y a lieu de faire observer que l'objectif de sauvegarde de la sécurité nationale, évoqué par les juridictions de renvoi et les gouvernements ayant présenté des observations, n'a pas encore été spécifiquement examiné par la Cour dans ses arrêts interprétant la directive 2002/58.

‡LW-BEHVMBJEH-GJDIBQW‡

135. 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.

136. Or, l'importance de l'objectif de sauvegarde de la sécurité nationale, lu à l'aune de l'article 4, paragraphe 2, TUE, dépasse celle des autres objectifs visés à l'article 15, paragraphe 1, de la directive 2002/58, notamment des objectifs de lutte contre la criminalité en général, même grave, ainsi que de sauvegarde de la sécurité publique. En effet, des menaces telles que celles visées au point précédent se distinguent, par leur nature et leur particulière gravité, du risque général de survenance de tensions ou de troubles, même graves, à la sécurité publique. Sous réserve du respect des autres exigences prévues à l'article 52, paragraphe 1, de la Charte, l'objectif de sauvegarde de la sécurité nationale est dès lors susceptible de justifier des mesures comportant des ingérences dans les droits fondamentaux plus graves que celles que pourraient justifier ces autres objectifs.

137. Ainsi, dans des situations telles que celles décrites aux points 135 et 136 du présent arrêt, l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, ne s'oppose pas, en principe, à une mesure législative qui autorise les autorités compétentes à enjoindre aux fournisseurs de services de communications électroniques de procéder à la conservation des données relatives au trafic et des données de localisation de l'ensemble des utilisateurs des moyens de communications électroniques pendant une période limitée, dès lors qu'il existe des circonstances suffisamment concrètes permettant de considérer que l'État membre concerné fait face à une menace grave telle que celle visée aux points 135 et 136 du présent arrêt pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible. Même si une telle mesure vise, de manière indifférenciée, tous les utilisateurs de moyens de communications électroniques sans que ceux-ci paraissent, de prime abord, présenter de rapport, au sens de la jurisprudence visée au point 133 du présent arrêt, avec une menace pour la sécurité nationale de cet État membre, il y a lieu néanmoins de considérer que l'existence d'une telle menace est de nature, par elle-même, à établir ce rapport.

138. L'injonction prévoyant la conservation préventive des données de l'ensemble des utilisateurs des moyens de communications électroniques doit, néanmoins, être temporellement limitée au strict nécessaire. S'il ne peut être exclu que l'injonction faite aux fournisseurs de services de communications électroniques de procéder à la conservation des données puisse, en raison de la persistance d'une telle menace, être renouvelée, la durée de chaque injonction ne saurait dépasser un laps de temps prévisible. De surcroît, une telle conservation des données doit être sujette à des limitations et encadrée par des garanties strictes permettant de protéger efficacement les données à caractère personnel des personnes concernées contre les risques d'abus. Ainsi, cette conservation ne saurait présenter un caractère systématique.

139. Eu égard à la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte résultant d'une telle mesure de conservation généralisée et indifférenciée des données, il importe d'assurer que le recours à celle-ci soit effectivement limité aux situations dans lesquelles il existe une menace grave pour la sécurité nationale, telles que celles visées aux points 135 et 136 du présent arrêt. À cet effet, il est essentiel qu'une décision faisant injonction aux fournisseurs de services de communications électroniques de procéder à une telle conservation des données puisse faire l'objet d'un

‡LW-BEHVMBJEH-GJDIBQW‡

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.

- *Sur les mesures législatives prévoyant la conservation préventive des données relatives au trafic et des données de localisation aux fins de la lutte contre la criminalité et de la sauvegarde de la sécurité publique.*

140. Pour ce qui est de l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales, conformément au principe de proportionnalité, seules la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique sont de nature à justifier des ingérences graves dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, telles que celles qu'implique la conservation des données relatives au trafic et des données de localisation. Dès lors, seules des ingérences dans lesdits droits fondamentaux ne présentant pas un caractère grave peuvent être justifiées par l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales en général [voir, en ce sens, arrêts du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, point 102, ainsi que du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, points 56 et 57 ; avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 149].

141. Une réglementation nationale prévoyant la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, en vue de lutter contre la criminalité grave, excède les limites du strict nécessaire et ne saurait être considérée comme étant justifiée dans une société démocratique, ainsi que l'exige l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte (voir, en ce sens, arrêt du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, point 107).

142. En effet, compte tenu du caractère sensible des informations que peuvent fournir les données relatives au trafic et les données de localisation, la confidentialité de ces dernières est essentielle pour le droit au respect de la vie privée. Ainsi, et compte tenu, d'une part, des effets dissuasifs sur l'exercice des droits fondamentaux consacrés aux articles 7 et 11 de la Charte, visés au point 118 du présent arrêt, que la conservation de ces données est susceptible d'entraîner et, d'autre part, de la gravité de l'ingérence que comporte une telle conservation, il importe, dans une société démocratique, que celle-ci soit, comme le prévoit le système mis en place par la directive 2002/58, l'exception et non la règle et que ces données ne puissent faire l'objet d'une conservation systématique et continue. Cette conclusion s'impose même à l'égard des objectifs de lutte contre la criminalité grave et de prévention des menaces graves contre la sécurité publique ainsi que de l'importance qu'il convient de leur reconnaître.

143. En outre, la Cour a souligné qu'une réglementation prévoyant la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation couvre les communications électroniques de la quasi-totalité de la population sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif poursuivi. Une telle réglementation, contrairement à l'exigence rappelée au point 133 du présent arrêt, concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques, sans que ces personnes se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales. Elle s'applique donc même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec cet objectif de lutte contre des actes de criminalité grave et, en particulier, sans que soit prévue une relation entre les données dont la conservation est prévue et une menace pour la sécurité publique (voir, en ce sens, arrêts du 8 avril 2014, Digital Rights, C-293/12 et

‡LW-BEHVMBJEH-GJDIBQW‡

C-594/12, EU:C:2014:238, points 57 et 58, ainsi que du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, point 105).

144. En particulier, comme l'a déjà jugé la Cour, une telle réglementation n'est pas limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique et/ou sur un cercle de personnes susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la lutte contre la criminalité grave (voir, en ce sens, arrêts du 8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, point 59, et du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, point 106).

145. Or, même les obligations positives des États membres susceptibles de découler, selon le cas, des articles 3, 4 et 7 de la Charte et portant, ainsi qu'il a été relevé aux points 126 et 128 du présent arrêt, sur la mise en place de règles permettant une lutte effective contre les infractions pénales ne sauraient avoir pour effet de justifier des ingérences aussi graves que celles que comporte une réglementation prévoyant une conservation des données relatives au trafic et des données de localisation dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte de la quasi-totalité de la population sans que les données des personnes concernées soient susceptibles de révéler un lien, au moins indirect, avec l'objectif poursuivi.

146. En revanche, conformément à ce qui a été relevé aux points 142 à 144 du présent arrêt, et eu égard à la conciliation nécessaire des droits et des intérêts en cause, les objectifs de lutte contre la criminalité grave, de prévention d'atteintes graves à la sécurité publique et, a fortiori, de sauvegarde de la sécurité nationale sont susceptibles de justifier, compte tenu de leur importance, au regard des obligations positives rappelées au point précédent et auxquelles s'est référée notamment la Cour constitutionnelle, l'ingérence particulièrement grave que comporte une conservation ciblée des données relatives au trafic et des données de localisation.

147. Ainsi, comme l'a déjà jugé la Cour, l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, ne s'oppose pas à ce qu'un État membre adopte une réglementation permettant, à titre préventif, une conservation ciblée des données relatives au trafic et des données de localisation aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, tout comme aux fins de la sauvegarde de la sécurité nationale, à condition qu'une telle conservation soit, en ce qui concerne les catégories de données à conserver, les moyens de communication visés, les personnes concernées ainsi que la durée de conservation retenue, limitée au strict nécessaire (voir, en ce sens, arrêt du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, point 108).

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, Télé2, C-203/15 et C-698/15, EU:C:2016:970, point 111).

‡LW-BEHVMBJEH-GJDIBQW‡

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, Télé2, 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.

- *Sur les mesures législatives prévoyant la conservation préventive des adresses IP et des données relatives à l'identité civile aux fins de la lutte contre la criminalité et de la sauvegarde de la sécurité publique.*

152. Il y a lieu de relever que les adresses IP, quoique faisant partie des données relatives au trafic, sont générées sans être rattachées à une communication déterminée et servent principalement à identifier, par l'intermédiaire des fournisseurs de services de communications électroniques, la personne physique propriétaire d'un équipement terminal à partir duquel une communication au moyen de l'Internet est effectuée. Ainsi, en matière de courrier électronique ainsi que 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. Cette catégorie de données présente donc un degré de sensibilité moindre que les autres données relatives au trafic.

153. Toutefois, les adresses IP pouvant 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 desdites adresses IP que nécessite un tel traçage constituent des ingérences graves dans les droits fondamentaux de l'internaute consacrés aux articles 7 et 8 de la Charte, pouvant avoir des effets dissuasifs tels que ceux visés au point 118 du présent arrêt.

154. Or, aux fins de la conciliation nécessaire des droits et des intérêts en cause exigée par la jurisprudence citée au point 130 du présent arrêt, il y a lieu de tenir compte du fait que, dans le cas d'une infraction commise en ligne, l'adresse IP peut constituer le seul moyen d'investigation permettant l'identification de la personne à laquelle cette adresse était attribuée au moment de la commission de cette infraction. À cela s'ajoute le fait que la conservation des adresses IP par les fournisseurs de services de communications électroniques au-delà de la durée d'attribution de ces données n'apparaît, en principe, pas nécessaire aux fins de la facturation des services en cause, de telle sorte

‡LW-BEHVMBJEH-GJDIBQW‡

que la détection des infractions commises en ligne peut, de ce fait, comme l'ont indiqué plusieurs gouvernements dans leurs observations soumises à la Cour, s'avérer impossible sans avoir recours à une mesure législative au titre de l'article 15, paragraphe 1, de la directive 2002/58. Tel peut notamment être le cas, ainsi que l'ont fait valoir ces gouvernements, des infractions particulièrement graves en matière de pédopornographie, telles que l'acquisition, la diffusion, la transmission ou la mise à disposition en ligne de pédopornographie, au sens de l'article 2, sous c), de la directive 2011/93/UE du Parlement européen et du Conseil, du 13 décembre 2011, relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil (JO 2011, L 335, p.1).

155. Dans ces conditions, s'il est vrai qu'une mesure législative prévoyant la conservation des adresses IP de l'ensemble des personnes physiques propriétaires d'un équipement terminal à partir duquel un accès à Internet peut être effectué viserait des personnes qui ne présentent, de prime abord, pas de lien, au sens de la jurisprudence citée au point 133 du présent arrêt, avec les objectifs poursuivis et que les internautes disposent, conformément à ce qui a été constaté au point 109 du présent arrêt, du droit de s'attendre, en vertu des articles 7 et 8 de la Charte, à ce que leur identité ne soit, en principe, pas dévoilée, une mesure législative prévoyant la conservation généralisée et indifférenciée des seules adresses IP attribuées à la source d'une connexion n'apparaît pas, en principe, contraire à l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, pourvu que cette possibilité soit soumise au strict respect des conditions matérielles et procédurales devant régir l'utilisation de ces données.

156. Eu égard au caractère grave de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte que comporte cette conservation, seule la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique sont de nature, à l'instar de la sauvegarde de la sécurité nationale, à justifier cette ingérence. En outre, la durée de conservation ne saurait excéder celle qui est strictement nécessaire au regard de l'objectif poursuivi. Enfin, une mesure de cette nature doit prévoir des conditions et des garanties strictes quant à l'exploitation de ces données, notamment par un traçage, à l'égard des communications et des activités effectuées en ligne par les personnes concernées.

157. En ce qui concerne, enfin, les données relatives à l'identité civile des utilisateurs des moyens de communications électroniques, ces données ne permettent pas, à elles seules, de connaître la date, l'heure, la durée et les destinataires des communications effectuées, non plus que les endroits où ces communications ont eu lieu ou la fréquence de celles-ci avec certaines personnes pendant une période donnée, de telle sorte qu'elles ne fournissent, mises à part les coordonnées de ceux-ci, telles que leurs adresses, aucune information sur les communications données et, par voie de conséquence, sur leur vie privée. Ainsi, l'ingérence que comporte une conservation de ces données ne saurait, en principe, être qualifiée de grave (voir, en ce sens, arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, points 59 et 60).

158. Il en découle que, conformément à ce qui a été exposé au point 140 du présent arrêt, les mesures législatives visant le traitement de ces données en tant que telles, notamment leur conservation et l'accès à celles-ci à la seule fin de l'identification de l'utilisateur concerné, et sans que lesdites données puissent être associées à des informations relatives aux communications effectuées, sont susceptibles d'être justifiées par l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales en général, auquel se réfère l'article 15, paragraphe 1, première phrase, de la directive 2002/58 (voir, en ce sens, arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, point 62).

‡LW-BEHVMBJEH-GJDIBQW‡

159. Dans ces conditions, eu égard à la conciliation nécessaire des droits et des intérêts en cause et pour les raisons figurant aux points 131 et 158 du présent arrêt, il y a lieu de considérer que, même en l'absence de lien entre l'ensemble des utilisateurs des moyens de communications électroniques et les objectifs poursuivis, l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, ne s'oppose pas à une mesure législative imposant, sans délai particulier, aux fournisseurs de services de communications électroniques la conservation des données relatives à l'identité civile de l'ensemble des utilisateurs des moyens de communications électroniques aux fins de la prévention, de la recherche, de la détection et de la poursuite d'infractions pénales ainsi que de la sauvegarde de la sécurité publique, sans qu'il soit nécessaire que les infractions pénales ou que les menaces contre ou les atteintes à la sécurité publique soient graves.

- *Sur les mesures législatives prévoyant la conservation rapide des données relatives au trafic et des données de localisation aux fins de lutte contre la criminalité grave*

160. En ce qui concerne les données relatives au trafic et les données de localisation traitées et stockées par les fournisseurs de services de communications électroniques sur la base des articles 5, 6 et 9 de la directive 2002/58, ou sur celle de mesures législatives prises en vertu de l'article 15, paragraphe 1, de celle-ci, telles que décrites aux points 134 à 159 du présent arrêt, il y a lieu de relever que ces données doivent, en principe, être, selon le cas, effacées ou rendues anonymes au terme des délais légaux dans lesquels doivent intervenir, conformément aux dispositions nationales transposant cette directive, leur traitement et leur stockage.

161. Toutefois, pendant ce traitement et ce stockage, peuvent se présenter des situations dans lesquelles survient la nécessité de conserver lesdites données au-delà de ces délais aux fins de l'élucidation d'infractions pénales graves ou d'atteintes à la sécurité nationale, et ce tant dans la situation où ces infractions ou ces atteintes ont déjà pu être constatées que dans celle où leur existence peut, au terme d'un examen objectif de l'ensemble des circonstances pertinentes, être raisonnablement soupçonnée.

162. À cet égard, il y a lieu de relever que la convention sur la cybercriminalité du Conseil de l'Europe du 23 novembre 2001 (série des traités européens – n° 185), laquelle a été signée par les 27 États membres et ratifiée par 25 d'entre eux, et dont l'objectif est de faciliter la lutte contre les infractions pénales commises au moyen des réseaux informatiques, prévoit, à son article 14, que les parties contractantes adoptent aux fins d'enquêtes ou de procédures pénales spécifiques certaines mesures quant aux données relatives au trafic déjà stockées, telles que la conservation rapide de ces données. En particulier, l'article 16, paragraphe 1, de cette convention stipule que les parties contractantes adoptent les mesures législatives qui se révèlent nécessaires pour permettre à leurs autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide des données relatives au trafic stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que ces données sont susceptibles de perte ou de modification.

163. Dans une situation telle que celle visée au point 161 du présent arrêt, il est loisible aux États membres, eu égard à la conciliation nécessaire des droits et des intérêts en cause visée au point 130 du présent arrêt, de prévoir, dans une législation adoptée en vertu de l'article 15, paragraphe 1, de la directive 2002/58, la possibilité, au moyen d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, d'enjoindre aux fournisseurs de services de communications électroniques de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont ils disposent.

‡LW-BEHVMBJEH-GJDIBQW‡

164. Dans la mesure où la finalité d'une telle conservation rapide ne correspond plus à celles pour lesquelles les données ont été collectées et conservées initialement et où tout traitement de données doit, en vertu de l'article 8, paragraphe 2, de la Charte, répondre à des fins déterminées, les États membres doivent préciser, dans leur législation, la finalité pour laquelle la conservation rapide des données peut avoir lieu. Eu égard au caractère grave de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte qu'est susceptible de comporter une telle conservation, seule la lutte contre la criminalité grave et, a fortiori, la sauvegarde de la sécurité nationale sont de nature à justifier cette ingérence. En outre, afin d'assurer que l'ingérence que comporte une mesure de ce type soit limitée au strict nécessaire, il convient, d'une part, que l'obligation de conservation porte sur les seules données de trafic et données de localisation susceptibles de contribuer à l'élucidation de l'infraction pénale grave ou de l'atteinte à la sécurité nationale concernée. D'autre part, 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.

165. À cet égard, il importe de préciser qu'une telle conservation rapide ne doit pas être limitée aux données des personnes concrètement soupçonnées d'avoir commis une infraction pénale ou une atteinte à la sécurité nationale. Tout en respectant le cadre dressé par l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, et compte tenu des considérations figurant au point 133 du présent arrêt, une telle mesure peut, selon le choix du législateur et tout en respectant les limites du strict nécessaire, être étendue aux données relatives au trafic et aux données de localisation afférentes à des personnes autres que celles qui sont soupçonnées d'avoir projeté ou commis une infraction pénale grave ou une atteinte à la sécurité nationale, pour autant que ces données peuvent, sur la base d'éléments objectifs et non discriminatoires, contribuer à l'élucidation d'une telle infraction ou d'une telle atteinte à la sécurité nationale, telles que les données de la victime de celle-ci, de son entourage social ou professionnel, ou encore de zones géographiques déterminées, telles que les lieux de la commission et de la préparation de l'infraction ou de l'atteinte à la sécurité nationale en cause. En outre, l'accès des autorités compétentes aux données ainsi conservées doit s'effectuer dans le respect des conditions résultant de la jurisprudence ayant interprété la directive 2002/58 (voir, en ce sens, arrêt du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, points 118 à 121 et jurisprudence citée).

166. Il convient encore d'ajouter que, ainsi qu'il ressort en particulier des points 115 et 133 du présent arrêt, l'accès à des données de trafic et à des données de localisation conservées par des fournisseurs en application d'une mesure prise au titre de l'article 15, paragraphe 1, de la directive 2002/58 ne peut en principe être justifié que par l'objectif d'intérêt général pour lequel cette conservation a été imposée à ces fournisseurs. Il s'ensuit, en particulier, qu'un accès à de telles données à des fins de poursuite et de sanction d'une infraction pénale ordinaire ne saurait en aucun cas être accordé lorsque leur conservation a été justifiée par l'objectif de lutte contre la criminalité grave ou, a fortiori, de sauvegarde de la sécurité nationale. En revanche, conformément au principe de proportionnalité tel qu'il a été précisé au point 131 du présent arrêt, un accès à des données conservées en vue de la lutte contre la criminalité grave peut, pour autant que soient respectées les conditions matérielles et procédurales entourant un tel accès visées au point précédent, être justifié par l'objectif de sauvegarde de la sécurité nationale.

‡LW-BEHVMBJEH-GJDIBQW‡

167. À cet égard, il est loisible aux États membres de prévoir dans leur législation qu'un accès à des données relatives au trafic et à des données de localisation peut, dans le respect de ces mêmes conditions matérielles et procédurales, avoir lieu à des fins de lutte contre la criminalité grave ou de sauvegarde de la sécurité nationale lorsque lesdites données sont conservées par un fournisseur d'une manière conforme aux articles 5, 6 et 9 ou encore à l'article 15, paragraphe 1, de la directive 2002/58 ».

En ce qui concerne les premières et deuxièmes questions préjudicielles posées par la Cour Constitutionnelle, la Cour de Justice a, dans le dispositif de l'arrêt, dit pour droit :

« 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 des droits fondamentaux de l'Union européenne, 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 des droits fondamentaux, 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

‡LW-BEHVMBJEH-GJDIBQW‡

– 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. [...] ».

1.3.3. Concernant la troisième question préjudicielle posée par la Cour Constitutionnelle, la Cour de justice a dit pour droit :

« Une juridiction nationale ne peut faire application d'une disposition de son droit national qui l'habilite à limiter dans le temps les effets d'une déclaration d'illégalité lui incombant, en vertu de ce droit, à l'égard d'une législation nationale imposant aux fournisseurs de services de communications électroniques, en vue, notamment, de la sauvegarde de la sécurité nationale et de la lutte contre la criminalité, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec 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 des droits fondamentaux. Cet article 15, paragraphe 1, interprété à la lumière du principe d'effectivité, impose au juge pénal national d'écarter des informations et des éléments de preuve qui ont été obtenus par une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec le droit de l'Union, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité, si ces personnes ne sont pas en mesure de commenter efficacement ces informations et ces éléments de preuve, provenant d'un domaine échappant à la connaissance des juges et qui sont susceptibles d'influencer de manière prépondérante l'appréciation des faits ».

1.4. À la suite de l'arrêt *La Quadrature du Net* de la Cour de Justice, dans son arrêt n° 57/2021 du 22 avril 2021, la Cour constitutionnelle s'est prononcée sur les recours dirigés contre la loi du mai 2016.

1.4.1. Dans cet arrêt, la Cour cite tout d'abord deux autres décisions de la Cour de Justice, à savoir :

1° l'arrêt du 2 octobre 2018 en cause *Ministerio Fiscal* (C-207/16) (ci-après l'arrêt « *Ministerio Fiscal* »), dans lequel la Cour de Justice dit pour droit :

« 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 et 8 de la charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens que l'accès d'autorités publiques aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé, telles que les nom, prénom et, le cas échéant, adresse de ces titulaires, comporte une ingérence dans les droits fondamentaux de ces derniers, consacrés à ces articles de la charte des

‡LW-BEHVMBJEH-GJDIBQW‡

droits fondamentaux, qui ne présente pas une gravité telle que cet accès devrait être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave ».

Dans cet arrêt, la Cour de Justice a motivé sa décision comme suit :

« *Sur le fond*

48. Par ses deux questions, qu'il convient d'examiner conjointement, la juridiction de renvoi demande, en substance, si l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7 et 8 de la Charte, doit être interprété en ce sens que l'accès d'autorités publiques aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé, lumière des articles 7 et 8 de la Charte, doit être interprété en ce sens que l'accès d'autorités publiques aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé, telles que les nom, prénom et, le cas échéant, adresse de ces titulaires, comporte une ingérence dans les droits fondamentaux de ces derniers, consacrés à ces articles de la Charte, qui présente une gravité telle que cet accès devrait être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave et, dans l'affirmative, à l'aune de quels critères la gravité de l'infraction en cause doit être appréciée.

49. À cet égard, il ressort de la décision de renvoi que, comme l'a relevé en substance M. l'avocat général au point 38 de ses conclusions, la demande de décision préjudicielle ne vise pas à déterminer si les données à caractère personnel en cause au principal ont été conservées par les fournisseurs de services de communications électroniques dans le respect des conditions visées à l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7 et 8 de la Charte. Cette demande porte, ainsi qu'il ressort du point 46 du présent arrêt, uniquement sur la question de savoir si et dans quelle mesure l'objectif poursuivi par la réglementation en cause au principal est susceptible de justifier l'accès d'autorités publiques, telles que la police judiciaire, à de telles données, sans que les autres conditions d'accès résultant de cet article 15, paragraphe 1, fassent l'objet de cette demande.

50. En particulier, cette juridiction s'interroge sur les éléments à prendre en compte afin d'apprécier si les infractions au regard desquelles des autorités policières peuvent être autorisées, à des fins d'enquête, à accéder à des données à caractère personnel conservées par les fournisseurs de services de communications électroniques, sont d'une gravité suffisante pour justifier l'ingérence que comporte un tel accès dans les droits fondamentaux garantis aux articles 7 et 8 de la Charte, tels qu'interprétés par la Cour dans ses arrêts du 8 avril 2014, *Digital Rights Ireland e.a.* (C-293/12 et C-594/12, EU:C:2014:238), et *Télé2 Sverige et Watson e.a.*

51. Quant à l'existence d'une ingérence dans ces droits fondamentaux, il y a lieu de rappeler que, comme l'a relevé M. l'avocat général aux points 76 et 77 de ses conclusions, l'accès des autorités publiques à de telles données est constitutif d'une ingérence dans le droit fondamental au respect de la vie privée, consacré à l'article 7 de la Charte, même en l'absence de circonstances permettant de qualifier cette ingérence de 'grave' et sans qu'il importe que les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou que les intéressés aient ou non subi d'éventuels inconvénients en raison de ladite ingérence. Un tel accès constitue également une ingérence dans le droit fondamental à la protection des données à caractère personnel garanti à l'article 8 de la Charte, puisqu'il constitue un traitement de données à caractère personnel [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 124 et 126 ainsi que jurisprudence citée].

‡LW-BEHVMBJEH-GJDIBQW‡

52. En ce qui concerne les objectifs susceptibles de justifier une réglementation nationale, telle que celle en cause au principal, régissant l'accès des autorités publiques aux données conservées par les fournisseurs de services de communications électroniques et dérogeant, ainsi, au principe de confidentialité des communications électroniques, il convient de rappeler que l'énumération des objectifs figurant à l'article 15, paragraphe 1, première phrase, de la directive 2002/58 revêt un caractère exhaustif, de telle sorte que cet accès doit répondre effectivement et strictement à l'un de ces objectifs (voir, en ce sens, arrêt *Télé2 Sverige et Watson e.a.*, points 90 et 115).

53. Or, s'agissant de l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales, il y a lieu d'observer que le libellé de l'article 15, paragraphe 1, première phrase, de la directive 2002/58 ne limite pas cet objectif à la lutte contre les seules infractions graves, mais vise les 'infractions pénales' en général.

54. À cet égard, la Cour a, certes, jugé que, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, seule la lutte contre la criminalité grave est susceptible de justifier un accès des autorités publiques à des données à caractère personnel conservées par les fournisseurs de services de communications qui, prises dans leur ensemble, permettent de tirer des conclusions précises concernant la vie privée des personnes dont les données sont concernées (voir, en ce sens, arrêt *Télé2 Sverige et Watson e.a.*, point 99).

55. La Cour a toutefois motivé cette interprétation par le fait que l'objectif poursuivi par une réglementation régissant cet accès doit être en relation avec la gravité de l'ingérence dans les droits fondamentaux en cause que cette opération entraîne (voir, en ce sens, arrêt *Télé2 Sverige et Watson e.a.*, point 115).

56. En effet, conformément au principe de proportionnalité, une ingérence grave ne peut être justifiée, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, que par un objectif de lutte contre la criminalité devant également être qualifiée de 'grave'.

57. En revanche, lorsque l'ingérence que comporte un tel accès n'est pas grave, ledit accès est susceptible d'être justifié par un objectif de prévention, de recherche, de détection et de poursuite d''infractions pénales' en général.

58. Il convient donc, avant tout, de déterminer si, en l'occurrence, en fonction des circonstances de l'espèce, l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte qu'un accès de la police judiciaire aux données en cause au principal comporterait doit être considérée comme étant 'grave'.

59. À cet égard, la demande en cause au principal par laquelle la police judiciaire sollicite, pour les besoins d'une enquête pénale, l'autorisation judiciaire d'accéder à des données à caractère personnel conservées par des fournisseurs de services de communications électroniques, a pour seul objet d'identifier les titulaires des cartes SIM activées, pendant une période de douze jours, avec le code IMEI du téléphone mobile volé. Ainsi qu'il a été relevé au point 40 du présent arrêt, cette demande vise l'accès aux seuls numéros de téléphone correspondant à ces cartes SIM ainsi qu'aux données relatives à l'identité civile des titulaires desdites cartes, telles que leurs nom, prénom et, le cas échéant, adresse. En revanche, ces données ne portent pas, comme l'ont confirmé tant le gouvernement espagnol que le ministère public lors de l'audience, sur les communications effectuées avec le téléphone mobile volé ni sur la localisation de celui-ci.

60. Il apparaît donc que les données visées par la demande d'accès en cause au principal permettent uniquement de mettre en relation, pendant une période déterminée, la ou les cartes SIM activées avec le téléphone mobile volé avec l'identité civile des titulaires de ces cartes SIM. Sans un recoupement avec les données afférentes aux

‡LW-BEHVMBJEH-GJDIBQW‡

communications effectuées avec lesdites cartes SIM et les données de localisation, ces données ne permettent de connaître ni la date, l'heure, la durée et les destinataires des communications effectuées avec la ou les cartes SIM en cause, ni les endroits où ces communications ont eu lieu ou la fréquence de celles-ci avec certaines personnes pendant une période donnée. Lesdites données ne permettent donc pas de tirer de conclusions précises concernant la vie privée des personnes dont les données sont concernées.

61. Dans ces conditions, l'accès aux seules données visées par la demande en cause au principal ne saurait être qualifié d'ingérence 'grave' dans les droits fondamentaux des personnes dont les données sont concernées.

62. Ainsi qu'il ressort des points 53 à 57 du présent arrêt, l'ingérence que comporterait un accès à de telles données est donc susceptible d'être justifiée par l'objectif de prévention, de recherche, de détection et de poursuite d''infractions pénales' en général, auquel se réfère l'article 15, paragraphe 1, première phrase, de la directive 2002/58, sans qu'il soit nécessaire que ces infractions soient qualifiées de 'graves'.

63. Eu égard aux considérations qui précèdent, il convient de répondre aux questions posées que l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7 et 8 de la Charte, doit être interprété en ce sens que l'accès d'autorités publiques aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé, telles que les nom, prénom et, le cas échéant, adresse de ces titulaires, comporte une ingérence dans les droits fondamentaux de ces derniers, consacrés à ces articles de la Charte, qui ne présente pas une gravité telle que cet accès devrait être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave ».

2° L'arrêt du 6 octobre 2020, en cause *Privacy International* (C-623/17) (ci-après l'arrêt « *Privacy International* »), prononcé en grande chambre, dans lequel la Cour de justice dit pour droit :

« L'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière de l'article 4, paragraphe 2, TUE ainsi que des articles 7, 8 et 11 et de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne, 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 des données de localisation aux services de sécurité et de renseignement ».

Cet arrêt repose sur la motivation suivante :

« *Sur la seconde question*

50. Par sa seconde question, la juridiction de renvoi cherche, en substance, à savoir si l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière de l'article 4, paragraphe 2, TUE ainsi que des articles 7, 8 et 11 et de l'article 52, paragraphe 1, 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 des données de localisation aux services de sécurité et de renseignement.

‡LW-BEHVMBJEH-GJDIBQW‡

51. À titre liminaire, il convient de rappeler que, selon les indications figurant dans la demande de décision préjudicielle, l'article 94 de la loi de 1984 autorise le ministre à imposer aux fournisseurs de services de communications électroniques, par voie d'instructions, lorsqu'il l'estime nécessaire dans l'intérêt de la sécurité nationale ou des relations avec un gouvernement étranger, de transmettre aux services de sécurité et de renseignement les données relatives aux communications en masse, ces données incluant les données relatives au trafic et les données de localisation ainsi que des informations sur les services utilisés, au sens de l'article 21, paragraphes 4 et 6, de la RIPA. Cette dernière disposition couvre, entre autres, les données nécessaires pour identifier la source d'une communication et la destination de celle-ci, déterminer la date, l'heure, la durée et le type de la communication, identifier le matériel utilisé ainsi que localiser les équipements terminaux et les communications, données au nombre desquelles figurent, notamment, le nom et l'adresse de l'utilisateur, le numéro de téléphone de l'appelant et le numéro appelé, les adresses IP de la source et du destinataire de la communication ainsi que les adresses des sites Internet visités.

52. Une telle communication par transmission des données concerne l'ensemble des utilisateurs des moyens de communications électroniques, sans qu'il soit précisé si cette transmission doit intervenir en temps réel ou de manière différée. Une fois transmises, ces données sont, selon les indications figurant dans la demande de décision préjudicielle, conservées par les services de sécurité et de renseignement et demeurent à la disposition de ces derniers aux fins de leurs activités, à l'instar des autres bases de données que ces services détiennent. En particulier, les données ainsi recueillies, qui sont soumises à des traitements et à des analyses de masse et automatisés, peuvent être recoupées avec d'autres bases de données comportant différentes catégories de données à caractère personnel en masse ou être divulguées hors de ces services et à des États tiers. Enfin, ces opérations ne sont pas subordonnées à l'autorisation préalable d'une juridiction ou d'une autorité administrative indépendante et ne donnent lieu à aucune information des personnes concernées.

53. La directive 2002/58 a pour finalité, ainsi qu'il ressort notamment de ses considérants 6 et 7, de protéger les utilisateurs des services de communications électroniques contre les dangers pour leurs données à caractère personnel et leur vie privée résultant des nouvelles technologies et, notamment, de la capacité accrue de stockage et de traitement automatisés de données. En particulier, ladite directive vise, ainsi que l'énonce son considérant 2, à garantir le plein respect des droits énoncés aux articles 7 et 8 de la Charte. À cet égard, il ressort de l'exposé des motifs de la proposition de directive du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques [COM(2000)385 final], à l'origine de la directive 2002/58, que le législateur de l'Union a entendu 'faire en sorte qu'un niveau élevé de protection des données à caractère personnel et de la vie privée continue à être garanti pour tous les services de communications électroniques, quelle que soit la technologie utilisée'.

54. À cet effet, l'article 5, paragraphe 1, de la directive 2002/58 dispose que 'les États membres garantissent, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes'. Cette même disposition souligne également que, '[e]n particulier, [les États membres] interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément à l'article 15,

‡LW-BEHVMBJEH-GJDIBQW‡

paragraphe 1', et précise que '[ce] paragraphe n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité'.

55. Ainsi, cet article 5, paragraphe 1, consacre le principe de confidentialité tant des communications électroniques que des données relatives au trafic y afférentes et implique, notamment, l'interdiction faite, en principe, à toute personne autre que les utilisateurs, de stocker, sans le consentement de ceux-ci, ces communications et ces données. Eu égard au caractère général de son libellé, cette disposition couvre nécessairement toute opération permettant à des tiers de prendre connaissance des communications et des données y afférentes à des fins autres que l'acheminement d'une communication.

56. L'interdiction d'intercepter les communications et les données y afférentes figurant à l'article 5, paragraphe 1, de la directive 2002/58 englobe donc toute forme de mise à disposition par les fournisseurs de services de communications électroniques de données relatives au trafic et de données de localisation à des autorités publiques, tels des services de sécurité et de renseignement, ainsi que la conservation desdites données par ces autorités, quelle que soit l'utilisation ultérieure qui est faite de celles-ci.

57. Ainsi, en adoptant cette directive, le législateur de l'Union a concrétisé les droits consacrés aux articles 7 et 8 de la Charte, de telle sorte que les utilisateurs des moyens de communications électroniques sont en droit de s'attendre, en principe, à ce que leurs communications et les données y afférentes restent, en l'absence de leur consentement, anonymes et ne puissent pas faire l'objet d'un enregistrement (arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, point 109).

58. Toutefois, l'article 15, paragraphe 1, de la directive 2002/58 permet aux États membres d'introduire des exceptions à l'obligation de principe, énoncée à l'article 5, paragraphe 1, de cette directive, de garantir la confidentialité des données à caractère personnel ainsi qu'aux obligations correspondantes, mentionnées notamment aux articles 6 et 9 de ladite directive, lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale, la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques. 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 l'un de ces motifs.

59. Cela étant, la faculté de déroger aux droits et aux obligations prévus aux articles 5, 6 et 9 de la directive 2002/58 ne saurait justifier que la dérogation à l'obligation de principe de garantir la confidentialité des communications électroniques et des données y afférentes et, en particulier, à l'interdiction de stocker ces données, explicitement prévue à l'article 5 de cette directive, devienne la règle (voir, en ce sens, arrêts du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, points 89 et 104, ainsi que du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, point 111).

60. En outre, il ressort de l'article 15, paragraphe 1, troisième phrase, de la directive 2002/58 que les États membres ne sont autorisés à prendre des mesures législatives visant à limiter la portée des droits et des obligations visés aux articles 5, 6 et 9 de cette directive que dans le respect des principes généraux du droit de l'Union, parmi lesquels figure le principe de proportionnalité, et des droits fondamentaux garantis par la Charte. À cet égard, la Cour a déjà jugé que l'obligation imposée par un État membre aux fournisseurs de services de communications électroniques, par une réglementation nationale, de conserver les données relatives au trafic aux fins de les

‡LW-BEHVMBJEH-GJDIBQW‡

rendre, le cas échéant, accessibles aux autorités nationales compétentes soulève des questions relatives au respect non seulement des articles 7 et 8 de la Charte, relatifs, respectivement, à la protection de la vie privée ainsi qu'à la protection des données à caractère personnel, mais également de l'article 11 de la Charte, relatif à la liberté d'expression (voir, en ce sens, arrêts du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, points 25 et 70, ainsi que du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, points 91 et 92 ainsi que jurisprudence citée).

61. Ces mêmes questions se posent également pour d'autres types de traitement de données, tels que leur transmission à des personnes autres que les utilisateurs ou l'accès à ces données en vue de leur utilisation [voir, par analogie, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 122 et 123 ainsi que jurisprudence citée].

62. Ainsi, l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58 doit tenir compte de l'importance tant du droit au respect de la vie privée, garanti à l'article 7 de la Charte, que du droit à la protection des données à caractère personnel, garanti à l'article 8 de celle-ci, telle qu'elle ressort de la jurisprudence de la Cour, ainsi que du droit à la liberté d'expression, ce droit fondamental, garanti à l'article 11 de la Charte, constituant l'un des fondements essentiels d'une société démocratique et pluraliste et faisant partie des valeurs sur lesquelles est, conformément à l'article 2 TUE, fondée l'Union (voir, en ce sens, arrêts du 6 mars 2001, Connolly/Commission, C-274/99 P, EU:C:2001:127, point 39, et du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, point 93 et jurisprudence citée).

63. Toutefois, les droits consacrés aux articles 7, 8 et 11 de la Charte n'apparaissent pas comme étant des prérogatives absolues, mais doivent être pris en considération par rapport à leur fonction dans la société (voir, en ce sens, arrêt du 16 juillet 2020, Facebook Ireland et Schrems, C-311/18, EU:C:2020:559, point 172 ainsi que jurisprudence citée).

64. En effet, ainsi qu'il ressort de l'article 52, paragraphe 1, de la Charte, celle-ci admet des limitations à l'exercice de ces droits, pour autant que ces limitations soient prévues par la loi, qu'elles respectent le contenu essentiel desdits droits et que, dans le respect du principe de proportionnalité, elles soient nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui.

65. Il convient d'ajouter que l'exigence selon laquelle toute limitation de l'exercice des droits fondamentaux doit être prévue par la loi implique que la base légale qui permet l'ingérence dans ces droits doit définir elle-même la portée de la limitation de l'exercice du droit concerné (arrêt du 16 juillet 2020, Facebook Ireland et Schrems, C-311/18, EU:C:2020:559, point 175 ainsi que jurisprudence citée).

66. En ce qui concerne le respect du principe de proportionnalité, l'article 15, paragraphe 1, première phrase, de la directive 2002/58 dispose que les États membres peuvent adopter une mesure dérogeant au principe de confidentialité des communications et des données relatives au trafic y afférentes lorsqu'une telle mesure est 'nécessaire, appropriée et proportionnée, au sein d'une société démocratique', au regard des objectifs que cette disposition énonce. Le considérant 11 de cette directive précise qu'une mesure de cette nature doit être 'rigoureusement' proportionnée au but poursuivi.

67. À cet égard, il convient de rappeler que la protection du droit fondamental au respect de la vie privée exige, conformément à la jurisprudence constante de la Cour, que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire. En outre, un objectif d'intérêt

‡LW-BEHVMBJEH-GJDIBQW‡

général ne saurait être poursuivi sans tenir compte du fait qu'il doit être concilié avec les droits fondamentaux concernés par la mesure, ce en effectuant une pondération équilibrée entre l'objectif et les intérêts et droits en cause [voir, en ce sens, arrêts du 16 décembre 2008, Satakunnan Markkinapörssi et Satamedia, C-73/07, EU:C:2008:727, point 56 ; du 9 novembre 2010, Volker und Markus Schecke et Eifert, C-92/09 et C-93/09, EU:C:2010:662, points 76, 77 et 86, ainsi que du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, point 52 ; avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 140].

68. Pour satisfaire à l'exigence de proportionnalité, une réglementation doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de telle sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus. Cette réglementation doit être légalement contraignante en droit interne et, en particulier indiquer en quelles circonstances et sous quelles conditions une mesure prévoyant le traitement de telles données peut être prise, garantissant ainsi que l'ingérence soit limitée au strict nécessaire. La nécessité de disposer de telles garanties est d'autant plus importante lorsque les données à caractère personnel sont soumises à un traitement automatisé, notamment lorsqu'il existe un risque important d'accès illicite à ces données. Ces considérations valent en particulier lorsqu'est en jeu la protection de cette catégorie particulière de données à caractère personnel que sont les données sensibles [voir, en ce sens, arrêts du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, points 54 et 55, ainsi que du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, point 117 ; avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 141].

69. S'agissant de la question de savoir si une réglementation nationale, telle que celle en cause au principal, satisfait aux exigences de l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, il convient de relever que la transmission des données relatives au trafic et des données de localisation à des personnes autres que les utilisateurs, telles que des services de sécurité et de renseignement, déroge au principe de confidentialité. Dès lors que cette opération est effectuée, comme en l'occurrence, de manière généralisée et indifférenciée, elle a pour effet de faire de la dérogation à l'obligation de principe de garantir la confidentialité des données la règle, alors que le système mis en place par la directive 2002/58 exige qu'une telle dérogation demeure l'exception.

70. En outre, conformément à la jurisprudence constante de la Cour, la transmission des données relatives au trafic et des données de localisation à un tiers constitue une ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, quelle que soit l'utilisation ultérieure qui est faite de ces données. À cet égard, il importe peu que les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou que les intéressés aient ou non subi d'éventuels inconvénients en raison de cette ingérence [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 124 et 126 ainsi que jurisprudence citée, et arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, points 115 et 116].

71. L'ingérence que comporte la transmission des données relatives au trafic et des données de localisation aux services de sécurité et de renseignement dans le droit consacré à l'article7 de la Charte doit être considérée comme étant particulièrement grave, compte tenu notamment du caractère sensible des informations que peuvent fournir ces données et, notamment, de la possibilité d'établir à partir de celles-ci le profil des personnes concernées, une telle information étant tout aussi sensible que le contenu même des

‡LW-BEHVMBJEH-GJDIBQW‡

communications. En outre, elle est susceptible de générer dans l'esprit des personnes concernées le sentiment que leur vie privée fait l'objet d'une surveillance constante (voir, par analogie, arrêts du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, points 27 et 37, ainsi que du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, points 99 et 100).

72. Il convient de relever encore qu'une transmission des données relatives au trafic et des données de localisation à des autorités publiques à des fins sécuritaires est susceptible, à elle seule, de porter atteinte au droit au respect des communications, consacré à l'article 7 de la Charte, et d'entraîner 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. De tels effets dissuasifs peuvent affecter en particulier les personnes dont les communications sont soumises, selon les règles nationales, au secret professionnel ainsi que les lanceurs d'alerte dont les activités sont protégées par la directive (UE)2019/1937 du Parlement européen et du Conseil, du 23 octobre 2019, sur la protection des personnes qui signalent des violations du droit de l'Union (JO 2019, L 305, p. 17). En outre, ces effets sont d'autant plus graves que le nombre et la variété des données conservées sont élevés (voir, en ce sens, arrêts du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, point 28 ; du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, point 101, ainsi que du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, point 118).

73. Enfin, compte tenu de la quantité importante de données relatives au trafic et de données de localisation susceptibles d'être conservées de manière continue par une mesure de conservation généralisée ainsi que du caractère sensible des informations que ces données peuvent fournir, la seule conservation desdites données par les fournisseurs de services de communications électroniques comporte des risques d'abus et d'accès illicite.

74. S'agissant des objectifs susceptibles de justifier de telles ingérences, plus particulièrement de l'objectif de sauvegarde de la sécurité nationale, en cause au principal, 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, en particulier à menacer directement la société, la population ou l'État en tant que tel, telles que notamment des activités de terrorisme (arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, point 135).

75. Or, l'importance de l'objectif de sauvegarde de la sécurité nationale, lu à l'aune de l'article 4, paragraphe 2, TUE, dépasse celle des autres objectifs visés à l'article 15, paragraphe 1, de la directive 2002/58, notamment des objectifs de lutte contre la criminalité en général, même grave, ainsi que de sauvegarde de la sécurité publique. En effet, des menaces telles que celles visées au point précédent se distinguent, par leur nature et leur particulière gravité, du risque général de survenance de tensions ou de troubles, mêmes graves, à la sécurité publique. Sous réserve du respect des autres exigences prévues à l'article 52, paragraphe 1, de la Charte, l'objectif de sauvegarde de la sécurité nationale est dès lors susceptible de justifier des mesures comportant des ingérences dans les droits fondamentaux plus graves que celles que pourraient justifier ces autres objectifs (arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, point 136).

‡LW-BEHVMBJEH-GJDIBQW‡

76. Toutefois, pour satisfaire à l'exigence de proportionnalité rappelée au point 67 du présent arrêt, selon laquelle les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire, une réglementation nationale comportant une ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte doit respecter les exigences résultant de la jurisprudence citée aux points 65, 67 et 68 du présent arrêt.

77. En particulier, s'agissant de l'accès d'une autorité à des données à caractère personnel, une réglementation ne saurait se limiter à exiger que l'accès des autorités aux données réponde à la finalité poursuivie par cette réglementation, mais elle doit également prévoir les conditions matérielles et procédurales régissant cette utilisation [voir, par analogie, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 192 et jurisprudence citée].

78. Ainsi, et dès lors qu'un accès général à toutes les données conservées, en l'absence de tout lien, même indirect, avec le but poursuivi, ne peut être considéré comme étant limité au strict nécessaire, une réglementation nationale régissant l'accès aux données relatives au trafic et aux données de localisation doit se fonder sur des critères objectifs pour définir les circonstances et les conditions dans lesquelles doit être accordé aux autorités nationales compétentes l'accès aux données en cause (voir, en ce sens, arrêt du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, point 119 et jurisprudence citée).

79. Ces exigences s'appliquent, a fortiori, à une mesure législative, telle que celle en cause au principal, sur le fondement de laquelle l'autorité nationale compétente peut imposer aux fournisseurs de services de communications électroniques de procéder à la communication par transmission généralisée et indifférenciée des données relatives au trafic et des données de localisation aux services de sécurité et de renseignement. En effet, une telle transmission a pour effet de mettre ces données à la disposition des autorités publiques [voir, par analogie, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 212].

80. Dès lors que la transmission des données relatives au trafic et des données de localisation a lieu de manière généralisée et indifférenciée, elle concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques. Elle s'applique donc même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement pourrait avoir un lien, même indirect ou lointain, avec l'objectif de sauvegarde de la sécurité nationale et, en particulier, sans que soit établie une relation entre les données dont la transmission est prévue et une menace pour la sécurité nationale (voir, en ce sens, arrêts du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, points 57 et 58, ainsi que du 21 décembre 2016, Télé2, C-203/15 et C-698/15, EU:C:2016:970, point 105). Eu égard au fait que la transmission de telles données aux autorités publiques équivaut, conformément à ce qui a été constaté au point 79 du présent arrêt, à un accès, il convient de considérer qu'une réglementation permettant une transmission généralisée et indifférenciée des données aux autorités publiques, implique un accès général.

81. Il en résulte qu'une réglementation nationale imposant aux fournisseurs de services de communications électroniques de procéder à la communication par transmission généralisée et indifférenciée des données relatives au trafic et des données de localisation aux services de sécurité et de renseignement, excède les limites du strict nécessaire et ne saurait être considérée comme étant justifiée, dans une société démocratique, ainsi que l'exige l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière de l'article 4, paragraphe 2, TUE ainsi que des articles 7, 8 et 11 et de l'article 52, paragraphe 1, de la Charte.

‡LW-BEHVMBJEH-GJDIBQW‡

82. Eu égard à l'ensemble des considérations qui précèdent, il convient de répondre à la seconde question que l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière de l'article 4, paragraphe 2, TUE ainsi que des articles 7, 8 et 11 et de l'article 52, paragraphe 1, 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 des données de localisation aux services de sécurité et de renseignement ».

1.4.2. Après avoir cité ces deux décisions de la Cour de Justice, la Cour constitutionnelle énonce la motivation et le dispositif de l'arrêt *La Quadrature du Net* de la Cour de Justice, répondant aux questions préjudicielles posées par son arrêt n° 96/2018.

Elle motive ensuite sa décision comme suit :

« B.15. Il ressort de l'arrêt de la Cour de justice du 6 octobre 2020 en cause. *La Quadrature du Net et autres*, précité, 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 des droits fondamentaux de l'Union européenne, 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, sauf dans les hypothèses limitées décrites par l'arrêt précité.

En ce qu'elle prévoit, par principe et sans limitation à ces hypothèses, une conservation généralisée et indifférenciée, par les opérateurs et fournisseurs de services de communications électroniques, des données d'identification, des données d'accès et de connexion, ainsi que des données de communication, visées à l'article 126, § 3, de la loi du 13 juin 2005, la loi attaquée viole par conséquent l'article 15, paragraphe 1, de la directive 2002/58/CE, lu à la lumière des dispositions précitées de la Charte des droits fondamentaux de l'Union européenne, et en combinaison avec les articles 10 et 11 de la Constitution.

B.16.1. Dans le dispositif de l'arrêt du 6 octobre 2020 en cause *La Quadrature du Net et autres*, précité, la Cour de justice précise cependant 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 des droits fondamentaux de l'Union européenne, ne s'oppose pas à divers types de mesures législatives que la Cour énumère. Sont ainsi admissibles, notamment, 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', ou encore des mesures législatives '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'. Ces mesures législatives doivent 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'.

‡LW-BEHVMBJEH-GJDIBQW‡

B.16.2. Sur la base de ces précisions de la Cour de justice, le Conseil des ministres soutient dans ses mémoires complémentaires qu'en tout état de cause, la loi attaquée ne doit pas être annulée en ce qu'elle prévoit l'obligation généralisée et indifférenciée de conservation, par les opérateurs et fournisseurs de services de communications électroniques, des adresses IP attribuées à la source d'une connexion, d'une part, et des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques, d'autre part.

Le Conseil des ministres en conclut que seuls doivent être annulés, le cas échéant, les alinéas 2 et 3 de l'article 126, § 3, de la loi du 13 juin 2005, qui visent respectivement les données de connexion et de localisation et les données de communication. Il estime que l'alinéa 1er de l'article 126, § 3, précité, qui vise les données d'identification, ne doit en revanche pas être annulé, pas plus que les autres dispositions de la loi attaquée, dès lors qu'elles contiennent les garanties nécessaires en termes de conservation des données et d'accès à celles-ci.

B.17. En l'espèce, il y a lieu de constater que la loi attaquée repose, dans son principe même, sur une obligation de conservation généralisée et indifférenciée de l'ensemble des données visées à l'article 126, § 3, de la loi du 13 juin 2005, et qu'elle poursuit, d'une manière générale, comme il est dit en B.3 et en B.4, des objectifs plus larges que la lutte contre la criminalité grave ou le risque d'atteinte à la sécurité publique.

La distinction que l'article 126, § 3, de la loi du 13 juin 2005 opère entre trois catégories de données (à savoir : les données d'identification, les données d'accès et de connexion, ainsi que les données de communication) n'a d'incidence que sur le point de départ de la durée de conservation des données, de douze mois en toute hypothèse, et éventuellement sur les possibilités d'accéder à celles-ci, pour les instances habilitées (voy. l'article 46*bis* du Code d'instruction criminelle et l'article 126, § 2, de la loi du 13 juin 2005). Cette catégorisation ne correspond par ailleurs pas aux distinctions qui sont opérées par la Cour de justice dans son arrêt du 6 octobre 2020 en ce qui concerne les différentes catégories de données susceptibles de faire l'objet d'une obligation de conservation généralisée et indifférenciée, moyennant le respect de plusieurs conditions (à savoir, en l'occurrence : les adresses IP attribuées à la source d'une connexion et les données relatives à l'identité civile des utilisateurs de moyens de communications électroniques).

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 des droits fondamentaux de l'Union européenne. En particulier, il appartient également au législateur, dans ce contexte, d'opérer les distinctions qui s'imposent entre les différents

‡LW-BEHVMBJEH-GJDIBQW‡

types de données soumises à conservation, de manière à garantir que, pour chaque type de donnée, l'ingérence soit limitée au strict nécessaire.

B.20. Compte tenu de ce qui précède, il y a lieu d'annuler les articles 2, b), 3 à 11 et 14 de la loi attaquée, qui sont indissociablement liés ».

Pour ces motifs, la Cour constitutionnelle, dans son arrêt n° 57/2021 du 22 avril 2021 décide d'annuler, sans en maintenir les effets pour une période déterminée, les articles 2, b), 3 à 11 et 14 de la loi du 29 mai 2016. Elle rejette le recours pour le surplus.

1.5. L'avant-projet à l'examen se donne pour objet de faire suite à cet arrêt de la Cour constitutionnelle du 22 avril 2021, ainsi qu'à la jurisprudence de la Cour de Justice qui fonde cet arrêt, spécialement l'arrêt *La Quadrature du Net*.

2. Compte-tenu de ce qui précède, l'avant-projet doit être plus spécialement examiné au regard de l'article 15 de la directive 2002/58/CE du Parlement et du Conseil du 12 juillet 2002 qui dispose comme suit :

« Application de certaines dispositions de la directive 95/46/CE

1. 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.

1*bis*. Le paragraphe 1 n'est pas applicable aux données dont la conservation est spécifiquement exigée par la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication [7] aux fins visées à l'article 1er, paragraphe 1, de ladite directive.

1*ter*. Les fournisseurs établissent, sur la base des dispositions nationales adoptées au titre du paragraphe 1, des procédures internes permettant de répondre aux demandes d'accès aux données à caractère personnel concernant les utilisateurs. Ils mettent, sur demande, à la disposition de l'autorité nationale compétente des informations sur ces procédures, sur le nombre de demandes reçues, sur la base juridique invoquée et sur leur réponse.

[7] *Note de bas de page 1 de la directive citée :* JO L 105 du 13.4.2006, p. 54.

‡LW-BEHVMBJEH-GJDIBQW‡

2. Les dispositions du chapitre III de la directive 95/46/CE relatif aux recours juridictionnels, à la responsabilité et aux sanctions sont applicables aux dispositions nationales adoptées en application de la présente directive ainsi qu'aux droits individuels résultant de la présente directive.

3. Le groupe de protection des personnes à l'égard du traitement des données à caractère personnel, institué par l'article 29 de la directive 95/46/CE, remplit aussi les tâches visées à l'article 30 de ladite directive en ce qui concerne les matières couvertes par la présente directive, à savoir la protection des droits et des libertés fondamentaux ainsi que des intérêts légitimes dans le secteur des communications électroniques ».

3. Concernant le droit interne, dès lors que les dispositions de la loi du 29 mai 2016, et avant celles-ci, les dispositions de la loi du 30 juillet 2013, ont été annulées, elles sont censées ne jamais avoir existé et les dispositions abrogées ou modifiées par ces lois redeviennent applicables telles quelles sont en vigueur, sans avoir égard aux modifications apportées par les deux lois précitées.

4. C'est dans ce contexte que les auteurs de l'avant-projet entendent dès lors adopter un dispositif qui a pour objet de mettre en place un système de conservation des données qui permettraient d'atteindre les objectifs dont la Cour de justice et la Cour constitutionnelle ont reconnu le caractère légitime, tout en se conformant aux décisions de ces hautes juridictions, dans leur dispositif et leur motivation, en particulier les limites et critères qui résultent de celles-ci en matière de conservation des données de trafic et de localisation par les opérateurs intervenant dans le secteur des communications électroniques, et d'accès à ces données par les autorités.

B. MISE EN ŒUVRE, PAR LE TEXTE EN PROJET, DES EXIGENCES DÉCOULANT DES ARRÊTS DE LA COUR DE JUSTICE ET DE LA COUR CONSTITUTIONNELLE, AINSI QUE DE LA JURISPRUDENCE PERTINENTE RÉCENTE DE LA COUR EUROPÉENNE DES DROITS DE L'HOMME

À titre préalable, la section de législation rappelle que sa saisine est limitée, par définition, au texte en projet et qu'il ne lui appartient pas, dans ces conditions, d'examiner si l'ensemble du droit positif belge, notamment judiciaire et relatif aux services de renseignement et de sécurité, est de nature à garantir le respect du droit à la vie privée, conformément notamment à la jurisprudence de la Cour européenne des droits de l'homme, dans la collecte et l'usage qui seraient faits des données dont la conservation est ici prévue. Ainsi, la compatibilité de la chaine de collecte, de conservation, d'accès et d'utilisation des données concernées avec les libertés et droits fondamentaux en cause, dépend d'autres dispositions en vigueur, qu'elles aient ou non une portée générale, dont la section de législation n'est pas saisie [8].

[8] En ce sens, voir l'avis n° 58.449/4.

‡LW-BEHVMBJEH-GJDIBQW‡

I.1. LES ENSEIGNEMENTS DES ARRÊTS *DIGITAL RIGHTS*, *MINISTERIO FISCAL*, ET *LA QUADRATURE DU NET*

1.1. Des arrêts *Digital Rights*, *MINISTERIO FISCAL* et *LA QUADRATURE DU NET*, ainsi que de l'arrêt n° 84/2015 prononcé subséquemment par la Cour constitutionnelle, il convient essentiellement de retenir les éléments suivants :

1° La conservation des données aux fins de permettre aux autorités nationales compétentes de disposer d'un accès éventuel à celles-ci, constitue une ingérence dans le droit fondamental au respect de la vie privée et les autres droits consacrés à l'article 7 et à l'article 8 de la Charte des droits fondamentaux de l'Union européenne, aggravée par la circonstance que les autorités pourront prendre connaissance de ces données.

2° Cette ingérence n'est toutefois pas de nature à porter atteinte au contenu essentiel de ces droits, lorsque l'accès donné au autorités nationales aux données concernées ne permet pas de prendre connaissance du contenu des communications électroniques en tant que tel.

3° Cette ingérence répond par ailleurs à un objectif d'intérêt général lorsqu'elle a pour objet la lutte contre le terrorisme international, la lutte contre la criminalité grave afin de garantir la sécurité publique et le droit de toute personne à la sûreté.

4° La question se pose dès lors de savoir si l'ingérence concernée est proportionnée au but poursuivi, à savoir si elle comprend les mesures strictement nécessaires pour atteindre ce but ; à ce propos, la réglementation en cause « doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant un minimum d'exigences de sorte que les personnes dont les données ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données ».

Sur ce point, ne satisfait pas à cette exigence de proportionnalité une législation qui :

a) couvre de manière généralisée toute personne et tous les moyens de communications électroniques ainsi que l'ensemble des données relatives au trafic sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif de lutte contre les infractions graves ;

b) n'impose pas que les personnes dont les données sont conservées se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales et ne prévoit aucune exception, de sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel ;

‡LW-BEHVMBJEH-GJDIBQW‡

c) ne requiert aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique et, notamment, n'est pas limitée à une conservation portant :

– soit sur des données afférentes à une période temporelle et/ou une zone géographique déterminée et/ou sur un cercle de personnes données susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave ;

– soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la prévention, à la détection ou à la poursuite d'infractions graves ;

d) « ne prévoit aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure à des fins de prévention, de détection ou de poursuites pénales concernant des infractions pouvant, au regard de l'ampleur et de la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, être considérées comme suffisamment graves pour justifier une telle ingérence » ; à cet égard, est problématique une législation qui « ne contient pas les conditions matérielles et procédurales y afférentes » et « ne dispose pas expressément que cet accès et l'utilisation ultérieure des données en cause doivent être strictement restreints à des fins de prévention et de détection d'infractions graves précisément délimitées ou de poursuites pénales afférentes à celles-ci » ; il en va spécialement ainsi lorsque la législation ne comporte « aucun critère objectif permettant de limiter le nombre de personnes disposant de l'autorisation d'accès et d'utilisation ultérieure des données conservées au strict nécessaire au regard de l'objectif poursuivi » et que « l'accès aux données conservées par les autorités nationales compétentes n'est pas subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante dont la décision vise à limiter l'accès aux données et leur utilisation à ce qui est strictement nécessaire aux fins d'atteindre l'objectif poursuivi et intervient à la suite d'une demande motivée de ces autorités présentée dans le cadre de procédures de prévention, de détection ou de poursuites pénales » ;

e) prévoit une durée générale de conservation des données « sans que soit opérée une quelconque distinction entre les catégories de données […] en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées » et ne précise pas « que la détermination de la durée de conservation doit être fondée sur des critères objectifs afin de garantir que celle-ci est limitée au strict nécessaire ». Il peut en être déduit qu'il est requis que « l'ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire » ;

f) ne prévoit pas de « règles spécifiques et adaptées à la vaste quantité des données dont la conservation est imposée, au caractère sensible de ces données ainsi qu'au risque d'accès illicite à celles-ci, règles qui seraient destinées notamment à régir de manière claire et stricte la protection et la sécurité des données en cause, afin de garantir leur pleine intégrité et confidentialité » ; il en va plus spécialement ainsi lorsque la législation n'impose pas aux opérateurs « un niveau particulièrement élevé de protection et de sécurité par des mesures techniques et organisationnelles », qui garantisse en outre la « destruction irrémédiable des données au terme de la durée de conservation de celles-ci » ;

‡LW-BEHVMBJEH-GJDIBQW‡

g) n'impose pas que les données en cause soient conservées sur le territoire de l'Union, avec pour conséquence que n'est dès lors pas « pleinement garanti le contrôle par une autorité indépendante, explicitement exigé par l'article 8, paragraphe 3, de la Charte, du respect des exigences de protection et de sécurité, telles que visées aux deux points précédents ».

2. En ce qui concerne spécifiquement la portée de l'article 15, paragraphe 1, de la directive 2002/58/CE, lu à la lumière de l'article 4, paragraphe 2 TUE ainsi que des articles 7, 8 et 11, de la Charte des droits fondamentaux de l'Union européenne, il y a lieu, pour l'essentiel, de retenir des arrêts *Ministerio Fiscal*, *Privacy International* et *La Quadrature du Net*, les éléments suivants :

1° N'est pas admissible 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 des données de localisation aux services de sécurité et de renseignement ;

2° Est admissible une législation nationale qui permet 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 cette injonction ne pouvant être émise que pour une période temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de cette menace ;

3° Est admissible une législation nationale qui permet 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 ;

4° Est admissible une législation nationale 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 ;

5° Est admissible une législation nationale qui prévoit, 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 ;

‡LW-BEHVMBJEH-GJDIBQW‡

6° Est admissible une législation nationale qui permet, aux fins de la lutte contre la criminalité grave et, à 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 ;

7° Plus ponctuellement, est admissible une législation qui permet l'accès d'autorités publiques aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé, telles que les nom, prénom et, le cas échéant, adresse de ces titulaires : une telle réglementation comporte certes une ingérence dans les droits fondamentaux de ces derniers, mais cette ingérence ne présente pas une gravité telle que cet accès devrait être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave.

Concernant les points 2° à 6° qui précédent, les législations concernées ne sont admissibles que si, en outre, elles 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.

3. Enfin, il faut également avoir à l'esprit que, dans son arrêt *La Quadrature du Net*, la Cour de Justice s'est également prononcée sur d'autres questions préjudicielles [9-10], posées par le Conseil d'État de France.

---

[9] Dans l'affaire C-511/18, le Conseil d'État de France a posé les questions suivantes :
« 1) L'obligation de conservation généralisée et indifférenciée, imposée aux fournisseurs sur le fondement des dispositions permissives de l'article 15, paragraphe 1, de la directive [2002/58], ne doit-elle pas être regardée, dans un contexte marqué par des menaces graves et persistantes pour la sécurité nationale, et en particulier par le risque terroriste, comme une ingérence justifiée par le droit à la sûreté garanti à l'article 6 de la [Charte] et les exigences de la sécurité nationale, dont la responsabilité incombe aux seuls États membres en vertu de l'article 4 [TUE] ?
2) La directive [2002/58] lue à la lumière de la [Charte] doit-elle être interprétée en ce sens qu'elle autorise des mesures législatives, telles que les mesures de recueil en temps réel des données relatives au trafic et à la localisation d'individus déterminés, qui, tout en affectant les droits et obligations des fournisseurs d'un service de communications électroniques, ne leur imposent pas pour autant une obligation spécifique de conservation de leurs données ?
3) La directive [2002/58], lue à la lumière de la [Charte], doit-elle être interprétée en ce sens qu'elle subordonne dans tous les cas la régularité des procédures de recueil des données de connexion à une exigence d'information des personnes concernées lorsqu'une telle information n'est plus susceptible de compromettre les enquêtes menées par les autorités compétentes ou de telles procédures peuvent-elles être regardées comme régulières compte tenu de l'ensemble des autres garanties procédurales existantes, dès lors que ces dernières assurent l'effectivité du droit au recours ? ».

[10] Dans l'affaire C-512/18, le Conseil d'État de France a posé les questions préjudicielles suivantes :
« 1) L'obligation de conservation généralisée et indifférenciée, imposée aux fournisseurs sur le fondement des dispositions permissives de l'article 15, paragraphe 1, de la directive [2002/58], ne doit-elle pas être regardée, notamment eu égard aux garanties et contrôles dont sont assortis ensuite le recueil et l'utilisation de ces données de connexion, comme une ingérence justifiée par le droit à la sûreté garanti à l'article 6 de la [Charte] et les exigences de la sécurité nationale, dont la responsabilité incombe aux seuls États membres en vertu de l'article 4 [TUE] ?
2) Les dispositions de la directive [2000/31], lues à la lumière des articles 6, 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la [Charte], doivent-elles être interprétées en ce sens qu'elles permettent à un État d'instaurer une réglementation nationale imposant aux personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne et aux personnes physiques ou morales qui assurent, même à titre gratuit, pour

‡LW-BEHVMBJEH-GJDIBQW‡

C'est dans ce contexte que dans cet arrêt, la Cour de Justice a dit pour droit :

« 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 des droits fondamentaux, doit être interprété en ce sens qu'il ne s'oppose pas à une réglementation nationale imposant aux fournisseurs de services de communications électroniques de recourir, d'une part, à l'analyse automatisée ainsi qu'au recueil en temps réel, notamment, des données relatives au trafic et des données de localisation et, d'autre part, au recueil en temps réel des données techniques relatives à la localisation des équipements terminaux utilisés, lorsque

– le recours à l'analyse automatisée est limité à des situations dans lesquelles un État membre se trouve confronté à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, le recours à cette analyse 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 situation justifiant ladite mesure ainsi que le respect des conditions et des garanties devant être prévues, et que

– le recours à un recueil en temps réel des données relatives au trafic et des données de localisation est limité aux personnes à l'égard desquelles il existe une raison valable de soupçonner qu'elles sont impliquées d'une manière ou d'une autre dans des activités de terrorisme et est soumis à un contrôle préalable, effectué, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, afin de s'assurer qu'un tel recueil en temps réel n'est autorisé que dans la limite de ce qui est strictement nécessaire. En cas d'urgence dûment justifiée, le contrôle doit intervenir dans de brefs délais ».

4. Ceci étant rappelé, comme la section de législation l'a déjà souligné dans son avis n° 58.449/4, il y a lieu d'avoir égard à la portée circonscrite des différentes décisions de la Cour de Justice et de la Cour constitutionnelle.

Ainsi, l'affaire *Digital Rights* concerne la conservation et l'accès subséquent à des données, telles que visées par la directive 2006/24/UE, à savoir la conservation et l'accès à des données « en vue de garantir la disponibilité [de celles-ci] à des fins de recherche, de détection et de poursuite d'infractions graves ». La portée de l'arrêt de la Cour de Justice et des conséquences à en tirer, aussi rigoureuses soient-elles, sont donc limitées à une conservation de données dont la finalité est, en sa phase ultime, la sanction pénale, par hypothèse, nécessairement non anodine, de comportements et d'actes constitutifs d'infractions graves.

Dans l'affaire *La Quadrature du Net*, la Cour de Justice s'est prononcée dans un contexte dans lequel la conservation considérée avait pour objectif, selon le cas, la sauvegarde de la sécurité nationale, la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique, ou la lutte contre la criminalité et la sauvegarde de la sécurité publique. Elle s'est également prononcée sur l'analyse automatisée de données en cas de menace grave pour la sécurité nationale, réelle, actuelle ou prévisible, et sur le recueil en temps réel de

mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services, de conserver les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires, afin que l'autorité judiciaire puisse, le cas échéant, en requérir communication en vue de faire respecter les règles relatives à la responsabilité civile ou pénale ? ».

‡LW-BEHVMBJEH-GJDIBQW‡

données relatives au trafic et des données de localisation limité aux personnes à l'égard desquelles il existe une raison valable de soupçonner qu'elles sont impliquées dans des activités de terrorisme.

Dans l'affaire *Ministerio Fiscal*, la Cour de Justice s'est prononcée à propos de l'accès d'autorités publiques aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé.

Enfin, dans l'arrêt *Privacy International*, la Cour de Justice était saisie d'une question portant sur 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 des données de localisation aux services de renseignement de sécurité.

L'avant-projet de loi doit donc être examiné en tenant compte de la circonstance que les exigences qui résultent des décisions précitées se situent essentiellement dans un contexte de lutte contre la criminalité, qui selon le cas, présente ou pas un caractère de gravité, et de protection de la sécurité nationale spécialement dans des cas où celle-ci est gravement menacée, en particulier par des actes de terrorisme.

Rien ne permet, à priori, d'étendre la portée de cet arrêt à une conservation ou à un accès à des données conservées qui auraient d'autres finalités comme la recherche, par un service de médiation, de l'auteur d'appels malveillants, l'identification de l'appelant ou du lieu d'un appel aux service d'urgence, en vue de permettre à ceux-ci d'intervenir afin de pouvoir garantir la sauvegarde des biens et des personnes, ou la recherche, indépendante de tout contexte infractionnel, d'une personne dont la disparition est inquiétante et dont il apparait que la vie pourrait être en danger imminent, ni même aux activités des services de renseignement et de sécurité.

Ces dernières hypothèses doivent donc être examinées non pas tant au regard de la jurisprudence précitée que de l'article 15, paragraphe 1, de la directive 2002/58/CE, dans la mesure où cette disposition permet d'autres dérogations que celles examinées dans les arrêts précités, ainsi qu'au regard des aspects plus généraux du droit au respect de la vie privée, garanti par l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, par l'article 7 de la Chartre des droits fondamentaux de l'Union européenne et par l'article 22 de la Constitution [11], et du droit à la protection des données à caractère personnel, garanti spécifiquement par l'article 8 de la Chartre des droits fondamentaux de l'Union européenne ainsi que de la réglementation européenne y afférente, comme le règlement (UE) 2016/679 du parlement européen 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

[11] Voir e.a., L. TASSONE, *« La protection des données dans la jurisprudence de la Cour européenne des droits de l'homme »* in « Enjeux européens et mondiaux de la protection des données personnelles », ouvrage collectif sous la direction D'A. GROSJEAN, Larcier, coll. Création Information Communication, p. 53 et s., et les références citées ; concernant les services de renseignement et de sécurité, voir e.a. l'avis n° 42.178/2 donné le 19 février 2007 sur un avant-projet devenu la loi du 4 février 2010 'relative aux méthodes de recueil des données par les services de renseignement et de sécurité', *Doc. parl.*, Sénat, 2006-2007, n° 3-2138/1, pp. 279-297, http://www.raadvst-consetat.be/dbx/avis/42178.pdf.

‡LW-BEHVMBJEH-GJDIBQW‡

la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)' (ci-après le « RGPD »).

5. Précisément en ce qui concerne le RGPD, l'arrêt *La Quadrature du Net* comporte des enseignements qui doivent être retenus.

Ainsi, dans son arrêt, la Cour de Justice a considéré :

« 193. Par la seconde question dans l'affaire C-512/18, la juridiction de renvoi cherche, en substance, à savoir si les dispositions de la directive 2000/31, lues à la lumière des articles 6 à 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doivent être interprétées en ce sens qu'elles s'opposent à une réglementation nationale imposant aux fournisseurs d'accès à des services de communication au public en ligne et aux fournisseurs de services d'hébergement la conservation généralisée et indifférenciée, notamment, des données à caractère personnel afférentes à ces services.

194. Tout en considérant que de tels services relèvent du champ d'application de la directive 2000/31, et non de celui de la directive 2002/58, la juridiction de renvoi est d'avis que l'article 15, paragraphes 1 et 2, de la directive 2000/31, lu en combinaison avec les articles 12 et 14 de celle-ci, n'instaure pas, par lui-même, une interdiction de principe de conserver des données relatives à la création de contenu à laquelle il pourrait seulement être dérogé de manière exceptionnelle. Cette juridiction se demande néanmoins si cette appréciation doit être retenue, compte tenu du respect nécessaire des droits fondamentaux consacrés aux articles 6 à 8 et 11 de la Charte.

195. En outre, la juridiction de renvoi précise que sa question vise l'obligation de conservation prévue à l'article 6 de la LCEN, lu en combinaison avec le décret n° 2011-219. Les données que doivent conserver les fournisseurs de services concernés à ce titre incluent, notamment, les données relatives à l'identité civile des personnes ayant fait usage de ces services, tels que leurs nom, prénom, leurs adresses postales associées, leurs adresses de courrier électronique ou de compte associées, leurs mots de passe et, lorsque la souscription du contrat ou du compte est payante, le type de paiement utilisé, la référence du paiement, le montant ainsi que la date et l'heure de la transaction.

196. De même, les données visées par l'obligation de conservation couvrent les identifiants des abonnés, des connexions et des équipements terminaux utilisés, les identifiants attribués aux contenus, les dates et heures de début et de fin des connexions et des opérations ainsi que les types de protocoles utilisés pour la connexion au service et pour le transfert des contenus. L'accès à ces données, dont la durée de conservation s'élève à un an, peut être sollicité dans le cadre des procédures pénales et civiles, en vue de faire respecter les règles relatives à la responsabilité civile ou pénale, ainsi que dans le cadre de mesures de recueil de renseignement auxquelles l'article L. 851-1 du CSI s'applique.

197. À cet égard, il y a lieu de relever que, conformément à son article 1er, paragraphe 2, la directive 2000/31 rapproche certaines dispositions nationales applicables aux services de la société de l'information visés à son article 2, sous a).

‡LW-BEHVMBJEH-GJDIBQW‡

198. De tels services englobent, certes, ceux qui sont fournis à distance au moyen d'équipements électroniques de traitement et de stockage de données, à la demande individuelle d'un destinataire de services et, normalement, contre rémunération, tels que des services d'accès à Internet ou à un réseau de communication ainsi que des services d'hébergement (voir, en ce sens, arrêts du 24 novembre 2011, Scarlet Extended, C-70/10, EU:C:2011:771, point 40 ; du 16 février 2012, SABAM, C-360/10, EU:C:2012:85, point 34 ; du 15 septembre 2016, Mc Fadden, C-484/14, EU:C:2016:689, point 55, ainsi que du 7 aout 2018, SNB-REACT, C-521/17, EU:C:2018:639, point 42 et jurisprudence citée).

199. Toutefois, l'article 1, paragraphe 5, de la directive 2000/31 dispose que celle-ci n'est pas applicable aux questions relatives aux services de la société de l'information qui sont couvertes par les directives 95/46 et 97/66. À cet égard, il ressort des considérants 14 et 15 de la directive 2000/31 que la protection de la confidentialité des communications ainsi que des personnes physiques à l'égard du traitement des données à caractère personnel dans le cadre des services de la société de l'information est uniquement régie par les directives 95/46 et 97/66, cette dernière interdisant, à son article 5, aux fins de la protection de la confidentialité des communications, toute forme d'interception ou de surveillance des communications.

200. Ainsi, des questions liées à la protection de la confidentialité des communications et des données à caractère personnel doivent être appréciées à l'aune de la directive 2002/58 et du règlement 2016/679, ceux-ci ayant remplacé respectivement la directive 97/66 et la directive 95/46, étant précisé que la protection que vise à assurer la directive 2000/31 ne peut en tout état de cause pas porter atteinte aux exigences résultant de la directive 2002/58 et du règlement 2016/679 (voir, en ce sens, arrêt du 29 janvier 2008, Promusicae, C-275/06, EU:C:2008:54, point 57).

201. L'obligation imposée par la réglementation nationale visée au point 195 du présent arrêt aux fournisseurs d'accès à des services de communication au public en ligne et aux fournisseurs de services d'hébergement de conserver des données à caractère personnel afférentes à ces services doit donc, comme l'a relevé en substance M. l'avocat général au point 141 de ses conclusions dans les affaires jointes La Quadrature du Net e.a. (C-511/18 et C‑512/18, EU:C:2020:6), être appréciée à l'aune de la directive 2002/58 ou du règlement 2016/679.

202. Ainsi, selon que la fourniture des services couverts par cette réglementation nationale relève ou non de la directive 2002/58, elle sera régie soit par cette dernière directive, en particulier par l'article 15, paragraphe 1, de celle-ci, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, soit par le règlement 2016/679, en particulier par l'article 23, paragraphe 1, dudit règlement, lu à la lumière des mêmes dispositions de la Charte.

203. En l'occurrence, il ne saurait être exclu, comme l'a relevé la Commission européenne dans ses observations écrites, que certains des services auxquels s'applique la réglementation nationale visée au point 195 du présent arrêt constituent des services de communications électroniques, au sens de la directive 2002/58, ce qu'il appartient à la juridiction de renvoi de vérifier.

204. À cet égard, il convient de relever que la directive 2002/58 couvre les services de communications électroniques qui remplissent les conditions énoncées à l'article 2, sous c), de la directive 2002/21, auquel renvoie l'article 2 de la directive 2002/58 et qui définit le service de communications électroniques comme étant 'le service fourni normalement contre rémunération qui consiste entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques, y compris les services de télécommunications et les services de

‡LW-BEHVMBJEH-GJDIBQW‡

transmission sur les réseaux utilisés pour la radiodiffusion'. S'agissant des services de la société de l'information, tels que visés aux points 197 et 198 du présent arrêt et couverts par la directive 2000/31, ceux-ci constituent des services de communications électroniques dès lors qu'ils consistent entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques (voir, en ce sens, arrêt du 5 juin 2019, Skype Communications, C-142/18, EU:C:2019:460, points 47 et 48)

205. Ainsi, les services d'accès à Internet, lesquels paraissent être couverts par la réglementation nationale visée au point 195 du présent arrêt, constituent, comme le confirme le considérant 10 de la directive 2002/21, des services de communications électroniques, au sens de cette directive (voir, en ce sens, arrêt du 5 juin 2019, Skype Communications, C-142/18, EU:C:2019:460, point 37). Tel est également le cas des services de messageries sur Internet, dont il ne semble pas exclu qu'ils relèvent également de cette réglementation nationale, dès lors que, sur le plan technique, ils impliquent entièrement ou principalement la transmission de signaux sur des réseaux de communications électroniques (voir, en ce sens, arrêt du 13 juin 2019, Google, C-193/18, EU:C:2019:498, points 35 et 38).

206. S'agissant des exigences découlant de l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, il convient de renvoyer à l'ensemble des constatations et des appréciations faites dans le cadre de la réponse apportée aux premières questions dans les affaires C-511/18 et C-512/18 ainsi qu'aux première et deuxième questions dans l'affaire C-520/18.

207. Quant aux exigences découlant du règlement 2016/679, il convient de rappeler que celui-ci vise, notamment, ainsi qu'il ressort de son considérant 10, à assurer un niveau élevé de protection des personnes physiques au sein de l'Union et, à cette fin, à assurer une application cohérente et homogène des règles de protection des libertés et des droits fondamentaux de ces personnes à l'égard du traitement des données à caractère personnel dans l'ensemble de l'Union (voir, en ce sens, arrêt du 16 juillet 2020, Facebook Ireland et Schrems, C-311/18, EU:C:2020:559, point 101).

208. À cette fin, tout traitement de données à caractère personnel doit, sous réserve des dérogations admises à l'article 23 du règlement 2016/679, respecter les principes régissant les traitements des données à caractère personnel ainsi que les droits de la personne concernée énoncés respectivement dans les chapitres II et III de ce règlement. En particulier, tout traitement de données à caractère personnel doit, d'une part, être conforme aux principes énoncés à l'article 5 dudit règlement et, d'autre part, satisfaire aux conditions de licéité énumérées à l'article 6 de ce même règlement (voir, par analogie, en ce qui concerne la directive 95/46, arrêt du 30 mai 2013, Worten, C-342/12, EU:C:2013:355, point 33 et jurisprudence citée).

209. Pour ce qui est, plus particulièrement, de l'article 23, paragraphe 1, du règlement 2016/679, il y a lieu de relever que celui-ci, à l'instar de ce qui est prévu à l'article 15, paragraphe 1, de la directive 2002/58, permet aux États membres de limiter, au regard des finalités qu'il prévoit et au moyen de mesures législatives, la portée des obligations et des droits qui y sont visés « lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir » la finalité poursuivie. Toute mesure législative prise sur ce fondement doit, en particulier, respecter les exigences spécifiques posées à l'article 23, paragraphe 2, de ce règlement.

‡LW-BEHVMBJEH-GJDIBQW‡

210. Ainsi, l'article 23, paragraphes 1 et 2, du règlement 2016/679 ne saurait être interprété comme pouvant conférer aux États membres le pouvoir de porter atteinte au respect de la vie privée, en méconnaissance de l'article 7 de la Charte, tout comme aux autres garanties prévues par celle-ci (voir, par analogie, en ce qui concerne la directive 95/46, arrêt du 20 mai 2003, Österreichischer Rundfunk e.a., C-465/00, C-38/01 et C-139/01, EU:C:2003:294, point 91). En particulier, à l'instar de ce qui vaut pour l'article 15, paragraphe 1, de la directive 2002/58, le pouvoir que confère l'article 23, paragraphe 1, du règlement 2016/679 aux États membres ne saurait être exercé que dans le respect de l'exigence de proportionnalité, selon laquelle les dérogations à la protection des données à caractère personnel et les limitations de celles-ci doivent s'opérer dans les limites du strict nécessaire (voir, par analogie, s'agissant de la directive 95/46, arrêt du 7 novembre 2013, IPI, C-473/12, EU:C:2013:715, point 39 et jurisprudence citée).

211. Il s'ensuit que les constatations et les appréciations faites dans le cadre de la réponse apportée aux premières questions dans les affaires C-511/18 et C-512/18 ainsi qu'aux première et deuxième questions dans l'affaire C-520/18 s'appliquent mutatis mutandis à l'article 23 du règlement 2016/679 ».

Pour conclure, la Cour de Justice a dit pour droit :

« La directive 2000/31/CE du Parlement européen et du Conseil, du 8 juin 2000, relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur ('directive sur le commerce électronique'), doit être interprétée en ce sens qu'elle n'est pas applicable en matière de protection de la confidentialité des communications et des personnes physiques à l'égard du traitement des données à caractère personnel dans le cadre des services de la société de l'information, cette protection étant, selon le cas, régie par la directive 2002/58, telle que modifiée par la directive 2009/136, ou par 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. L'article 23, paragraphe 1, du règlement 2016/679, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale imposant aux fournisseurs d'accès à des services de communication au public en ligne et aux fournisseurs de services d'hébergement la conservation généralisée et indifférenciée, notamment, des données à caractère personnel afférentes à ces services ».

6. Enfin, il convient d'avoir particulièrement égard à l'invitation formulée par la Cour constitutionnelle dans son arrêt n° 57/2021.

Pour rappel, la Cour constitutionnelle a considéré que :

– Un changement de perspective s'impose 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 être soumise à des règles claires et précises concernant la portée et l'application de la mesure en cause et imposant des exigences minimales.

‡LW-BEHVMBJEH-GJDIBQW‡

– 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 ».

Dans ce but, il appartient au législateur 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.

I.2. LA JURISPRUDENCE DE LA COUR EUROPÉENNE DES DROITS DE L'HOMME

De manière plus générale, il convient également d'avoir égard au droit au respect de la vie privée, garanti par l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et par l'article 22 de la Constitution [12].

De la jurisprudence de la Cour européenne des droits de l'homme [13], s'agissant spécialement de la surveillance secrète et de l'interception de masse des communications et des données y afférentes, il y a lieu de retenir, en substance, les principes suivants :

– 1° la surveillance secrète des citoyens n'est admissible que dans la mesure où elle est strictement nécessaire à la sauvegarde des institutions démocratiques. Des dispositions législatives qui accordent des pouvoirs de surveillance secrète de la correspondance, des envois postaux et des télécommunications sont, devant une situation exceptionnelle telle la menace par des formes complexes d'espionnage et par le terrorisme, nécessaires dans une société démocratique à la sécurité nationale et/ou à la défense de l'ordre et à la prévention des infractions pénales ;

– 2° L'organisation d'un tel régime doit toutefois être « prévu par la loi » et « nécessaire » ; dans ce cadre, la Cour européenne des droits de l'homme examine si le cadre juridique national définit clairement :

1. Les motifs pour lesquels l'interception en masse peut être autorisée ;

2. Les circonstances dans lesquelles les communications d'un individu peuvent être interceptées ;

3. La procédure d'octroi d'une autorisation ;

4. Les procédures à suivre pour la sélection, l'examen et l'utilisation des éléments interceptés ;

[12] Voir e.a., L. TASSONE, *« La protection des données dans la jurisprudence de la Cour européenne des droits de l'homme »* in « Enjeux européens et mondiaux de la protection des données personnelles », ouvrage collectif sous la direction d'A. Grosjean, Larcier, coll. Création Information Communication, p. 53 et s. , et les références citées ; concernant les services de renseignement et de sécurité, voir e.a. l'avis n° 42.178/2.

[13] Voir notamment, pour un arrêt de principe, Cour.eur.D.H, arrêt *Klass et autres c. Allemagne*, 9 septembre 1978. Pour un rappel récent de la jurisprudence en la matière et des principes en la matière tels qu'ils résultent de celle-ci, voir Cour.eur.D.H, arrêt *Big Brother watch et autre c. Royaume-Uni*, 25 mai 2021, 322 à 364.

‡LW-BEHVMBJEH-GJDIBQW‡

5. Les précautions à prendre pour la communication de ces éléments à d'autres parties ;

6. Les limites posées à la durée de l'interception et de la conservation des éléments interceptés, et les circonstances dans lesquelles ces éléments doivent être effacés ou détruits ;

7. Les procédures et modalités de supervision, par une autorité indépendante, du respect des garanties énoncées ci-dessus, et les pouvoirs de cette autorité en cas de manquement ;

8. Les procédures de contrôle indépendant à posteriori du respect des garanties et les pouvoirs conférés à l'organe compétent pour traiter les cas de manquement.

Le processus doit ainsi être encadré par des « garanties de bout en bout », qui permettent de s'assurer que la nécessité et la proportionnalité des mesures prises est appréciée à chaque étape du processus de la surveillance, spécialement de l'interception des données ; ces garanties impliquent [14] notamment que

– les activités d'interception, à tout le moins de masse, doivent être soumises à l'autorisation d'une autorité indépendante dès le départ, à savoir lors de la définition de l'objet et de l'étendue de l'activité ;

– les activités doivent faire l'objet d'une supervision et d'un contrôle indépendant opéré à posteriori [15].

EXAMEN DE L'AVANT-PROJET

OBSERVATION PRÉALABLE

Avant toute autre observation, il échet de rappeler que dans son arrêt n° 57/2021, faisant suite à l'arrêt *La Quadrature du Net*, la Cour constitutionnelle a invité le législateur à opérer un changement de perspective dans la conservation des données concernées, de sorte que celle-ci demeure l'exception et non la règle, et qu'elle soit organisée par des règles claires et précises concernant la portée et l'application de la mesure en cause et imposant des exigences minimales de telle sorte que l'ingérence se limite au strict nécessaire et réponde à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi. La Cour constitutionnelle a suggéré que, dans ce but, le législateur opère les distinctions qui s'imposent entre les différents types de données soumises à conservation.

[14] Voir à ce propos, e.a., Cour.eur.D.H, arrêt *Big Brother watch et autre c. Royaume-Uni* , 25 mai 2021, 350.

[15] La Cour européenne des droits de l'homme considère « qu'en ce qui concerne l'interception en masse, l'interception et la conservation des données de communication associées, ainsi que les recherches effectuées sur celles-ci, doivent être analysées au regard des mêmes garanties que celles applicables au contenu des communications, mais qu'il n'est pas nécessaire que les dispositions juridiques régissant le traitement des données de communication associées soient identiques en tous points à celles régissant le traitement du contenu des communications ». Elle considère en tout cas que l'exigence d'une autorisation indépendante vaut pour ces deux catégories (voir à ce propos, e.a., Cour.eur.D.H, arrêt *Big Brother watch et autre c. Royaume-Uni*, 25 mai 2021, 363 et 364, et 417 et 418).

‡LW-BEHVMBJEH-GJDIBQW‡

L'avant-projet à l'examen se donne pour objet de répondre clairement à cet arrêt, en s'inscrivant dans les balises ainsi posées par la Cour constitutionnelle.

L'avant-projet appelle toutefois différentes observations générales, au regard, notamment, de la limitation au strict nécessaire des différents régimes de conservation organisés par catégories de données et de finalités, de la clarté et de la précision des régimes en projet, et de leur conformité au principe de légalité inscrit à l'article 22 de la Constitution, ce outre les observations particulières qui seront formulées ensuite.

OBSERVATIONS GÉNÉRALES

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, en vue d'assurer la sécurité nationale, dans des situations où l'État fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible

1. Pour rappel, selon l'enseignement de l'arrêt *La Quadrature du Net*, est admissible une législation qui permet qu'une injonction soit donnée 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, en vue d'assurer la sécurité nationale, dans des situations où l'État fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible.

Il faut toutefois que la décision emportant cette injonction puisse 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. Par ailleurs, cette injonction ne peut être émise que pour une période temporellement limitée au strict nécessaire, mais elle peut être renouvelée en cas de persistance de cette menace.

2.1.1. L'article 31 de l'avant-projet à l'examen entend insérer, dans la loi du 30 novembre 1998 'organique des services de renseignements et de sécurité' un article 18/17/1, rédigé comme suit :

> « 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 pour procéder à la conservation généralisée et indifférenciée des données de trafic et de localisation de moyens de communications électroniques générées et traités par eux.
>
> La réquisition est effectuée par écrit par le dirigeant du service et mentionne la nature de l'avis conforme de la commission, la nature de l'avis conforme du président de la commission ou la nature de l'autorisation du ministre concerné visée à l'article 18/10 § 3, alinéa 3, selon le cas.
>
> L'autorisation du dirigeant du service est transmise au ministre compétent.

‡LW-BEHVMBJEH-GJDIBQW‡

Le service de renseignement et de sécurité concerné peut requérir le concours de l'Institut visé à l'article 2, 1° de la loi du 13 juin 2005 relative aux communications électroniques pour transmettre la réquisition à tous les opérateurs concernés.

Le dirigeant du service peut requérir, par une décision écrite, des personnes dont il présume qu'elles ont une expertise technique utile de prêter leur concours à la mise en œuvre de cette méthode. Cette réquisition mentionne la nature de l'avis conforme de la commission, la nature de l'avis conforme du président de la commission ou la nature de l'autorisation du ministre concerné, selon le cas.

Toute personne qui refuse de procéder à la conservation requise est punie d'une amende de vingt-six euros à vingt mille euros.

La méthode est autorisée pour une durée ne pouvant excéder 6 mois sans préjudice de la procédure visée à l'article 18/10, § 5.

Le service de renseignement et de sécurité concerné fait rapport à la commission tous les deux mois 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.

Le Roi peut déterminer, sur la proposition du ministre de la Justice, du ministre de la Défense et du ministre qui a les communications électroniques dans ses attributions, des modalités de collaboration des opérateurs ».

2.1.2. Il y a lieu de constater que la disposition en projet répond aux exigences de droit européen dans la mesure où elle limite la possibilité d'injonction aux opérateurs à la seule fin de garantir la sécurité nationale, dans des situations où l'État fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible.

2.1.3. Quant à la durée de l'opération – laquelle doit être limitée au strict nécessaire – le système mis en place prévoit qu'

– elle est limitée à six mois maximum, étant entendu que le service de renseignement et de sécurité concerné fait rapport à la Commission [16] tous les deux mois sur l'évolution de la menace, rapport qui a pour objet de mettre en évidence les éléments qui justifient soit le maintien de la conservation généralisée et indifférenciée, soit la fin de celle-ci.

– elle peut être prolongée aux conditions strictes de l'article 18/10, § 5, de la loi du 30 novembre 1998 [17].

[16] Il s'agit de la Commission instituée par l'article 43/1 de la loi du 30 novembre 1998.

[17] Selon cette disposition :
« Le dirigeant du service peut, sur avis conforme préalable de la commission, autoriser la prolongation de la méthode exceptionnelle de recueil de données pour une nouvelle période ne pouvant excéder deux mois à compter de l'échéance de la méthode en cours, sans préjudice de l'obligation qui lui est faite de mettre fin à la méthode dès que la menace potentielle qui la justifie a disparu, que la méthode n'est plus utile à la finalité pour laquelle elle a été décidée ou qu'il constate une illégalité. Dans ce cas, le dirigeant du service concerné porte à la connaissance de la commission sa décision motivée de mettre fin à la méthode exceptionnelle.
Une seconde prolongation et toute nouvelle prolongation de la méthode exceptionnelle de recueil de données n'est possible qu'en présence de circonstances particulières nécessitant de prolonger l'utilisation de cette méthode. Ces motifs particuliers sont indiqués dans la décision. Si ces circonstances particulières font défaut, il doit être mis fin à la méthode.
Les conditions prévues aux paragraphes 1er à 3 sont applicables aux modalités de prolongation de la méthode exceptionnelle de recueil de données qui sont prévues dans le présent paragraphe ».

‡LW-BEHVMBJEH-GJDIBQW‡

Ce système, qui résulte de la combinaison de l'article 18/10, en vigueur, et de l'article 18/17/1, en projet, de la loi du 30 novembre 1998, apparait ainsi de nature à répondre aux exigences résultant du droit européen sur ce point.

2.1.4.1. Par contre, des difficultés se posent à propos de la question de savoir si l'opération envisagée est soumise :

– à « l'autorisation d'une autorité indépendante dès le départ – dès la définition de l'objet et de l'étendue de l'opération » – selon les termes de la jurisprudence de la Cour européenne des droits de l'homme, spécialement l'arrêt *Big Brother watch* [18] ;

– à « 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 » – selon les termes de la jurisprudence de la Cour de Justice.

2.1.4.2. Concernant l'arrêt *Big Brother watch*, comme mentionné précédemment, la Cour européenne des droits de l'homme considère que

> « l'interception en masse, l'interception et la conservation des données de communication associées, ainsi que les recherches effectuées sur celles-ci, doivent être analysées au regard des mêmes garanties que celles applicables au contenu des communications, mais qu'il n'est pas nécessaire que les dispositions juridiques régissant le traitement des données de communication associées soient identiques en tous points à celles régissant le traitement du contenu des communications ».

Elle considère en tout cas que l'exigence d'une autorisation indépendante vaut pour ces deux catégories.

Interrogé à ce propos, les délégués du Ministre ont répondu ce qui suit, concernant la portée de la notion de « l'interception et la conservation des données de communication associées » :

> « Door deze niet afzonderlijk te benoemen, impliceert het Hof volgens […] dat haar conclusie enkel van toepassing is wanneer ook de bulk interceptie van de inhoud van communicatie georganiseerd wordt. Het Hof spreekt zich niet uit over de bewaring van enkel de meta-data, waarbij verondersteld mag worden dat deze maatregel minder intrusief is dan het bewaren van de inhoud van de communicatie.
>
> Minder intrusief, maar nog steeds intrusief. Daarom voorzien we de waarborg van de BIM-commissie die voorafgaandelijk toestemming moet geven in het geval van een ernstige dreiging tegen de nationale veiligheid, of een mechanisme dat in de wet beschreven staat dat ook betrekking heeft op de nationale veiligheid ».

Il convient par ailleurs de relever que, selon l'article 18/10, § 1er, de la loi du 30 novembre 1998, « [l]e dirigeant du service met fin à la méthode exceptionnelle lorsque la menace potentielle grave qui la justifie a disparu, lorsque la méthode n'est plus utile pour la finalité pour laquelle elle avait été mise en œuvre, ou quand il a constaté une illégalité. Il informe dès que possible la [c]ommission de sa décision ».

[18] Voir à ce propos, e.a., Cour.eur.D.H., arrêt *Big Brother watch et autre c. Royaume-Uni*, 25 mai 2021, 350.

‡LW-BEHVMBJEH-GJDIBQW‡

Au regard des explications ainsi communiquées, il y a effectivement lieu de constater que l'arrêt *Big Brother watch* ne se prononce pas sur un système qui aurait pour seul objet la conservation de données associées à des contenus de communications électroniques, mais sur un système qui englobait l'interception des contenus, des métadonnées, interception qui ne visait pas uniquement le stockage, la conservation de ces données, mais également l'accès à celles-ci et leur analyse [19].

Il apparait donc délicat d'étendre l'enseignement de cet arrêt, spécialement les exigences en matière de contrôle préalable par une juridiction ou un organisme indépendant, au mécanisme de conservation généralisée et indifférenciée envisagée par le texte en projet.

Si toutefois tel devait être le cas, il conviendrait alors de relever qu'il ressort de l'article 18/10, § 1er, de la loi du 30 novembre 1998 que l'avis conforme de la commission sera requis préalablement à la décision du dirigeant du service. La commission vérifiera ainsi

> « si les dispositions légales relatives à l'utilisation de la méthode exceptionnelle pour le recueil de données, ainsi que les principes de subsidiarité et de proportionnalité prévus à l'article 18/9 § § 2 et 3, sont respectés et qui contrôle les mentions prescrites par le § 2 ».

Cette commission, dont l'article 43/1, § 1er de la loi du 30 novembre 1998 prévoit qu'elle est composée de magistrats et effectue sa tâche de contrôle en toute indépendance répond à la notion d'« autorité administrative indépendante au sens des jurisprudences rappelées ci-avant. Son avis conforme est contraignant : en vertu de l'article 18/10, § 3, alinéa 2, lorsque son avis est négatif, l'opération envisagée ne peut pas être mise en œuvre.

Il reste que, selon l'article 18/10, § 3, alinéa 3, de la loi du 30 novembre 1998,

> « Si la commission ne rend pas d'avis dans le délai de quatre jours ou informe le service concerné qu'elle est dans l'impossibilité de délibérer dans ce délai conformément à l'article 43, paragraphe 1er, alinéa 7, le service concerné peut saisir le ministre compétent, qui autorisera ou n'autorisera pas la mise en œuvre dans les plus brefs délais de la méthode envisagée. Le ministre communique sa décision aux présidents de la commission et du Comité permanent R ».

Dans les deux hypothèses énoncées, à défaut d'intervention de la commission, c'est le Ministre qui prend la décision d'autoriser l'opération. Or, le Ministre ne constitue pas une « autorité administrative indépendante » dont l'intervention serait requise [20].

2.1.4.3. Au regard des missions confiées au Comité permanent R par les articles 43/2 et suivants de la loi du 30 novembre 1998, le système mis en place ne parait pas poser de difficulté par rapport aux exigences de contrôle énoncées par la Cour de Justice.

2.2. Le dispositif en projet appelle toutefois une observation fondamentale au regard du droit constitutionnel.

[19] Voir, sur le système examiné par la Cour européenne des droits de l'homme, les paragraphes 15 à 17 de l'arrêt.

[20] Cour eur. D.H. arrêt du 25 mai 2021, *Big Brother watch et autre c. Royaume-Uni* , 377.

‡LW-BEHVMBJEH-GJDIBQW‡

La conservation « généralisée et indifférenciée » organisée par l'article 18/17/1, en projet suppose ainsi qu'une injonction soit donnée à tous les opérateurs fournissant des services de communications électroniques. Même si seuls certains opérateurs préalablement identifiés étaient requis de procéder à cette conservation, il n'en reste pas moins qu'un ordre leur serait ainsi donné de conserver les données de trafic et de localisation de manière généralisée et indifférenciée.

Aussi, cette « injonction », fût-elle limitée dans le temps ne constitue pas un acte administratif à portée individuelle, revêt-elle un caractère général et abstrait, dont les opérateurs sont le medium. Par conséquent, la décision d'imposer cette conservation « généralisée et indifférenciée » est de nature réglementaire.

Concernant l'attribution d'un pouvoir réglementaire à une autorité qui n'est pas responsable politiquement devant les assemblées législatives concernées – c'est-à-dire, à une autorité autre que le Roi agissant sous le contreseing d'un Ministre, ou qu'un Ministre –, la section de législation a déjà observé à de nombreuses reprises que l'attribution d'une compétence réglementaire à des agents ou à des organismes publics ou à leurs organes est difficilement compatible avec les principes généraux du droit public belge (article 33 et 108 de la Constitution), en ce qu'elle porte atteinte au principe de l'unité du pouvoir réglementaire et échappe à tout contrôle parlementaire direct. Les actes réglementaires de ce type sont en outre dépourvus des garanties dont est assortie la réglementation classique, telles que celles en matière de publication. Si dans le passé, la section de législation a déjà jugé admissibles certaines exceptions à l'interdiction de déléguer une compétence réglementaire à des agents ou des organismes publics, il s'agissait généralement de délégations de portée limitée ou accessoire et d'une technicité telle qu'il pouvait être considéré que les organismes qui devaient appliquer la réglementation concernée, étaient également les mieux placés pour l'élaborer [21].

La décision de principe d'imposer la conservation généralisée et indifférenciée des données de trafics et de localisation de moyens de communications électroniques ne revêt d'évidence pas un caractère limité ou accessoire et n'est pas d'une technicité telle qu'elle pourrait justifier qu'elle soit déléguée aux agents des services de renseignement et de sécurité.

Sous réserve de l'observation 2.1.4.2 et 2.1.4.3, c'est au Roi qu'il appartient, *in fine*, de prendre une telle décision à portée générale et abstraite.

Le texte en projet sera revu à la lumière de cette observation.

2.3. Le système mis en place par l'avant-projet à l'examen est susceptible d'engendrer une autre hypothèse dans laquelle une conservation généralisée et indifférenciée des métadonnées serait opérée.

[21] Voir entre autres, à ce propos, l'avis n° 69.160/4 donné le 6 mai 2021 sur un avant-projet de loi « introduisant des mesures de sécurité supplémentaires pour la fourniture de services mobiles 5G » et l'avis n° 69.166/4 donné le 10 juin 2021 sur un avant-projet de loi « portant transposition du code des communications électroniques européen et modification de diverses dispositions en matière de communications électroniques ».

‡LW-BEHVMBJEH-GJDIBQW‡

Il s'agit du cas prévu à l'article 126/1, § 3, alinéa 1er, 2°, en projet, de la loi du 13 juin 2005, qui permet la conservation des données de communications électroniques, visées au paragraphe 2 du même article, dans toutes les zones dont le niveau de menace, déterminé en vertu 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 10 juillet 2006 relative à l'analyse de la menace', et aussi longtemps qu'un niveau d'au moins 3 perdure pour ces zones.

Cette hypothèse est ainsi réglée, dans l'intention des auteurs de l'avant-projet, non pas au titre des cas de conservation généralisée et indifférenciée des données, mais au titre des situations de conservation ciblée de celles-ci.

Or, le passé récent a montré que le niveau 3 de menace était susceptible d'être atteint sur l'ensemble du territoire national, et ce, le cas échéant, pour une période relativement longue.

Dans l'hypothèse où le niveau 3 de menace serait atteint sur l'ensemble du territoire, le système aboutirait ainsi à une conservation généralisée et indifférenciée des métadonnées. La prudence impose donc de considérer que, pour cette situation spécifique, ce sont les principes relatifs à la conservation généralisée et indifférenciée qui trouvent à s'appliquer, et non ceux relatifs à la conservation ciblée.

Dans la mesure de cette hypothèse spécifique, le système en projet parait répondre aux exigences énoncées plus haut, quant aux finalités de la conservation [22] et à sa limitation dans le temps [23].

Par contre, se pose la question de savoir comment il sera satisfait à l'exigence de « contrôle effectif » au sens des jurisprudences rappelées ci-avant.

Le dispositif en projet sera revu et complété à la lumière de cette observation.

La conservation ciblée des données relatives au trafic et des données de localisation délimitée, 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

1. Pour rappel, selon l'enseignement de l'arrêt *La Quadrature du Net*, est admissible la conservation ciblée des données relatives au trafic et des données de localisation 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

[22] Le dispositif mis en place par la loi du 10 juillet 2006 et par l'arrêté royal du 28 novembre 2006 a vocation à s'appliquer, en première intention, à des menaces qui ont trait à des activités de terrorisme et d'extrémisme (voir l'article 3 de la loi du 10 juillet 2006 et l'article 8, 1°, b) et c) de la loi du 30 novembre 1998). Le niveau 3 de menace correspond à une menace grave, c'est-à-dire « possible et vraisemblable », le niveau 4 de menace correspond à une menace « très grave », c'est-à-dire « sérieuse et imminente », conformément à l'article 11, § 6, de l'arrêté royal du 28 novembre 2006.

[23] Les zones concernées ne font l'objet de l'opération de conservation qu'aussi longtemps qu'elles se trouvent à un niveau 3 ou 4 de menace.

‡LW-BEHVMBJEH-GJDIBQW‡

strict nécessaire, mais renouvelable, 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.

2. L'avant-projet à l'examen entend organiser le régime d'une telle conservation par l'insertion d'un article 126/1 nouveau dans la loi du 13 juin 2005.

En substance, cette disposition envisage la conservation de trois catégories de données de trafic et de localisation énumérées en son paragraphe 2 (données d'accès et de connexion, données de communications, données des appels infructueux). Le Roi est chargé de fixer les données à conserver, dans ces trois catégories, ainsi que les exigences auxquelles elles doivent répondre.

3. La conservation a pour finalité, selon la paragraphe 1er, alinéa 3, en projet, 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.

Ces finalités correspondent formellement à celles mentionnées par l'arrêt *La Quadrature du Net*, à l'exception de « la sauvegarde des intérêts vitaux d'une personne physique ». Toutefois, concernant cette finalité, il y a lieu de constater qu'elle relève d'un autre contexte que celui des questions préjudicielles auxquelles la Cour de Justice a répondu dans son arrêt *La Quadrature du Net*.

En tout état de cause, une telle finalité peut, à priori, être considérée comme relevant de la sauvegarde de la sécurité publique et des obligations positives incombant à ce titre aux États membres, en vue de garantir la vie et la sécurité des personnes.

Au regard des finalités de conservation, l'article 126/1 en projet n'apparait dès lors pas poser des difficultés au regard de la jurisprudence de la Cour de Justice et de la Cour constitutionnelle.

4.1.1. Le ciblage de la conservation concernée repose sur l'établissement de différentes catégories de zones géographiques, qui sont énumérées par le paragraphe 3 de la disposition en projet, à savoir :

1° les arrondissements judiciaires dans lesquels au moins trois infractions par mille habitants, parmi celles énumérées à l'article 90*ter* du Code d'instruction criminelle, ont été constatées durant l'année, sur une moyenne des trois années précédant celle en cours, ainsi que les zones de police présentant les mêmes caractéristiques et situées dans les arrondissements judiciaires qui ne répondent pas aux conditions précitées ;

2° les zones dont le niveau de la menace, déterminé en vertu de la loi du 10 juillet 2006 est au moins de niveau 3, et aussi longtemps qu'un niveau d'au moins 3 perdure pour ces zones ;

‡LW-BEHVMBJEH-GJDIBQW‡

3° les zones particulièrement exposées à des menaces pour la sécurité nationale ou à des risques élevés de criminalité grave ; sont mentionnés dans cette catégorie les ports, les gares, les stations de métro et de pré-métro, les bâtiments affectés à différents services comme la justice, la police locale et fédérale, les douanes et accises ; sont également visés les communes dans lesquelles se trouvent des domaines militaires, les prisons et les maisons de transition, les armuriers et stands de tir, les établissements visés par la réglementation en matière de protection contre les radiations ionisantes, les établissements « Seveso », les communes comportant une ou plusieurs infrastructures critiques, le réseau ASTRID, ainsi que les réseaux et systèmes d'information qui soutiennent la fourniture des services essentiels des opérateurs de services essentiels ;

4° les zones où il y a une menace grave potentielle pour les intérêts vitaux du pays ou pour les besoins essentiels de la population ; sont mentionnés à ce titre les zones neutres et les cabinets ministériels, 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 de la Défense et approuvée par le Conseil national de sécurité, les autoroutes et les parkings publics attenant, les assemblées législatives, les maisons communales et les hôtels de ville, les sièges des conseils provinciaux, le palais royal, les domaines royaux, les bâtiments affectés à différents services comme la justice, la police locale et fédérale, la sûreté de l'État ; sont également visés les communes dans lesquelles se trouvent des domaines militaires, et les communes frontalières, les hôpitaux et la Banque Nationale de Belgique ;

5° les zones où il y a une menace grave potentielle pour les intérêts des institutions internationales ; sont mentionnés à ce titre les ambassades et représentations diplomatiques, les bâtiments affectés à l'Union européenne, et à l'OTAN, les bureaux des institutions de l'Espace économique européen et les bureaux des Nations-Unies.

Les autorités compétentes dans l'une des matières en relation avec l'objet de la zone sont chargées de transmettre chaque année, à la date et au service déterminés par le Roi, les informations nécessaires à la détermination concrète des zones géographiques. Elles sont également tenues d'informer sans délai ce service lorsqu'une zone ne correspond plus au critère concerné afin qu'il soit mis fin le plus rapidement possible à l'obligation de conservation. La liste des zones est mise à jour chaque année, et mise à la disposition, selon le cas, du Comité permanent R par les services de renseignement et de sécurité, ou de l'Organe de contrôle de l'information policière.

4.1.2. Pour les zones relevant des catégories citées aux points 3°, 4° et 5°, ci-avant, il est prévu que, 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 en charge des communications électroniques, et après avis des Autorités de protection des données compétentes et de l'Institut belge des services postaux et des télécommunications (ci-après « l'Institut »), le Roi peut fixer d'autres zones, par un arrêté qui doit être renouvelé tous les trois ans. À défaut de renouvellement, l'obligation de conservation dans les zones géographiques additionnelles cesse de s'appliquer, et ce jusqu'à l'entrée en vigueur d'une éventuel nouvel arrêté royal.

‡LW-BEHVMBJEH-GJDIBQW‡

Il est également prévu que

« 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 ».

4.1.3. Par ailleurs, 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 en charge de communications électroniques, et après avis des Autorités de protection des données compétentes et de l'Institut, les paramètres techniques et les données que les opérateurs utilisent pour limiter la conservation de données aux zones visées, la liste des différentes autorités compétentes dans les matières concernées, les modalités de communication des informations par les autorités compétentes vers le 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 pour la zone concernée.

4.1.4. Un rapport d'évaluation annuel est établi, qui est adressé à la Chambre des représentants et à l'Organe de contrôle de l'information policière. Par contre, s'agissant de la transparence administrative et de l'information du public, l'article 126/1, § 3, dernier alinéa, en projet, prévoit :

« La loi du 11 avril 1994 relative à la publicité de l'administration et la loi du 5 aout 2006 relative à l'accès du public à l'information en matière d'environnement ne s'appliquent pas aux informations, documents ou données, sous quelque forme que ce soit, visés au présent article, à l'exception des statistiques de criminalité visées à l'alinéa 1er, point 1° ».

4.1.5. De manière concrète, les opérateurs seront tenus de conserver les données pour toutes les communications effectuées à partir de l'une des zones précitées, ou vers cette zone. Les seules données d'un utilisateur final qui seront conservées sont celles traitées ou générées lorsqu'il se trouve dans la zone concernée.

Toutefois, il est prévu que

« [l]orsque la technologie utilisée par l'opérateur ne permet pas de limiter la conservation de données aux zones visées au paragraphe 3, il conserve au moins les données nécessaires pour couvrir l'entièreté 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 ».

4.2.1. Le système ainsi mis en place pose question sur différents points.

4.2.2. Tout d'abord, comme le relève le commentaire de l'article, dans son arrêt *La Quadrature du net*, la Cour de Justice a considéré que la conservation ciblée de données pouvait se fonder sur des critères géographiques

« 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.[…] Ces zones peuvent être, notamment, des lieux caractérisés par un

‡LW-BEHVMBJEH-GJDIBQW‡

> 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 » [24].

Il y a lieu de constater que les auteurs de l'avant-projet se sont efforcés, dans le choix des zones retenues, de se limiter à la mise en œuvre des critères mentionnés par la Cour de Justice.

Il faut également constater que le commentaire de l'article entend justifier les raisons pour lesquelles, au regard des critères ainsi mis en œuvre, chaque type de zone pouvait et devait être inclus dans l'énumération retenue.

Il reste toutefois que, d'une part, le nombre et la variété des zones ainsi énumérées sont considérables, et que, d'autre part, leur addition aboutit à couvrir une partie assez importante du territoire.

Pour certaines zones, la qualification de « lieu caractérisé par un nombre élevé d'actes de criminalité grave », ou de « lieu particulièrement exposés à la commission d'actes de criminalité grave, en tant que fréquenté par un nombre très élevé de personnes », ou encore de « lieu stratégique », n'apparait pas évidente.

Il en va ainsi, à titre d'exemples, des maisons de transition visées à la loi du 17 mai 2006 'relative au statut juridique externe des personnes condamnées à une peine privative de liberté et aux droits reconnus à la victime dans le cadre des modalités d'exécution de la peine', des autoroutes dans leur ensemble, des maisons communales et hôtels de ville ou encore des sièges des conseils provinciaux.

Aussi, la section de législation ne peut-elle que prendre acte des justifications déjà données, et inviter les auteurs de l'avant-projet à justifier plus avant encore le choix des zones retenues. À défaut de justification claire, précise et spécifique pour chaque type de zone, le texte en projet sera entaché d'un aléa lié à la question de savoir si le régime de conservation envisagé se limite effectivement au « strict nécessaire ».

L'énumération des zones envisagées sera réexaminée en conséquence.

4.2.3. La question se pose de savoir par quelle autorité le périmètre de chaque zone sera délimité, étant entendu que la précision de ce périmètre et sa limitation au strict nécessaire sont requises au regard de l'arrêt *La Quadrature du Net*.

[24] Paragraphe 150 de l'arrêt.

‡LW-BEHVMBJEH-GJDIBQW‡

Ainsi, dans le système prévu par le texte en projet, l'autorité compétente dans la matière en rapport avec l'objet de la zone sera chargée de transmettre chaque année au service désigné par le Roi, les informations nécessaires à la détermination concrète des zones géographiques. Elle devra également informer sans délai le même service lorsqu'une zone géographique ne correspond plus au critère concerné afin qu'il soit mis un terme le plus rapidement possible à la conservation des données [25].

Par ailleurs, il est prévu que chaque année, et chaque fois qu'il est informé d'une modification, le service désigné par le Roi met à jour la liste des zones géographiques de conservation.

Le dispositif en projet reste toutefois en défaut de définir les critères concrets et techniques à prendre en compte pour définir le périmètre de la zone, de manière telle que les zones relevant d'une même catégorie soient définies selon la même méthodologie [26]. La section de législation n'aperçoit pas non plus quelle autorité sera chargée de la définition du périmètre proprement dit, ou de sa modification. Il est uniquement prévu, à cet égard, que le service désigné par le Roi met à jour la liste des zones, annuellement et « chaque fois qu'il est informé d'une modification », ce qui suppose, s'agissant de la modification de la liste, que le pouvoir de décision revient aux autorités compétentes en la matière concernée par la zone, autorités dont le Roi peut arrêter la liste, sans y être toutefois tenu.

Or, dès lors que la définition des périmètres des zones ainsi que leur inscription sur la liste ou leur retrait de celle-ci, conditionnent l'obligation imposée aux opérateurs de conserver les données y afférentes, l'ensemble de ces décisions doivent être adoptées ou à tout le moins approuvées par une autorité unique, aux fins d'assurer le respect du principe d'égalité, spécialement entre les personnes susceptibles de voir leurs données conservées. Par ailleurs, ces actes constituent des actes à portée générale et abstraite dans leurs effets ; ils sont donc de nature réglementaire et ne peuvent être adoptés que par une autorité responsable politiquement devant le Parlement, à savoir, s'agissant de l'autorité fédérale, le Roi [27-28].

4.2.4. L'article 126/1, § 5, en projet, habilite le Roi, pour les trois catégories de zones prévues à l'article 126/1, § 3, alinéa 1er, 3°, 4° et 5°, en projet, à fixer des « zones additionnelles ».

Les critères qui doivent être en mis en œuvre par le Roi ne sont pas précisés.

[25] La section de législation suppose qu'il s'agit, par exemple, d'hypothèses où des arrondissements judiciaires ou des zones de police ne présenteraient plus lors d'une nouvelle année, le taux de criminalité minimum requis pour être classés comme zone de conservation, ou bien lorsqu'un bâtiment affecté à un usage qui justifie son classement dans une zone de conservation serait affecté à un autre usage qui ne le justifierait plus.

[26] Ainsi, il ne serait pas admissible, à titre d'exemple, que la zone contenant une maison communale, une ambassade ou un hôpital, comporte également les abords directs du bâtiment, alors que la zone contenant un autre maison communale, une autre ambassade ou un autre hôpital se limiterait strictement au bâtiment concerné.

[27] Le cas échéant, à condition que la méthode de calcul ait été préalablement fixée par le législateur ou par le Roi, il pourrait être envisager de charger un ou plusieurs ministres de cette détermination.

[28] Voir, en un sens similaire, l'avis n° 69.160/4 donné le 6 mai 2021.

‡LW-BEHVMBJEH-GJDIBQW‡

Certes, le paragraphe 6 en projet prévoit :

« 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 5, 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 5 répondent toujours aux critères visés au paragraphe 3, alinéa 1er, points 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.

[…] ».

La portée des principes définis par l'alinéa 3 de cette disposition n'apparait toutefois pas clairement.

La section de législation se demande ainsi si ces principes s'appliqueront de manière contraignante au Roi, lors de la mise en œuvre de l'habilitation qui Lui est conférée en vue d'ajouter des types de zones dans les trois catégories précitées, ou s'il s'agit d'une invitation faite au législateur futur, invitation qui, par hypothèse ne saurait le contraindre.

En tout état de cause, le principe de légalité attaché à l'article 22 de la Constitution impose que l'habilitation conférée au Roi soit encadrée de manière suffisante et que, par conséquent, le texte en projet soit rédigé de manière telle que les principes énoncés à l'article 126/1, § 6, alinéa 3, en projet s'imposent à Lui sans ambiguïté.

À cet égard, il ressort des explications communiquées par les délégués du Ministre que, lorsque le Roi mettra en œuvre l'habilitation concernée, Il sera tenu de s'inscrire dans les critères énoncés *in limine* des dispositions qui prévoient les trois catégories de zones concernées. Ainsi, à titre d'exemple, s'il est envisagé d'ajouter une zone à la catégorie prévue au paragraphe 3, alinéa 1er, 5°, en projet, le Roi devra être en mesure de justifier l'ajout au regard de l'existence d' « une menace potentielle grave pour les intérêts des institutions internationales accueillies sur le territoire national ». Ce mécanisme a ainsi vocation à encadrer l'habilitation conférée au Roi.

‡LW-BEHVMBJEH-GJDIBQW‡

4.2.5. Le dernier alinéa du paragraphe 3 de la disposition en projet est rédigé comme suit :

> « La loi du 11 avril 1994 relative à la publicité de l'administration et la loi du 5 aout 2006 relative à l'accès du public à l'information en matière d'environnement ne s'appliquent pas aux informations, documents ou données, sous quelque forme que ce soit, visés au présent article, à l'exception des statistiques de criminalité visées à l'alinéa 1er point 1° ».

4.2.5.1. La disposition en projet rend ainsi inapplicable la loi du 11 avril 1994 'relative à la publicité de l'administration', et ce, de manière extrêmement générale, aux « informations, documents ou données, sous quelque forme que ce soit, visés [à l'article 126/1, en projet] ».

Sur ce point [29], il y a lieu d'avoir égard à l'article 32 de la Constitution qui dispose :

> « Chacun a le droit de consulter chaque document administratif et de s'en faire remettre copie, sauf dans les cas et conditions fixés par la loi, le décret ou la règle visée à l'article 134 ».

Si l'article 32 de la Constitution habilite le législateur concerné à prévoir des cas dans lesquels le droit de consulter chaque document administratif et de s'en faire remettre copie ne s'applique pas, les exceptions ainsi mises en place doivent, dans le respect des principes d'égalité et de non-discrimination, poursuivre un but légitime et demeurer proportionnées au but légitime poursuivi.

La loi du 11 avril 1994, qui organise le régime général d'accès aux documents administratifs, prévoit déjà des exceptions à l'accès à certains documents. Ainsi, l'article 6, § 1er, de cette loi dispose que l'autorité administrative rejette la demande de consultation, d'explication ou de communication sous la forme de copie d'un document administratif si elle a constaté que l'intérêt de la publicité ne l'emporte pas notamment sur la protection de la sécurité de la population ou de l'ordre public, ou encore, la sûreté ou la défense nationales. Cette disposition organise un système de refus au cas par cas de l'accès à un document administratif ou de la communication d'une copie de ce document, sans instituer un régime général d'interdiction à priori d'accès à une catégorie spécifique de documents ou de limitation à priori de l'accès d'un document déterminé à telles catégories de personnes.

Un tel système de décision individuelle à posteriori permet de garantir la protection de la sécurité publique, de l'ordre public, et de la sureté et de la défense nationales.

Un tel régime d'actes à portée individuelle susceptibles de recours, *in fine*, auprès de la section du contentieux administratif du Conseil d'État, est ainsi de nature à garantir la proportionnalité des restrictions apportées au droit d'accès aux documents administratifs.

[29] Pour des observations similaires, voir, *mutatis mutandis*, l'avis n° 69.160/4.

‡LW-BEHVMBJEH-GJDIBQW‡

Pour sa part, le texte en projet restreint de manière radicale le droit à la transparence administrative en ce qui concerne, de manière tout-à-fait générale, tous les « informations, documents ou données, sous quelque forme que ce soit, visés [à l'article 126/1, en projet] ».

Il appartient aux auteurs de l'avant-projet d'être en mesure de démontrer que la différence de traitement qu'institue le dispositif à l'examen entre les personnes qui se trouvent à priori exclues de toute possibilité de prendre connaissance de la liste des zones sensibles, et les personnes qui souhaitent prendre connaissance d'autres documents administratifs sensibles sur le plan de la sécurité publique, de l'ordre public, et de la sûreté et de la défense nationales, auxquelles s'applique le système mis en place par la loi du 11 avril 1994, spécialement son article 6, repose sur une justification objective et raisonnable rendant cette différence de traitement conforme aux principes d'égalité et de non-discrimination [30].

En tout état de cause, il convient que le régime en projet demeure conforme au principe de proportionnalité. À ce propos, l'exclusion du champ d'application de la loi du 11 avril 1994 de tous les « informations, documents ou données, sous quelque forme que ce soit, visés [à l'article 126/1, en projet], à l'exception des statistiques de criminalité visées à l'alinéa 1er point 1°, de l'article » apparait excessive dans la généralité de ses termes. Il conviendrait ainsi de limiter l'exclusion envisagée aux catégories d'informations, documents ou données pour lesquelles le régime dérogatoire se justifie effectivement.

4.2.5.2. Dans la mesure où elle entend déroger à la loi du 5 aout 2006 'relative à l'accès du public à l'information en matière d'environnement', la disposition en projet appellerait en principe, *mutatis mutandis*, les mêmes observations que celles formulées au point précédent.

Toutefois, il convient de ne pas perdre de vue que cette loi a pour objet la transposition de la directive 2003/4/CE du Parlement européen et du Conseil du 28 janvier 2003 'concernant l'accès du public à l'information en matière d'environnement et abrogeant la directive 90/313/CEE du Conseil'.

Au regard du système organisé par les articles 3 et 4 de la directive, qui ne s'applique certes qu'aux informations environnementales, telles que définies en son article 2, 1°, seules des dérogations au cas par cas à l'obligation de communication, sont admissibles. Ces dérogations peuvent reposer notamment sur la nécessité de garantir la sécurité publique ou la défense nationale [31], mais aucun régime général d'exclusion à priori ne peut être organisé.

La disposition à l'examen ne peut dès lors être admise dans la mesure où elle prévoit que la loi du 5 aout 2006 est inapplicable aux informations, documents et données concernées qui constituent des informations environnementales au sens de la directive.

4.2.5.3. La disposition à l'examen sera revue à la lumière des observations qui précèdent.

[30] Voir C.C., 19 décembre 2013, n° 169/2013.

[31] Article 4, paragraphe 2, de la directive.

‡LW-BEHVMBJEH-GJDIBQW‡

4.3.1. Comme mentionné ci-avant, la disposition en projet prévoit :

> « Chaque autorité compétente dans l'une des matières visées aux paragraphe 3, alinéa 1er, 1° à 5°, transmet chaque année à la date déterminée par le Roi et au service désigné par le Roi, les informations nécessaires à la détermination concrète des zones géographiques ».

Par ailleurs, ces autorités sont tenues d'informer sans délai 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 au paragraphe 1er dans cette zone ».

Enfin le Roi peut – sans donc y être tenu – établir la liste des différentes autorités concernées.

Dans la mesure où l'objet de zones de conservation relèverait de matières qui sont de la compétences des Communautés et des Régions [32], cette disposition présente une difficulté : elle impose de manière unilatérale des obligations à ces niveaux de pouvoir, qui sont soumis ainsi à ces obligations, non pas uniquement au titre d'une matière qui relève de la compétence fédérale, mais précisément, en raison de leurs compétences propres dans leurs matières [33-34].

Un mécanisme de collaboration qui implique l'intervention des Communautés et des Régions, ou d'organes relevant de celles-ci, en raison de leurs compétences propres, doit faire l'objet d'une coopération au sens de l'article 92*bis*, de la loi spéciale du 8 aout 1980 'de réformes institutionnelles'. Un autre biais pourrait consister à créer un organe de décision ou consultatif au sein duquel les Communautés et les Régions seraient représentées, conformément à l'article 92*ter* de la même loi spéciale.

À ce propos, s'il est vrai que dans la matière des communications électroniques, la Cour constitutionnelle et la section de législation ont déjà admis que d'autres formes de coopération, tel un accord du comité de concertation sur la législation concernée, pouvaient être admises, ce n'est que dans la mesure où, compte tenu des compétences résiduelles de l'autorité fédérale en matière de communications électroniques et des compétences d'attribution des Communautés en matière d'aspects de contenu et techniques des services de médias audiovisuels et sonores, il convenait que les infrastructures concernées soient « réglées en coopération entre l'État fédéral et les Communautés, afin de faire en sorte que ces autorités harmonisent leurs

[32] À titre d'exemple, il en va ainsi, fût-ce en partie, des ports, aéroports, stations de métro et pré-métro, communes, et conseils provinciaux et des hôpitaux.

[33] Ainsi, le mécanisme prévu par la disposition en projet ne peut être comparé, par exemple, à la situation dans laquelle se trouve l'administration d'une Communauté ou d'une Région, qui est tenue au respect de la législation fédérale en matière de bien-être au travail, ce en sa qualité d'employeur.

[34] *Mutatis mutandis*, dans son avis n° 37.295/4 donné le 28 juin 2004 sur un avant-projet devenu la loi du 13 juin 2005 'relative aux communications électroniques', http://www.raadvst-consetat.be/dbx/avis/37295.pdf, la section de législation a observé :
« L'autonomie respective des communautés et des régions s'oppose en effet à ce que l'État fédéral ou une entité fédérée décide unilatéralement d'associer les autorités d'autres entités fédérale ou fédérées à l'exercice de ses propres compétences. Seule une loi adoptée à la majorité spéciale ou un accord de coopération pourrait imposer une telle concertation ».

‡LW-BEHVMBJEH-GJDIBQW‡

normes respectives et pour éviter que cette infrastructure et ces services soient soumis à des dispositions contradictoires » [35-36].

Tel n'est pas le cas de l'avant-projet à l'examen : il ne s'agit pas d'éviter des contradictions entre deux législations relevant chacune de la compétence de niveaux de pouvoir différents, mais, le cas échéant, pour l'autorité fédérale d'imposer, au titre de ses compétences propres, des obligations à d'autres niveaux de pouvoir, en raison de leurs compétences propres.

Par conséquent, il ne peut être garanti que l'accord du Comité de concertation sur le texte en projet s'avère suffisant, en l'espèce, au titre de mécanisme de coopération.

En tout état de cause, il ressort du dossier communiqué à la section de législation que, concernant l'avant-projet à l'examen, la concertation organisée a eu lieu sur la base de l'accord de coopération du 17 novembre 2006 entre l'État fédéral, la Communauté flamande, la Communauté française et la Communauté germanophone 'relatif à la consultation mutuelle lors de l'élaboration d'une législation en matière de réseaux de communications électroniques, lors de l'échange d'informations et lors de l'exercice des compétences en matière de réseaux de communications électroniques par les autorités de régulation en charge des télécommunications ou de la radiodiffusion et la télévision'. Les Régions n'ont dès lors pas participé à celle-ci.

5. Quant à la durée de conservation, l'article 126/1, § 1er, en projet, prévoit que les données visées au paragraphe 2 doivent être conservées pendant douze mois à partir de la communication, sauf si une autre durée est fixée dans le même article.

Les autres durées prévues à l'article 126/1, en projet, sont à l'exception de celles prévues au paragraphe 3, 1°, alinéa 2, c), et alinéa 3, c), toutes inférieures à douze mois. Il s'agit des durées de six et, neuf mois prévues au paragraphe 3, 1°, alinéa 2, a) et b), et alinéa 3, a) et b),en fonction du taux de criminalité décelé dans la zone concernée.

Il n'apparait pas, à priori, que ces durées de conservation poseraient des difficultés particulières, d'autant que celles prévues au paragraphe 3, 1°, alinéas 2 et 3, précité entendent garantir la proportionnalité de la conservation au regard de l'importance de la criminalité dans l'arrondissement judiciaire ou la zone de police considérés.

6.1. La dernière condition mise à l'opération de conservation ici envisagée, selon l'enseignement de l'arrêt *La Quadrature du Net*, réside dans le caractère temporellement limité au strict nécessaire, de l'opération.

---

[35] C.C. , 8 novembre 2006, n° 163/2006, B.4 ; voir également C.C. , 14 juillet 2004, n° 132/2004, B.6.1., rédigé en ces termes :
« Sur la base de l'article 92*bis* de la loi spéciale du 8 aout 1980 de réformes institutionnelles, l'État, les communautés et les régions peuvent conclure des accords de coopération qui portent notamment sur la création et la gestion conjointes de services et institutions communs, sur l'exercice conjoint de compétences propres, ou sur le développement d'initiatives en commun. Ils disposent en outre d'autres instruments en vue de donner forme à leur coopération ».

[36] Voir spécialement l'avis n° 42.495/4 le 19 mars 2007 sur un avant-projet devenu le décret de la Communauté française du 2 juillet 2007 'remplaçant les articles 81 à 83 et 90 à 98 du décret du 27 février 2003 sur la radiodiffusion', annulés par la Cour constitutionnelle le 8 novembre 2006, http://www.raadvst-consetat.be/dbx/avis/42495.pdf.

‡LW-BEHVMBJEH-GJDIBQW‡

Le point 151 de l'arrêt exprime plus clairement cette exigence en ces termes :

> « 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 ».

Semble ainsi visée non pas tant la durée de conservation des données, que la durée de la période au cours de laquelle les données doivent être stockées en vue de leur conservation [37].

6.2. Dans le système mis en place par l'article 126/1 en projet, il n'est pas prévu de limiter les opérations de conservation dans les différentes zones envisagées, moyennant une éventuelle prolongation.

La raison en est que la plupart des zones retenues se fondent sur la présence de bâtiments ou installations affectés à certaines fonctions dont les auteurs de l'avant-projet considèrent qu'ils présentent, en raison de la nature-même de ces fonctions, un risque spécifique au regard des objectifs poursuivis. En d'autres termes, dans l'intention des auteurs de l'avant-projet, aussi longtemps que les bâtiments et installations sont affectés à ces fonctions, la nécessité de la conservation des données se justifie. Le même raisonnement vaut pour les zones définies en fonction du niveau de menace, où les auteurs de l'avant-projet considèrent la conservation nécessaire aussi longtemps que la menace est au minimum de niveau 3. Il en va de même pour les zones définies en fonction du taux de criminalité, aussi longtemps que le taux est atteint.

Par ailleurs, aux fins de limiter les opérations de conservation au strict nécessaire, chaque autorité compétente pour la matière concernée par la zone est tenue d'informer sans délai le service désigné par le Roi de ce que la zone concernée ne répond plus au critère qui classe celle-ci dans les zones de conservation. Ce service est en outre chargé d'actualiser la liste des zones chaque année et chaque fois qu'il est informé d'une modification par l'une des autorités compétentes. Enfin, un rapport annuel est présenté à la Chambre des représentants, qui examine en particulier si les catégories de zones géographiques énumérées dans la loi ou l'arrêté visé au paragraphe 5 de la disposition en projet répondent toujours aux critères en lien avec les objectifs poursuivis et s'il est nécessaire de les maintenir ou si d'autres zones doivent être incluses.

Ces mécanismes visent à garantir qu'aucun périmètre initialement soumis au régime de l'article 126/1 en projet n'y sera maintenu que dans la mesure de ce qui est strictement nécessaire aux finalités concernées.

Si la section de législation comprend la logique du système mis en place, il ne peut toutefois être garanti que celui-ci répond intégralement à la condition exprimée au point 151 de l'arrêt *La Quadrature du Net*.

[37] Comparer avec l'article 39*quinquies*, en projet, du Code d'instruction criminelle (article 17 de l'avant-projet).

‡LW-BEHVMBJEH-GJDIBQW‡

Ainsi, ce point laisse à penser qu'il est attendu que le mécanisme repose sur une limitation temporelle à priori, moyennant renouvellement éventuel, tandis que le mécanisme en projet se fonde lui sur une opération durable, non limitée dans le temps, à laquelle il est mis fin, en principe, dès que la nécessité ne la justifie plus.

7.1. Enfin, la disposition à l'examen appelle des observations plus ponctuelles.

7.2. Certaines des zones énumérées se concilient difficilement avec cette notion, qui implique la détermination d'un périmètre géographique. Il en va ainsi du réseau utilisé par ASTRID, et des réseaux et systèmes d'information qui soutiennent la fourniture des services essentiels des opérateurs de services essentiels, visés à l'article 126/1, § 3, 3°, o) et p), en projet.

Le texte en projet gagnerait à être complété aux fins de mieux cerner la définition géographique de ces réseaux.

De même, les zones « dont le niveau de la menace, déterminé en vertu de la loi du 10 juillet 2006 relative à l'analyse de la menace est au moins de niveau 3, et aussi longtemps qu'un niveau d'au moins 3 perdure pour ces zones » sont délicates à déterminer. En effet, selon l'article 11, § 6, de l'arrêté royal du 28 novembre 2006, le niveau de menace est déterminé au regard d'une personne, d'un groupement, ou d'un événement : dès lors qu'elle concerne une personne ou un groupement limité, la définition du niveau de menace ne se prête pas nécessairement à une localisation géographique. La section de législation suppose dès lors que le système en projet ne concerne que les cas où la menace est localisable au sein d'une aire géographique, ce que le texte en projet devrait prévoit expressément.

7.3. Les bâtiments affectés aux institutions visées aux chapitres 5 à 7 du titre III de la Constitution, les communes dans lesquelles se trouvent les domaines militaires et les bâtiments affectés à la police fédérale ou à la police locale sont repris au titre de zones de conservation, d'une part, au paragraphe 3, 3°, respectivement e), h) et f), en projet, comme zones « particulièrement exposées à des menaces pour la sécurité nationale ou à des risques élevés de criminalité grave ») et, d'autre part, au 4°, d), respectivement vi), vii) et viii), en projet, « pour ce qui concerne la souveraineté nationale et les institutions établies par la Constitution et les lois, décrets ou les ordonnances ».

La section de législation n'aperçoit pas la logique et l'utilité qu'il y a à inclure ces types de zones dans deux catégories différentes, ce qui prête par ailleurs à confusion. La question se pose de savoir si ce doublon ne trouve pas sa cause dans une erreur.

7.4. La disposition en projet n'envisage pas et ne règle pas la situation, qui ne saurait être exclue, dans laquelle, en raison des matières pour lesquelles elles sont compétentes, plusieurs autorités au sens des paragraphes 3 et 5, de la disposition en projet, seraient compétentes pour un même type de zone.

‡LW-BEHVMBJEH-GJDIBQW‡

7.5. Dans la catégorie des zones où il y a une menace grave potentielle pour les intérêts vitaux du pays ou pour les besoins essentiels de la population, figurent « 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 de la Défense et approuvée par le Conseil national de sécurité ».

Selon le commentaire de l'article, ce type de zone renvoie en réalité, d'une part, aux missions du service de la Sûreté de l'État, qui, selon l'article 7, 1°, de la loi du 30 novembre 1998, a pour mission, notamment

> « de rechercher, d'analyser et de traiter le renseignement relatif à toute activité qui menace […] le potentiel scientifique ou économique défini par le Conseil national de sécurité, ou tout autre intérêt fondamental du pays défini par le Roi sur proposition du Conseil national de sécurité ».

D'autre part, il est renvoyé à l'article 11, § 1er, 1°, c), de la même loi, qui confie au Service Général du Renseignement et de la Sécurité notamment la mission de rechercher, d'analyser et de traiter le renseignement relatif à toute activité qui menace ou pourrait menacer

> « le potentiel scientifique et économique en rapport avec les acteurs, tant personnes physiques que personnes morales, qui sont actifs dans les secteurs économiques et industriels liés à la défense et qui figurent sur une liste approuvée par le Conseil national de sécurité, sur proposition du ministre de la Justice et du ministre de la Défense ».

Au regard de cette précision, la section de législation constate que la disposition à l'examen mentionne 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 de la Défense et approuvée par le Conseil national de sécurité ». S'agissant de l'atteinte au potentiel économique et scientifique, l'article 7, 1°, de la loi du 30 novembre 1998, qui a trait à la Sûreté de l'État, ne prévoit pas l'établissement d'une telle liste par ce service, tandis que l'article 11, § 1er, 1°, c), de la même loi, prévoit que le Service Général du Renseignement et de la Sécurité établira, lui, une liste, dans des conditions similaires à celles prévues par la disposition à l'examen, mais qui ne visent que les secteurs économiques et industriels liés à la Défense.

Aux fins d'éviter l'élaboration de plusieurs listes, qui le cas échéant, pourraient comporter des doublons ou se contredire, il appartient aux auteurs de l'avant-projet de revoir l'ensemble des dispositions précitées aux fins d'assurer la cohérence entre celles-ci, dans la mesure où elles concernent la protection du potentiel économique et scientifique sur le territoire national et l'élaboration de liste(s) y relative(s).

7.6. L'article 126/1, § 3, en projet, mentionne, à de multiples reprises, « les infractions visées à l'article 90*ter*, du Code d'instruction criminelle ». Dans un souci de transparence et de sécurité juridique, il s'indiquerait de renvoyer de manière plus précise à celles des subdivisions de l'article concerné qui mentionnent les infractions dont question.

8. En conclusion, l'article 126/1 en projet sera réexaminé et revu à la lumière des observations qui précèdent.

‡LW-BEHVMBJEH-GJDIBQW‡

La conservation généralisée et indifférenciée des adresses IP attribuées à la source 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

1. L'article 7 de l'avant-projet entend remplacer la totalité de l'article 126 de la loi du 13 juin 2005, de sorte qu'il disposerait comme suit :

« § 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 de souscription de l'abonné ainsi que les données techniques qui sont nécessaires pour identifier l'utilisateur final, l'équipement terminal ou le service de communications électroniques employé, à l'exception des données qui sont liées à une seule communication électronique, pour autant qu'ils traitent ou génèrent ces données dans le cadre de la fourniture des réseaux ou services de communications concernés.

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

Ces données sont conservées pour les autorités et les finalités visées à l'article 127/1.

Les données visées au présent article sont conservées à partir de la date d'activation du service jusqu'à douze mois après la date à partir de laquelle une communication est possible pour la dernière fois à l'aide du service utilisé.

Par dérogation à l'alinéa 3, les adresses IP dynamiques, autres que celle qui a été utilisée pour souscrire au service, sont conservées jusqu'à douze mois après la fin de la session.

§ 2. Le Roi fixe après avis des Autorités de protection des données compétentes et de l'Institut, les données à conserver ainsi que les exigences auxquelles ces données doivent répondre ».

Le commentaire de l'article justifie cette disposition comme suit :

« Pour mettre en œuvre l'arrêt de la Cour constitutionnelle du 22 avril 2021 et l'arrêt Quadrature du Net de la Cour de Justice de l'Union européenne, ne sont plus visées par l'obligation de conservation que les données de souscription et les données techniques qui sont nécessaires pour identifier l'utilisateur final, l'équipement terminal ou le service de communications électroniques employé, à l'exception des données qui sont liées à une seule communication électronique (tels que l'identifiant créé pour chaque communication). Le présent article est applicable lorsqu'un service de communications électroniques est fourni en Belgique.

La durée de conservation de 12 mois a été maintenue, dès lors que cette durée correspond à la durée de conservation strictement nécessaire pour permettre aux autorités de mener à bien leurs enquêtes, en particulier en matière de lutte contre la criminalité grave.

Une distinction est effectuée entre l'adresse IP utilisée pour souscrire au service et les autres adresses IP. En effet, l'adresse IP utilisée pour souscrire au service est une donnée qui doit être conservée par l'opérateur dans le cadre de l'article 127, afin de pouvoir établir ou vérifier l'identité de l'abonné.

‡LW-BEHVMBJEH-GJDIBQW‡

Les données de souscription comprennent entre autres le numéro de téléphone, l'adresse email, le numéro d'abonné, la date de début et de fin de la souscription. Le Conseil d'État français, qui a été amené à examiner la législation française en matière de conservation de données de trafic pour les autorités (arrêt du 21/04/2021 n^{os} 393099, 394922, 397844, 397851, 424717, 424718, FRENCH DATA NETWORK et autres), a considéré à cet égard ce qui suit : « il résulte clairement de la directive du 12 juillet 2002 et du RGPD qu'ils ne s'opposent pas à une obligation de conservation généralisée et indifférenciée, pour une durée d'un an, des informations autres que celles relatives à l'identité civile fournies lors de la souscription d'un contrat par un utilisateur ou lors de la création d'un compte, d'une part, et des données relatives aux paiements, d'autre part, mentionnées respectivement aux 3° et 4°, de l'article 1er du décret du 25 février 2011 (point 36)

Les identifiants techniques qui ne sont pas rattachés à une communication déterminée mais qui servent principalement à identifier l'utilisateur final, l'équipement terminal ou le service de communications électroniques employé comprennent entre autres l'adresse IP source, l'IMEI (*International Mobile Equipment Identity*), l'IMSI (International Mobile Subscriber Identity), l'ICCID (*Integrated Circuit Card Identifier*), l'adresse MAC, le MSISDN (*Mobile Station Integrated Services Digital Network*), ou d'autres identifiants qui seront développés dans le cadre de la 5G ou en fonction de l'évolution des technologies employées. À ce jour, la Cour de justice de l'Union européenne ne s'est prononcée que sur l'adresse IP source mais pas sur les autres données techniques précitées, dont la conservation est également nécessaire à des fins d'identification.

Les données nécessaires pour identifier l'utilisateur final, l'équipement ou le service de communications électroniques peuvent inclure des données de trafic. A titre d'exemple, la conservation de certaines données de trafic sera nécessaire pour relier l'adresse IP à une personne spécifique ou pour retrouver le numéro de téléphone utilisé ou le numéro MSISDN (« *Mobile Subscriber Integrated Services Digital Network* », à savoir le numéro de téléphone avec le préfixe international) servi.

Comme l'indique la Cour de Justice dans son arrêt *Quadrature du Net* du 6/10/2020, l'adresse IP source est le seul moyen susceptible de permettre l'identification de l'auteur d'une infraction en ligne (point 154 de l'arrêt).

Dans l'arrêt de la Cour de Justice *Ministerio Fiscal* (C-207/16, point 20), a été considérée comme ne constituant pas une ingérence grave aux droits fondamentaux (vie privée et protection des données à caractère personnel), la demande de la police judiciaire, pour les besoins d'une enquête pénale, de se voir transmettre les numéros de téléphone activés, pendant une période de douze jours, avec le code relatif à l'identité internationale d'équipement mobile (ci-après le « code IMEI ») du téléphone mobile volé ainsi que les données à caractère personnel relatives à l'identité civile des titulaires ou des utilisateurs des numéros de téléphone correspondant aux cartes SIM activées avec ce code.

Au vu de l'utilité que représentent ces données techniques afin de permettre l'identification d'auteurs d'infractions en ligne ou hors ligne, la mesure de conservation prévue est proportionnée » [38].

2. L'article 126 en projet, doit être mis en rapport avec l'arrêt *La Quadrature du Net*, ainsi qu'avec l'arrêt n° 57/2021 de la Cour constitutionnelle.

[38] Exposé des motifs, pp 30-32.

‡LW-BEHVMBJEH-GJDIBQW‡

Pour rappel, dans le dispositif de son arrêt *La Quadrature du Net*, la Cour de Justice a dit en effet 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 des droits fondamentaux de l'Union européenne, ne s'oppose 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 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,

[…] ».

La Cour de Justice opère ainsi une distinction entre :

– d'une part, la conservation généralisée et indifférenciée des adresse IP attribuées à une source de connexion, laquelle peut être imposée aux opérateurs par la législation uniquement aux fins de 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, laquelle peut être imposée aux opérateurs par la législation 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 temporelle limitée au strict nécessaire ».

3. La disposition à l'examen vise quant à elle :

– les données de souscription de l'abonné, qui ne sont pas définies, mais à propos desquelles le commentaire de l'article précise qu'elles « comprennent entre autres le numéro de téléphone, l'adresse email, le numéro d'abonné, la date de début et de fin de la souscription », et

– les données qui sont nécessaires pour identifier l'utilisateur final, l'équipement terminal ou le service de communications électroniques employé, qui, elles non plus, ne sont pas définies mais dont le commentaire de l'article mentionne qu'elles « comprennent entre autres l'adresse IP source, l'IMEI (*International Mobile Equipment Identity*), l'IMSI *(International Mobile Subscriber Identity*), l'ICCID (*Integrated Circuit Card Identifier*), l'adresse MAC, le MSISDN (*Mobile Station Integrated Services Digital Network*), ou d'autres identifiants qui seront développés dans le cadre de la 5G ou en fonction de l'évolution des technologies employées ».

‡LW-BEHVMBJEH-GJDIBQW‡

S'agissant des données visées par la disposition en projet qui ne constitueraient pas des données uniquement relatives à « l'identité civile des utilisateurs de moyens de communications électroniques » mais sont des adresses IP source, ou des données dont la conservation est susceptible d'entrainer des risques similaires à ceux que présentent la conservation et l'accès à des données IP source [39], il y a lieu de constater que rien, dans la disposition en projet, ne limite la conservation de ces données à des fins de sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique.

Certes, l'article 126, § 1er, alinéa 3, en projet, prévoit-il que « ces données sont conservées pour les autorités et les finalités visées à l'article 127/1 ». Cependant, dans l'article 127/1, en projet, s'agissant spécialement des 1° et 2° de son paragraphe 1er, les finalités sont exprimées de manière générale et ne sont pas limitées à « la sauvegarde de la sécurité nationale, la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique ».

4. Il en résulte que le système mis en place par l'article 126 en projet, combiné avec l'article 127/1 en projet n'est pas de nature à garantir le respect de l'article 15, paragraphe 1, de la directive 2002/58/CE, lu à la lumière de l'enseignement de l'arrêt *La Quadrature du Net*, en ce qui concerne la conservation générale et non différenciée des adresses IP source, et par analogie, de toutes les données assimilables, dont la conservation présente des risques similaires à ceux qui sont attachés à la conservation des adresses IP source, tels que relevés par la Cour de Justice.

Le dispositif en projet sera revu et complété à la lumière de cette observation.

5. Enfin, la disposition à l'examen prévoit que les données qu'elle vise sont conservées « à partir de la date d'activation du service jusqu'à douze mois après la date à partir de laquelle une communication est possible pour la dernière fois à l'aide du service utilisé ». Pour les adresses IP dynamiques, autres que celles qui sont utilisées pour souscrire au service, il est prévu qu'elles sont conservées jusqu'à douze mois après la fin de la session.

De tels délais peuvent paraitre relativement longs au regard des exigences résultant de l'enseignement de l'arrêt *La quadrature du Net*.

[39] Dans son arrêt *La Quadrature du Net*, la Cour de Justice a relevé, à propos des adresses IP source, ce qui suit :
« 152. Il y a lieu de relever que les adresses IP, quoique faisant partie des données relatives au trafic, sont générées sans être rattachées à une communication déterminée et servent principalement à identifier, par l'intermédiaire des fournisseurs de services de communications électroniques, la personne physique propriétaire d'un équipement terminal à partir duquel une communication au moyen de l'Internet est effectuée. Ainsi, en matière de courrier électronique ainsi que 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. Cette catégorie de données présente donc un degré de sensibilité moindre que les autres données relatives au trafic.
153.Toutefois, les adresses IP pouvant 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 desdites adresses IP que nécessite un tel traçage constituent des ingérences graves dans les droits fondamentaux de l'internaute consacrés aux articles 7 et 8 de la Charte, pouvant avoir des effets dissuasifs tels que ceux visés au point 118 du présent arrêt ». C'est la gravité de l'ingérence ainsi considérée qui a amené la Cour de Justice à réserver à cette catégorie de données un traitement plus sévère que celui réservé aux données relatives à l'identité civile des utilisateurs.

‡LW-BEHVMBJEH-GJDIBQW‡

Le commentaire de l'article précise à ce propos :

« La durée de conservation de 12 mois a été maintenue, dès lors que cette durée correspond à la durée de conservation strictement nécessaire pour permettre aux autorités de mener à bien leurs enquêtes, en particulier en matière de lutte contre la criminalité grave ».

Cette justification revêt un caractère très général, et relève de l'affirmation de principe.

Les auteurs de l'avant-projet doivent être en mesure de mieux justifier les délais retenus, ce sur la base d'éléments concrets et probants.

La disposition à l'examen sera réexaminée à la lumière de cette observation.

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

1. Selon l'enseignement de l'arrêt *La Quadrature du Net*, est admissible une législation permettant 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.

L'article 9 de l'avant-projet, qui entend remplacer l'article 127 de la loi du 13 juin 2005 vise à organiser une conservation ayant cet objet.

Au regard des exigences de droit international et européen rappelées ci-avant, sur le principe, cette disposition ne parait pas poser de difficulté.

Il n'en demeure pas moins que l'autorisation générale, donnée aux opérateurs par l'article 127, § 2, alinéa 2, en projet, de « réaliser, de manière automatique, une comparaison entre les paramètres biométriques sur la photo de la pièce d'identité de l'abonné et ceux du visage » peut paraitre disproportionnée par rapport à l'objectif poursuivi, compte tenu, spécialement, de ce que ces données pourraient être recueillies auprès de tous les abonnés personnes physiques, généralement quelconques, de tous les opérateurs, sans même que cette possibilité soit encadrée par le législateur et limitée à des cas spécifiques rendant la mesure nécessaire.

Interrogés sur ce point, les délégués du Ministre ont toutefois expliqué que l'opération de comparaison biométrique envisagée interviendrait uniquement le temps nécessaire pour identifier la personne et n'impliquerait aucun stockage ni conservation subséquente de données. Dans ce contexte, la mesure envisagée ne parait pas disproportionnée.

‡LW-BEHVMBJEH-GJDIBQW‡

Dans un autre ordre d'idées, et très subsidiairement, la section de législation n'aperçoit pas comment l'article 127, § 2, alinéa 2, en projet, est supposé s'articuler avec l'habilitation conférée au Roi par l'article 127, § 3, alinéa 1er, 1° et 2°, en projet, qui permet à Celui-ci de « déterminer si l'opérateur doit lui-même identifier ses abonnés ou s'il peut seulement rendre cette identification possible » et de « déterminer les méthodes d'identification que les opérateurs peuvent utiliser, y compris soumettre une méthode d'identification proposée par un opérateur à une autorisation préalable du ministre [en charge des communications électroniques] et du ministre de la Justice ».

L'article 9 de l'avant-projet sera revu à la lumière de ces observations.

Le recours à une injonction faite aux fournisseurs de services de communications électroniques, 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 aux fins de la lutte contre la criminalité grave et, à fortiori, de la sauvegarde de la sécurité nationale

1. Pour rappel, il résulte de l'arrêt *La Quadrature du Net* qu'aux fins de la lutte contre la criminalité grave et, à fortiori, de la sauvegarde de la sécurité nationale, est admissible une législation qui permet qu'une injonction soit donnée 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.

2.1. L'article 32 de l'avant-projet entend insérer un paragraphe 1er*bis*/1 dans l'article 84 de la loi du 2 aout 2002 'relative à la surveillance du secteur financier et aux services financiers', rédigé comme suit :

> « Dans le cas d'infractions aux articles 14 ou 15 du Règlement 596/2014 ou aux dispositions prises sur la base ou en exécution de ces articles, l'auditeur ou, en son absence, l'auditeur adjoint peut ordonner aux acteurs visés au paragraphe 1er, alinéa 2, de conserver les données visées au paragraphe 1er, alinéa 1er, qui risquent d'être supprimées ou rendues anonymes, jusqu'à ce qu'il ait obtenu d'un juge d'instruction l'autorisation de requérir la communication de ces données.
>
> Les paragraphes 1er, alinéas 4 et 5, et 3 s'appliquent par analogie à l'ordre visé à l'alinéa 1er.
>
> 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.
>
> L'auditeur ou, en son absence, l'auditeur adjoint fait part au juge d'instruction de l'ordre visé à l'alinéa 1er au moment où il lui adresse sa demande d'autorisation préalable pour requérir la communication des données visées au paragraphe 1er, alinéa 1er. Si le juge d'instruction refuse de donner l'autorisation de requérir la communication des données sur lesquelles porte l'ordre ou s'il estime que l'ordre n'était pas légitime ou pas justifié, cet ordre s'éteint ».

‡LW-BEHVMBJEH-GJDIBQW‡

2.2.1. Eu égard à l'enseignement de l'arrêt *La Quadrature du Net*, cette disposition appelle deux observations.

2.2.2. Tout d'abord se pose la question de savoir si l'opération de « *quick freeze* » ainsi autorisée se limite bien à des faits qui relèvent de « la lutte contre la criminalité grave et, à fortiori, de la sauvegarde de la sécurité nationale ».

À ce propos, le commentaire de l'article mentionne ce qui suit :

> « Cette possibilité de quick freeze n'est en outre prévue que pour les violations de l'interdiction d'abus de marché (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)), qui constituent une infraction grave. Leur impact sur l'intégrité des marchés financiers et sur la confiance des investisseurs est en effet important. Il s'agit, au sein du secteur financier, de l'une des infractions les plus graves, comme en témoignent notamment le fait que le règlement relatif aux abus de marché exige pour ces infractions des amendes maximales d'un montant minimum considérablement plus élevé que pour les infractions aux autres dispositions du règlement et à la plupart des autres législations financières européennes, ainsi que le fait que la directive 2014/57/UE du Parlement européen et du Conseil du 16 avril 2014 relative aux sanctions pénales applicables aux abus de marché impose aux États membres de prévoir également des sanctions pénales pour les abus de marché (disposition transposée dans les articles 39 et 40 de la loi du 2 aout 2002). Dans le cadre des enquêtes généralement longues et complexes qui concernent les abus de marché, les données de communications électroniques jouent souvent un rôle important dans l'administration de la preuve, par exemple pour constater que des personnes ont, à un moment donné, été en contact l'une avec l'autre et qu'il existe une relation entre deux ou plusieurs personnes ».

Certes, le règlement 596/2014, prévoit, en son article 30, à l'égard des manquements à ses articles 14 et 15, des sanctions qui apparaissent lourdes, dans l'absolu, et en tout cas plus lourdes que celles prévues pour d'autres infractions.

Ainsi, pour les personnes physiques, en son article 30, paragraphe 2, ce règlement impose aux États membres de faire en sorte que les autorités compétentes puissent imposer une sanction administrative pécuniaire d'un montant maximal d'au moins 5 000 000 EUR.

Pour les personnes morales, ce montant maximal est d'au moins 15 000 000 EUR ou 15 % du chiffre d'affaires annuel total de la personne morale tel qu'il ressort des derniers comptes disponibles approuvés par l'organe de direction de l'entreprise.

Il reste toutefois que ces sanctions constituent, selon le règlement lui-même, des sanctions pécuniaires administratives, et non pénales.

Par ailleurs, le règlement ne fixe pas de montant minimum pour ces sanctions, mais uniquement le plancher du montant maximum de la sanction.

‡LW-BEHVMBJEH-GJDIBQW‡

Quant aux articles 39 et 40 de la loi du 2 aout 2002, auxquels renvoie le commentaire de l'article, les sanctions pénales minimales qu'ils prévoient sont respectivement :

– pour l'article 39, § 1er : un emprisonnement d'un mois et une amende de 300 euros ;

– pour l'article 40, § 6 : un emprisonnement de trois mois et une amende de 50 euros.

Dans ces contextes, il parait difficile de considérer que, dans l'absolu, toutes les infractions couvertes par ces différentes dispositions participent, par nature, de la notion de « criminalité grave » [40].

Si la section de législation comprend la logique des justifications invoquées dans le commentaire des articles, il convient, aux fins d'assurer la conformité du dispositif en projet avec les principes dégagés par l'arrêt *La Quadrature du Net*, de limiter le pouvoir d'injonction envisagé aux faits dont le caractère de gravité est établi ou peut être présumé sur la base des éléments dont dispose l'auditeur ou l'auditeur adjoint.

2.2.3. Par ailleurs, le mécanisme en projet gagnerait à être complété aux fins de prévoir que la demande d'accès aux données formée auprès du juge d'instruction doit être concomitante à l'injonction de « *quick freeze* » adressée à ou aux opérateurs concernés, ou, à tout le moins, intervenir sans délai en suite de cette dernière.

Une telle simultanéité ou quasi simultanéité est en effet de nature à mieux garantir un contrôle juridictionnel effectif, comme requis par le droit européen.

2.2.4. L'article 32 de l'avant-projet sera revu à la lumière de ces observations.

3. L'article 24 de l'avant-projet envisage d'insérer un article 16/2/1, dans la loi du 30 novembre 1998.

Outre les observations particulières qu'appelle cette disposition compte tenu des ambiguïtés, imprécisions et autres difficultés dont elle est entachée, et qui sont abordées dans les observations particulières ci-après, la section de législation s'interroge sur la manière dont il sera satisfait à l'exigence de contrôle juridictionnel effectif, qui résulte de l'enseignement de l'arrêt *La Quadrature du Net*.

L'article 24 sera réexaminé à la lumière de cette observation.

[40] Comparer sur ce point avec l'article 39*quinquies*, en projet, du Code d'instruction criminel (article 17 de l'avant-projet) qui visent des infractions qui « peuvent donner lieu à un emprisonnement correctionnel principal d'un an ou à une peine plus lourde ».

‡LW-BEHVMBJEH-GJDIBQW‡

OBSERVATIONS PARTICULIÈRES

ARRÊTÉ DE PRÉSENTATION

L'arrêté de présentation sera rédigé comme suit :

« Philippe I^er^, Roi des Belges,

À tous, présents et à venir, Salut.

Sur la proposition du Ministre de la Ministre des Télécommunications, du Ministre de la Justice et de la Ministre de la Défense,

NOUS AVONS ARRÊTÉ ET ARRÊTONS :

La Ministre des Télécommunications, le Ministre de la Justice et la Ministre de la Défense sont chargés de présenter en Notre nom aux Chambres législatives et de déposer à la Chambre des représentants le projet de loi dont la teneur suit : » [41].

DISPOSITIF

Article 4

1. Le paragraphe 4, alinéa 3, en projet, de l'article 122 de la loi du 13 juin 2005 prévoit que les opérateurs sont tenus de conserver les données de localisation et les autres données de trafic nécessaires aux fins de détecter et d'analyser une fraude présumée ou une utilisation malveillante présumée d'un réseau de communications, au minimum quatre mois.

Le commentaire de l'article mentionne à ce propos que :

« Le délai de quatre mois a été retenu pour l'application de l'alinéa 3, étant donné que la fraude peut avoir un impact sur la facturation de l'opérateur envers l'abonné (ou d'une entreprise envers l'abonné).

Le délai minimal de quatre mois de conservation tient compte d'un cycle complet de facturation (premier mois suivant la consommation du service), d'une durée de contestation minimale (de 15 jours à 1 mois, le deuxième mois suivant la consommation du service), d'une période de traitement de la contestation permettant un échange entre l'abonné et l'opérateur (le troisième mois suivant la contestation du service) et d'une période de retard possible dans ce traitement (le quatrième mois suivant la consommation).

Le délai de 4 mois permettra aussi de prendre en compte les évolutions en matière de fraude ».

[41] *Principes de technique législative – Guide de rédaction des textes législatifs et réglementaires*, www.raadvst-consetat.be, onglet « Technique législative », recommandations n^os^ 226 et 227, formule F 5.

‡LW-BEHVMBJEH-GJDIBQW‡

Si ces explications apparaissent, *prima facie*, comme pouvant justifier un délai de conservation de quatre mois, par contre, la disposition en projet devrait mieux encadrer la conservation des données concernées au-delà de ce délai, aux fins de prévoir un délai maximum et en tout cas limité au strict nécessaire compte tenu des finalités de la conservation, la lutte contre la fraude, d'une part, et celle, d'autre part, contre les appels malveillants qui constituent, par nature, deux finalités distinctes.

2. Le paragraphe 4, alinéa 4, en projet, de l'article 122, de la loi du 13 juin 2005, est rédigé comme suit :

> « Lorsqu'un opérateur a détecté une fraude potentielle ou avérée ou une utilisation malveillante potentielle ou avérée du réseau, il prend les mesures appropriées, compte tenu des possibilités techniques les plus récentes, pour éviter que l'utilisateur final ne subisse un préjudice ou ne soit importuné ».

Telle qu'elle est rédigée, cette disposition peut être comprise comme imposant des obligations extrêmement larges aux opérateurs, obligations qui pourraient impliquer que ceux-ci soient tenus de procéder à des mesures en vue de protéger les intérêts d'un utilisateur, certes, mais qui interviendraient au détriment d'un autre, sur la base d'éléments non autrement établis par une autorité administrative ou un organe juridictionnel à la suite d'une instruction appropriée. De telles obligations sont sujettes à critiques au regard du droit au respect de la vie privée, de la liberté d'expression et du principe d'égalité et de non-discrimination.

Toutefois, le commentaire de l'article explique, à ce propos :

> « Lorsque l'opérateur a détecté une fraude potentielle ou avérée envers son abonné, il lui revient de prendre les mesures les plus appropriées pour protéger son abonné. Une de ces mesures peut être l'information de ce dernier, par exemple l'information que l'appel pourrait être frauduleux.
>
> Par ailleurs, les opérateurs doivent pouvoir contribuer à établir une utilisation malveillante du réseau (par exemple en confirmant qu'une certaine communication entrante a bien eu lieu dans le cadre d'une plainte d'harcèlement par téléphone).
>
> En pratique, en cas de harcèlement par téléphone, la victime doit s'adresser au service de médiation pour les télécommunications.
>
> Ce dernier, qui a pour mission l'aide aux victimes et n'est pas rattaché à un service de police, pourra alors obtenir via les opérateurs concernés les nom, prénom et adresse de l'auteur du harcèlement par téléphone et pourra fournir ces données à la victime de ce harcèlement (voir article 43*bis*, § 3, 7°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques). En pratique, un délai de conservation des données inférieur à 12 mois serait problématique, au vu des différentes étapes susmentionnés à suivre. Il convient également de souligner que le harcèlement par téléphone n'aura pas d'impact sur la facturation de l'opérateur à l'abonné, étant donné qu'il s'agit de communications entrantes ».

‡LW-BEHVMBJEH-GJDIBQW‡

Interrogés sur la portée de la disposition à l'examen, les délégués du Ministre ont par ailleurs exposés, en substance, que

– s'agissant des fraudes et utilisations malveillantes, les interventions ainsi attendues des opérateurs se limitent aux fraudes et utilisations malveillantes du réseau, qui revêtent un caractère manifeste et généralisé, comme des utilisations adressées à l'ensemble ou un groupe d'utilisateurs finaux en vue d'un but lucratif ou de nuire ;

– pour le surplus, les utilisations malveillantes à l'égard de personnes déterminées, comme des comportements de harcèlement par le biais de réseaux de communications ne sont pas visées en tant que tels par les obligations générales imposées aux opérateurs, le système en projet n'ayant pas vocation à modifier le système existant qui implique l'intervention préalable du service de médiation.

De l'ensemble de ces éléments, il résulte que les obligations imposées aux opérateurs par l'alinéa reproduit ci-avant s'avèrent en réalité, dans l'intention des auteurs de l'avant-projet, d'une portée plus restreinte que la compréhension que l'on pourrait avoir de cette disposition, telle qu'elle est rédigée.

Il y a toutefois lieu d'avoir égard à l'alinéa 6 de l'article 122, § 4, en projet qui permet notamment au Roi de déterminer, par arrêté délibéré en Conseil des ministres et après avis de l'Institut et des Autorités de protection des données compétentes, notamment « les actions que l'opérateur doit ou peut entreprendre lorsqu'il détecte une fraude présumée ou avérée ou une utilisation malveillante présumée ou avérée du réseau ».

En vue de justifier que le Roi puisse – sans y être tenu – déterminer ces actions, le commentaire de l'article mentionne :

> « L'adoption de cet arrêté royal n'est pas obligatoire, au vu des défis suivants. D'abord, les fraudes évoluent significativement avec le temps. Certains types de fraude peuvent disparaitre ou diminuer en importance alors que de nouveaux types de fraude peuvent voir le jour.
>
> […]
>
> De plus, les actions que l'opérateur prend lorsqu'il détecte une fraude potentielle ou avérée peuvent être diverses en fonction du type de fraude et du degré de certitude que l'opérateur a par rapport au fait qu'il s'agit bien d'une fraude (seulement des indices ou une certitude à cet égard) ».

Compte tenu de ces justifications, la question se pose de savoir si l'intention est effectivement de limiter les obligations imposées à l'opérateur aux nuisances (fraudes ou utilisations malveillantes) manifestes, ce qui serait de nature à mieux garantir la proportionnalité de la disposition envisagée au regard des droits et libertés évoqués plus haut, ou si telle n'est pas l'intention.

Par ailleurs, si la section de législation peut comprendre que l'évolution et la diversification rapides de ces nuisances requièrent certaines souplesse et forme de réactivité, les droits et libertés précités seraient mieux garantis si le Roi était tenu – et non simplement autorisé – à définir les actions, ou catégories d'actions à entreprendre par l'opérateur, en distinguant en outre l'hypothèse des nuisances manifestes ou « avérées » des autres hypothèses.

‡LW-BEHVMBJEH-GJDIBQW‡

Enfin, les critères encadrant l'habilitation ainsi conférée au Roi doivent être précisés par le législateur, pour satisfaire au principe de légalité inscrit à l'article 22 de la Constitution.

3. Il ressort des explications communiquées par les délégués du Ministre que l'établissement de la réalité d'une utilisation malveillante du réseau, telle que visée à l'article 122, § 4, alinéa 6, en projet, n'incombera pas à l'opérateur mais aux autorités compétentes en la matière, comme le service de médiation.

Le texte en projet sera revu et complété aux fins de le préciser.

4. La disposition à l'examen sera revue à la lumière de ces observations.

Article 5

1. L'article 5, 1°, entend remplacer l'article 123, § 1er, de la loi du 13 juin 2005, afin d'y traiter spécifiquement de la conservation des données de localisation autres que les données relatives au trafic.

Cette disposition transpose l'article 9 de la directive 2002/58/CE, qui dispose comme suit :

> « 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 ».

‡LW-BEHVMBJEH-GJDIBQW‡

2. Il résulte de cette disposition que, lorsque les données concernées 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.

Deux hypothèses sont donc prévues, à la condition que ces données « puissent être traitées » :

– soit les données ont été rendues anonymes ;

– soit l'utilisateur ou l'abonné a donné son consentement ; elles ne peuvent alors être traitées que dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée.

Le texte en projet prévoit pour sa part, cinq hypothèses. Celles figurant à l'article 123, § 1er, 1°, 2° et 5°, en projet, de la loi du 13 juin 2005 ne figurent pas dans l'article 9 de la directive 2002/58/CE.

L'une de ces trois autres hypothèses envisagées ne pose pas de difficulté en soi. Ainsi, lorsque le traitement est « nécessaire pour répondre à une obligation légale » (article 123, § 1er, 5°, en projet), il va de soi que, du moment que la disposition légale prévoyant ce traitement répond elle-même au prescrit de la directive 2002/58/CE, spécialement son article 15, paragraphe 1, le traitement est admissible. En d'autres termes, si difficulté il y a, cette dernière ne résiderait dès lors pas dans l'article 123, § 1er, 5°, en projet, de la loi du 13 juin 2005, mais, le cas échéant dans la ou les dispositions prévoyant « l'obligation légale », dispositions qui se situent ailleurs dans le projet et à l'examen desquelles il est renvoyé.

Par contre, les hypothèses visées à l'article 123, § 1er, 1° et 2°, posent question. Elle visent la conservation et le traitement qui sont :

1° « nécessaire[s] pour le bon fonctionnement et la sécurité du réseau ou du service, les données étant conservées le temps nécessaire à cette fin », ou

2° « nécessaire[s] pour déceler des fraudes ou l'utilisation malveillante du réseau, les données étant conservées le temps nécessaire à cette fin ».

Ces deux hypothèses évoquent celles envisagées également par l'article 4 de l'avant-projet, qui a trait, pour sa part, aux données relatives au trafic, visées par l'article 6 de la directive 2002/58/CE.

‡LW-BEHVMBJEH-GJDIBQW‡

Si l'article 15, paragraphe 1, de la même directive, permet aux États membres d'adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus notamment en son article 9, c'est aux conditions prévues par cet article 15. Il faut, spécialement, que la mesure envisagée 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. Une telle mesure, qui consisterait en la conservation de données, doit par ailleurs être limitée dans le temps, à ce qui est nécessaire.

S'agissant de l'article 123 en projet, il y a lieu de relever que

1° le commentaire de l'article ne mentionne aucune des hypothèses dont il est question ; à fortiori, le commentaire de l'article ne permet pas de comprendre en quoi et d'apprécier si les mesures envisagées répondraient aux conditions de l'article 15, paragraphe 1, de la directive 2002/58/CE, spécialement en ce qui concerne la nécessité, le but, et la proportionnalité ;

2° la mention, dans le texte en projet, de ce que les données sont conservées « le temps nécessaire » à la finalité envisagée manque de précision ; il conviendrait que le législateur fixe à toute le moins un délai de conservation maximum, qu'il doit, en outre, être en mesure de justifier.

L'article 123, § 1er, 1° et 2°, en projet, sera réexaminé à la lumière de ces deux observations.

3. Le 2°, premier tiret, entend supprimer les mots « définitivement ou temporairement » qui figurent dans l'article 123, § 2, 1°, e), de la loi du 13 juin 2005.

Le commentaire de l'article s'en explique comme suit :

> « Le paragraphe 2 ne vise plus le retrait temporaire ou définitif du consentement, étant donné qu'une telle distinction n'est pas prévue dans la notion de consentement au sens du RGDP ».

Cette justification perd toutefois de vue que, selon l'article 9 de la directive 2002/58/CE, les utilisateurs et abonnés qui ont donné leur consentement au traitement des données de localisation autres que les données relatives au trafic, 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.

La disposition à l'examen sera revue de sorte que l'article 123 de la loi du 13 juin 2005 prévoie expressément cette possibilité.

‡LW-BEHVMBJEH-GJDIBQW‡

Article 7

Même si le paragraphe 2 en projet habilite le Roi à définir les données à conserver et les exigences auxquelles elles doivent répondre, le dispositif en projet gagnerait à définir expressément à tout le moins la notion de « données de souscription ». Il en va de même de la notion de « réseaux électroniques sous-jacents ».

Article 10

1. L'article 127/1 en projet énonce, de manière assez générale, quelles catégories d'autorités ont accès aux données conservées en vertu des articles 122, 123, 126, 126/1, et 127, et en vue de quelles finalités.

Dans la philosophie du texte en projet, et comme s'en explique le commentaire de l'article,

> « [p]our qu'une autorité puisse obtenir des données de l'opérateur, il est nécessaire qu'elle réponde à une des finalités visées à l'article 127/1 et que sa loi organique ou sectorielle lui donne le pouvoir d'obtenir ces données de l'opérateur ».

S'il est aisément compréhensible que, dans l'intention des auteurs de l'avant-projet, les conditions de conservation des données ont vocation à figurer dans la loi du 13 juin 2005, tandis que les conditions d'accès à celles-ci ont vocation à figurer dans les législations organiques des autorités auxquelles il est envisagé de donner l'accès, il n'en demeure pas moins que, pour donner un effet utile à la finalité ou aux finalités d'une conservation, il convient que les autorités ayant accès aux données poursuivent la même finalité. Il convient également que la finalité soit définie avec suffisamment de précision et que les règles définissant les finalités de conservation et d'accès soient facilement compréhensibles.

La question se pose de savoir si le système mis en place par l'article 127/1 en projet, combiné avec les dispositions générales relatives à la conservation des données, d'une part, et avec les dispositions spécifiques qui conditionnent l'accès aux données, d'autre part, rencontre ces exigences.

2. Les objectifs des auteurs de l'avant-projet sont, par l'adoption de l'article 127/1, selon le commentaire de l'article,

> « […] d'une part, d'apporter, dans une certaine mesure, de la sécurité juridique aux opérateurs quant aux autorités disposant d'un droit d'accès aux données qu'ils conservent, et, d'autre part, d'apporter de la transparence aux utilisateurs finaux quant à l'utilisation de leurs données d'identification, de trafic et de localisation ».

La section de législation se demande toutefois si, telle qu'elle est rédigée, cette disposition ne risque pas d'entrainer un effet pervers, allant à l'encontre de la sécurité juridique.

‡LW-BEHVMBJEH-GJDIBQW‡

Ainsi, même si elle renvoie expressément, en matière d'accès, aux conditions prévues par les dispositions spécifiques qui habilitent les catégories d'autorités concernées à avoir accès aux données conservées, l'article 127/1 en projet peut donner l'impression que toutes les catégories d'autorités y visées ont accès à toutes les données visées aux articles 122, 123, 126, 126/1.

Or, ceci peut être source de confusion.

Ainsi, la conservation généralisée et indifférenciée des adresses IP source visées à l'article 123 de la loi du 13 juin 2005, tel que le projet envisage de le modifier, et les données qui font l'objet d'une conservation ciblée, visée par l'article126/1 en projet ne peuvent être conservées qu'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.

Cette limitation n'apparait pas à la lecture de l'article 127/1 dont le paragraphe 1er, 1°, se réfère, de manière tout à fait générale, à la prévention, la recherche, la détection de la poursuite d'infractions pénales, d'infractions passibles d'une sanction administrative à caractère pénal, ou d'infraction commises à l'aide d'un réseau de communications électroniques.

Certes, s'agissant de la conservation géographique ciblée, l'article 126/1 mentionne que les données concernées 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 personnes physiques. Par ailleurs, 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 (article 17 de l'avant-projet).

Il reste toutefois que, dès lors que l'article 127/1, § 1er, en projet, entend décrire la finalité de l'accès, celle-ci doit pourvoir être mise en rapport avec la finalité du régime de conservation mis en place. Or, s'agissant de la conservation des adresses IP source, aucune finalité spécifique n'est mentionnée à l'article 126, § 1er, en projet, qui renvoie seulement aux finalités visées à l'article 127/1 en projet. Ce renvoi s'avère insuffisant aux regard des exigences de la Cour de Justice en ce qui concerne les fins de sauvegarde de la sécurité nationale, de lutte contre la criminalité grave et de prévention des menaces graves contre la sécurité publique.

La disposition en projet doit dès lors revue aux fins de faire apparaitre clairement le lien entre la finalité de la conservation et la finalité de l'accès, et de lever toute ambiguïté qui serait de nature à laisser supposer, par exemple, que dans des cas où la conservation ne pourrait avoir lieu qu'à des fins de lutte contre la criminalité grave, des autorités pourraient y avoir accès en vue de lutter contre une criminalité non grave.

2. L'appréciation de la notion de « sanction administrative à caractère pénal » – à savoir, selon le commentaire de l'article, une sanction qualifiée d'administrative en droit interne, mais susceptible d'être qualifiée de pénale au sens de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales – ne peut être laissée ni à l'opérateur qui donnerait l'accès aux données conservées ni à l'autorité qui demanderait l'accès aux données.

‡LW-BEHVMBJEH-GJDIBQW‡

Cette notion éminemment jurisprudentielle dépend ainsi d'une appréciation au cas par cas, qui ne se concilie pas avec la prévisibilité et la précision attendue d'une législation qui met en place un système d'ingérence dans le droit au respect de la vie privée.

3. Compte tenu des éléments ainsi mis en exergue, la section de législation se demande si la disposition à l'examen n'est pas plus de nature à nuire à la sécurité juridique qu'à garantir celle-ci.

Elle sera réexaminée à la lumière des observations qui précèdent.

Article 11

1. La section de législation n'aperçoit pas la portée de l'alinéa 3 de l'article 127/2, § 2, en projet, qui prévoit :

> « Les opérateurs sont en mesure d'établir des liens entre les données conservées pour les autorités ».

Le commentaire de l'article mentionne à ce propos :

> « Il revient aux opérateurs de décider comment ils s'organisent pour la conservation des données au bénéfice des autorités (en particulier les données conservées conformément aux articles 126, 126/1, 127). Dès lors, si une même donnée est visée dans plusieurs articles, ils peuvent conserver la donnée une seule fois. Par contre, les opérateurs doivent être mesure d'établir des liens entre les données conservées pour les autorités. Ceci est nécessaire vu que pour répondre à une demande d'une autorité, un opérateur pourrait être amené à consulter des données conservées sur base de différents articles ».

Ce faisant, le commentaire de l'article ne permet pas de mieux comprendre quelle sera la nature du « lien » à établir par l'opérateur entre les données conservées.

Il convient à tout le moins que la disposition à l'examen n'impose pas d'obligation telle que l'opérateur s'en trouverait ainsi chargé d'apprécier le contenu des données concernées et la pertinence, en opportunité, d'établir un lien entre celles-ci. En d'autres termes, le lien à établir ne peut être que technique ou technologique, et l'établissement de celui-ci ne peut amener l'opérateur à se livrer, en quelque sorte, à un examen ou une analyse des données auxquelles seules les autorités qui y ont accès peuvent se livrer.

Selon les délégués du Ministre interrogés à ce propos, telle n'est pas l'intention. La disposition à l'examen et le commentaire de l'article seront revus aux fins de faire apparaitre sans ambiguïté l'intention qui y préside.

3. Concernant la destruction des données, prévue par l'article 127/2, § 3, alinéa 2, 1°, en projet, le dispositif répondrait mieux aux exigences relatives à la destruction irrémédiable des données si, une autorité, tel l'Institut, était spécifiquement chargée de contrôler régulièrement cette destruction [42].

[42] Voir, en ce sens, l'avis n° 58.449/4, point 3.4.2.2.2.

‡LW-BEHVMBJEH-GJDIBQW‡

Article 12

Selon le paragraphe 3 de l'article 127/3 en projet,

« Le Roi peut déterminer, après avis des autorités de protection des données compétentes et de l'Institut :

1° les exigences auxquelles la Cellule de coordination doit répondre, en particulier au niveau de la disponibilité et de l'accessibilité ;

2° les exigences auxquelles un membre de la Cellule de coordination doit répondre, en ce compris lui imposer, le cas échéant, de faire l'objet d'un avis de sécurité positif ;

3° si un avis de sécurité positif est imposé, les catégories d'opérateurs qui sont dispensés de l'obligation de désigner un officier de sécurité comme prévu à l'article 22*quinquies*, § 6, de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, ainsi que les règles qui s'appliquent en l'absence d'un tel officier ;

4° les règles permettant que les autorités belges qui ont besoin de connaître les coordonnées de la Cellule de coordination et de ses membres en soient informés ;

5° les autres règles régissant la collaboration entre les opérateurs et les autorités belges ou avec certaines d'entre elles, y compris, 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, le Roi peut prévoir des règles différentes selon 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 le lieu où ils opèrent leurs activités ».

Cette disposition appelle plusieurs observations.

2. L'article 127/3, § 3, en projet, prévoit que le Roi « peut » fixer les règles dont l'objet y est énuméré, et non pas qu'Il « fixe » celles-ci.

Par conséquent, en l'absence de mise en œuvre par le Roi de la possibilité qui Lui est conférée par la disposition en projet, aucune règle ne sera fixée concernant les différents points énumérés.

À titre d'exemple, il pourrait ainsi advenir qu'aucune règle ne soit fixée concernant les exigences auxquelles les membres de la Cellule de coordination doivent répondre.

‡LW-BEHVMBJEH-GJDIBQW‡

Or, ces exigences sont essentielles en vue d'assurer que la Cellule de coordination collaborera de manière effective et efficace avec les autorités, et qu'elle disposera de toutes les garanties appropriées pour la conservation et la transmission sécurisée des données concernées, conformément au prescrit de la loi en projet.

Par conséquent, il convient que l'habilitation en projet soit rédigée de manière telle que le Roi ne soit pas simplement autorisé à fixer les règles concernées, mais qu'il soit tenu de les fixer.

3. Il appartient au législateur de déterminer les critères à mettre en œuvre par le Roi lorsqu'Il pourvoira à l'exécution de la disposition en projet, spécialement s'agissant des règles prévues au paragraphe 3, alinéa 1er, 2° et 3°, en projet.

Il en va particulièrement ainsi de la question de principe de savoir si un avis de sécurité positif sera ou non requis, indépendamment même des règles différentes qui seraient imposées à des catégories d'opérateurs différentes, sur la base des critères prévus à l'alinéa 2 du paragraphe 3 en projet [43].

4. La disposition en projet sera revue et complétée à la lumière des observations qui précèdent.

Article 13

L'article 13 de l'avant-projet envisage d'insérer dans la loi du 13 juin 2005 un article 127/4 nouveau, rédigé comme suit :

> « Par arrêté délibéré en Conseil des ministres, le Roi fixe, sur proposition du ministre de la Justice et du ministre, après avis des autorités de protection des données compétentes et de l'Institut, les conditions dans lesquelles les fournisseurs de réseaux privés de communications électroniques et de services de communications électroniques qui ne sont pas accessibles au public enregistrent et conservent les données permettant l'identification des personnes concernées de l'équipement terminal ou du service de communications électroniques employé, à l'exception des données qui sont liées à une seule communication électronique, en vue de la poursuite et la répression d'infractions pénales, et en vue de la répression d'appels malveillants vers les services d'urgence, en vue de la recherche par le service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques, ainsi qu'en vue de l'accomplissement des missions de renseignement prévues par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.
>
> Par arrêté délibéré en Conseil des ministres, le Roi fixe, sur proposition du ministre de la Justice et du ministre, après avis des autorités de protection des données compétentes et de l'Institut, les mesures techniques et administratives imposées aux fournisseurs visées à l'alinéa 1er, en vue de permettre l'identification des personnes concernées, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des communications non accessibles au public aux conditions prévues

[43] Dans un sens similaire, voir l'avis n° 58.449/4, observation sous l'article 5.

‡LW-BEHVMBJEH-GJDIBQW‡

par les articles 46*bis*, 88*bis*, 90*ter* à 90*decies*, 464/13, 464/25 et 464/26 du Code d'instruction criminelle, ainsi qu'aux conditions prévues par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Les fournisseurs visés à l'alinéa 1er font en sorte que les données mentionnées à l'alinéa 1er soient accessibles de manière illimitée depuis la Belgique ».

Ces habilitations sont manifestement excessives. S'agissant des fournisseurs de réseaux privés de communications électroniques et de services de communications électroniques qui ne sont pas accessibles au public, elles ont en effet pour objet d'habiliter le Roi à fixer intégralement les régimes applicables :

– en matière d'enregistrement et de conservation des données permettant l'identification des personnes concernées, de l'équipement terminal ou du service de communications électroniques employé, en vue, de surcroit, de la poursuite et la répression d'infractions pénales, de la répression d'appels malveillants vers les services d'urgence, de la recherche par le service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques, et de l'accomplissement des missions de renseignement prévues par la loi du 30 novembre 1998 ;

– en ce qui concerne les mesures en vue de permettre l'identification des personnes concernées, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des communications non accessibles au public aux conditions prévues par le Code d'instruction criminelle et par la loi du 30 novembre 1998.

Eu égard au principe de légalité inscrit à l'article 22 de la Constitution, de telles ingérences dans le droit au respect de la vie privée, plus spécialement la conservation et l'accès à des données à caractère personnel doivent être organisées par un régime encadré à suffisance par le législateur.

Un tel régime fait totalement défaut en l'espèce.

Par conséquent, la disposition à l'examen sera fondamentalement revue.

Article 14

1. Au paragraphe 2, alinéa 3, en projet, il convient de remplacer les mots « visés à l'alinéa 1er » par les mots « visés à l'alinéa 2 ».

2. Au paragraphe 2, alinéa 6, en projet, il convient de définir la nature de la nullité envisagée : s'agit-il d'une nullité de plein droit et d'ordre public, comme on peut le supposer ?

‡LW-BEHVMBJEH-GJDIBQW‡

Article 16

1. L'article 16 entend insérer un 2°/1 dans l'article 14, § 2, de la loi du 17 janvier 2003 'relative au statut du régulateur des secteurs des postes et des télécommunications belges', en vue de permettre à l'Institut de « demander aux opérateurs les données d'identification, de trafic ou de localisation, au sens de la loi du 13 juin 2005 relative aux communications électroniques pour autant que cela soit nécessaire à l'accomplissement de l'une de ses missions ».

L'Institut pourrait ainsi avoir accès à l'ensemble des données énumérées, sans qu'une distinction soit opérée entre les catégories de données et sans que soit explicitée la finalité précise, qui justifie l'accès.

L'article 127/1, § 1er, en projet, ne permet pas de mieux circonscrire l'ingérence à laquelle l'Institut est ainsi habilité à procéder puisque cet article 127/1, § 1er, en projet, se borne à prévoir que la conservation des données visées aux articles 122, 123, 126, 126/1 et 127, de la loi du 13 juin 2005, tels qu'ils résulteront de leur modification par le texte en projet, a pour finalité, s'agissant de l'Institut, la mise en œuvre et le contrôle de la loi du 13 juin 2005.

Quant au commentaire de l'article, il mentionne :

> « La disposition insérée vise à permettre à l'Institut d'avoir accès aux données d'identification, de trafic ou de localisation, au sens de la loi du 13 juin 2005 relative aux communications électroniques, lorsque cela s'avère nécessaire à l'accomplissement de l'une de ses missions.
>
> Tel est le cas notamment en cas de contrôle du respect par les opérateurs de leurs obligations légales, telles que l'obligation d'adresser une facturation détaillée, prévue à l'article 110 de la loi du 13 juin 2005 relative aux communications électroniques, ou dans le cadre de la mise en œuvre de l'article 114 de cette même loi. Par exemple, en matière de facturation détaillée, l'IBPT doit être en mesure de demander à l'opérateur de lui fournir un échantillon de factures. Or, ces factures reprennent des données de trafic, telles que les destinataires, dates, heures et durées des communications passées ».

2. Force est de constater qu'un accès aussi général que celui prévu par le texte en projet ne parait pas se justifier sur le plan de la proportionnalité, au regard de l'article 15, paragraphe 1, de la directive 2002/58/CE compris à la lumière de la jurisprudence y relative de la Cour de Justice.

L'exemple mentionné au commentaire de l'article, qui apparait extrêmement ciblé, dément au contraire la nécessité de l'ampleur de l'accès autorisé.

Tout aussi fondamentalement, la question se pose de savoir quelles sont les garanties effectives dont les personnes concernées bénéficieraient contre les éventuels abus.

3. La disposition à l'examen sera revue à la lumière des observations qui précèdent.

‡LW-BEHVMBJEH-GJDIBQW‡

Article 24

1. Il résulte du commentaire de l'article que l'article 16/2/1 en projet de la loi du 30 novembre 1998, vise, en son alinéa 1er, 1°, une injonction de « *quick freeze* » classique des données déjà conservées par les opérateurs, tandis que l'alinéa 1er, 2°, concerne une injonction de « *quick freeze* » pour l'avenir.

Cette distinction n'apparait pas clairement du dispositif en projet, spécialement la portée exacte de l'injonction prévue par l'alinéa 1er, 2°, en projet.

2. Par ailleurs, concernant la durée de conservation des données, il convient de distinguer les deux hypothèses précitées.

Ainsi, pour l'opération de « *quick freeze* » classique, l'alinéa 4 de la disposition en projet répond à la question de savoir quel sera le délai de conservation des données dont la conservation a été ordonnée.

Par contre, s'agissant de l'opération de « *quick freeze* » pour l'avenir, la disposition en projet manque de clarté : elle ne permet pas de faire la distinction entre la durée de la mesure de « *quick freeze* », d'une part, et la durée de conservation des données ainsi gelées, d'autre part. Sur ce point, aux fins de garantir que l'opération de « *quick freeze* » pour l'avenir n'excède pas ce qui est strictement nécessaire à la sécurité nationale, le texte en projet devrait être complété aux fins de fixer une durée maximum de l'opération, sous réserve d'un éventuel renouvellement [44]. Un autre biais pourrait consister à limiter la conservation des données à la durée du « *quick freeze* ». Il convient en tout cas de lever toute ambiguïté sur cette question.

Enfin, la section de législation n'aperçoit pas, dans le contexte du système ainsi mis en place, la portée exacte de l'alinéa 8 qui prévoit que les données conservées par les opérateurs sont détruites douze mois après le début de leur conservation.

3. La disposition en projet sera revue aux fins de lever toute ambiguïté quant au système mis en place, notamment quant à la durée de l'opération de « *quick freeze* » pour l'avenir, à la durée de conservation des données, ce en vue de garantir que ces durées soient limitées au strict nécessaire, et que les données soient détruites par les opérateurs dès que cette nécessité n'est plus rencontrée.

[44] Comparer avec l'article 39*quinquies*, alinéa 3, 6ème et 7ème tirets, en projet, du Code d'instruction criminelle (article 17 de l'avant-projet).

‡LW-BEHVMBJEH-GJDIBQW‡

Article 28

Comme l'avait déjà souligné la section de législation dans son avis n° 42.178/2 donné le 19 février 2007 sur un avant-projet devenu la loi du 4 février 2010 'relative aux méthodes de recueil des données par les services de renseignement et de sécurité' [45], les principes de proportionnalité et de subsidiarité conditionnent le recours aux méthodes spécifiques et, à fortiori, aux méthodes exceptionnelles, en vue de garantir que celles-ci seront mises en œuvre dans des conditions respectueuses des droits fondamentaux.

Pour garantir le respect de ces principes, la disposition en projet devrait être complétée aux fins de prévoir la durée maximale – moyennant le cas échéant prolongation justifiée par la stricte nécessité – du repérage ou de la localisation, durée qui serait proportionnée à la gravité des éléments justifiant le recours à la méthode.

Par ailleurs, au titre des garanties procédurales, la section de législation n'aperçoit pas ce qui peut justifier que, pour la méthode spécifique envisagée, une décision écrite du dirigeant du service ne soit pas requise, comme c'est le cas pour d'autres méthodes spécifiques.

La disposition à l'examen sera revue à la lumière de ces observations.

Article 34

L'article 62, paragraphe 2, alinéa 2, en projet, de la loi du 7 avril 2019 'établissant un cadre pour la sécurité des réseaux et des systèmes d'informations d'intérêt général pour la sécurité publique' prévoit que pour avoir accès aux données d'identification, de trafic et de localisation conservées par les opérateurs, le Centre pour la Cybersécurité (en abrégé « CSIRT ») national « respecte les règles et les procédures prévues par la loi du 13 juin 2005 relative aux communications électroniques ».

Cette disposition manque de précision. Elle doit viser les dispositions précises de la loi du 13 juin 2005 qui auront vocation à s'appliquer au CSIRT national, le cas échéant, selon différentes hypothèses.

L'article 62 en projet sera revu et complété en conséquence.

Article 36

1. L'article 36 prévoit que la loi en projet « entre en vigueur [lire : « produit ses effets »] le jour où l'annulation de la loi du 29 mai 2016 par l'arrêt n°57/2021 de la Cour constitutionnelle prend effet ».

[45] http://www.raadvst-consetat.be/dbx/avis/42178.pdf.

‡LW-BEHVMBJEH-GJDIBQW‡

Le commentaire de l'article mentionne :

« La loi prend effet rétroactivement afin de ne pas créer un vide juridique dans lequel des données importantes de communications électroniques qui pourraient être cruciales pour l'enquête ne soient plus conservées ».

Tel qu'il est rédigé, l'article 36 entend faire rétroagir la loi à l'examen au jour où l'annulation de la loi du 29 mai 2016 a elle-même pris effet, soit, au jour de l'entrée en vigueur de cette loi.

2.2. En effet, l'avant-projet à l'examen se donne pour objet la mise en place d'un système articulé de conservation et d'accès à des données à caractère personnel dans la sphère des communications électroniques.

Le cœur du mécanisme en projet réside dans les articles 126 à 127/4 que l'avant-projet entend insérer dans la loi du 13 juin 2005.

La méconnaissance de ces nouvelles dispositions sera sanctionnée pénalement en vertu des modifications que l'article 15 de l'avant-projet entend apporter à l'article 145, § 1er, de la même loi.

Cet article 15 entend par ailleurs ajouter un paragraphe 3*ter* au même article 145, rédigé comme suit :

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

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

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

Par conséquent, l'effet rétroactif conféré à l'avant-projet par son article 36 méconnait le principe de la non-rétroactivité des lois pénales consacré par l'article 7 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales et par l'article 15 du Pacte international relatif aux droits civils et politiques.

‡LW-BEHVMBJEH-GJDIBQW‡

2.3. Par ailleurs, il convient de rappeler que, dans son arrêt n° 57/2021, la Cour constitutionnelle a refusé de faire application de la possibilité offerte par l'article 8, alinéa 3, de la loi spéciale du 6 janvier 1989 'sur la Cour constitutionnelle', de maintenir les effets des dispositions annulées de la loi du 29 mai 2016. Ce faisant, elle a mis en œuvre ce que la Cour de justice avait elle-même jugé dans son arrêt *La Quadrature du Net*, à savoir qu'il serait porté

> « atteinte à la primauté et à l'application uniforme du droit de l'Union si des juridictions nationales avaient le pouvoir de donner aux dispositions nationales la primauté par rapport au droit de l'Union auquel ces dispositions contreviennent, serait-ce même à titre provisoire » [46].

L'annulation prononcée a donc elle-même « pris effet » *ex tunc*, au jour de l'entrée en vigueur de la loi du 29 mai 2016.

La rétroactivité conférée au dispositif à l'examen aboutira à conférer *ex post* un fondement légal à une série d'ingérences dans le droit au respect de la vie privée qui s'en trouvent aujourd'hui dépourvues, par l'effet de l'arrêt d'annulation n° 57/2021, non asso de la Cour constitutionnelle, non assorti de limite dans le temps, compte tenu de l'arrêt *La Quadrature du Net* de la Cour de Justice. En tant qu'elle a pour effet de valider pour le passé des ingérences, dans les droits fondamentaux des personnes – dont les données ont été conservées – qui doivent être considérées comme contraires au droit de l'Union, pareille rétroactivité n'est pas admissible au regard du droit de l'Union [47].

3. Il résulte des considérations qui précèdent que l'article 36 doit être omis.

*

[46] Point 217.

[47] Il convient de rappeler, pour le surplus, que la Cour constitutionnelle dans son arrêt n° 57/2021 du 22 avril 2021, a expressément envisagé que les preuves qui auraient été recueillies en application des dispositions annulées de la loi du 29 mai 2016 puissent être déclarées admissibles au cas par cas :
« B.24.3. Il appartient au juge pénal compétent de statuer, le cas échéant, sur l'admissibilité des preuves qui ont été recueillies lors de la mise en œuvre des dispositions annulées, conformément à l'article 32 du titre préliminaire du Code de procédure pénale et à la lumière des précisions apportées par la Cour de justice dans l'arrêt du 6 octobre 2020 précité »

‡LW-BEHVMBJEH-GJDIBQW‡

Aangezien de adviesaanvraag ingediend is op basis van artikel 84, § 1, eerste lid, 2°, van de wetten 'op de Raad van State', gecoördineerd op 12 januari 1973, beperkt de afdeling Wetgeving overeenkomstig artikel 84, § 3, van de voornoemde gecoördineerde wetten haar onderzoek tot de rechtsgrond van het voorontwerp,‡ de bevoegdheid van de steller van de handeling en de te vervullen voorafgaande vormvereisten.

Wat die drie punten betreft, geeft het voorontwerp aanleiding tot de volgende opmerkingen.

VOORAFGAANDE VORMVEREISTEN

Over dit voorontwerp van wet dat ter fine van advies voorgelegd is, is overleg gepleegd op de Ministerraad van 7 mei 2021, waarop besloten is dat over de ontworpen tekst een openbare raadpleging gehouden moet worden en dat die tekst om advies voorgelegd moet worden aan de Gegevensbeschermingsautoriteiten en aan de Raad van State. De resultaten van al die raadplegingen zullen vervolgens binnen de betrokken Werkgroep Beleidscoördinatie besproken worden, waarna de eventueel aangepaste tekst van het voorontwerp voorgelegd zal worden aan het Interministerieel Comité voor Telecommunicatie en Radio-Omroep en Televisie en aan het Overlegcomité.[1]

Na dat overleg zal die Werkgroep opnieuw samenkomen en "[i]ndien er zich in de schoot van de Werkgroep nog problemen stellen bij eventuele aanpassingen die nodig zouden zijn", zal de ontworpen tekst opnieuw aan de Ministerraad voorgelegd worden. In het andere geval, als er binnen de Werkgroep geen problemen meer zijn, zal het voorontwerp ter ondertekening aan de Koning voorgelegd worden met het oog op indiening bij de Kamer van volksvertegenwoordigers.

De afdeling Wetgeving wijst er voorts op dat het advies van het Controleorgaan op de politionele informatie gegeven is op 21 mei 2021, dat de openbare raadpleging, harerzijds, afgesloten is op 4 juni 2021 en dat het advies van het Vast Comité I, ten slotte, uitgebracht is op 14 juni 2021. Die stukken zijn aan de afdeling Wetgeving overgezonden na de indiening van de adviesaanvraag en zijn *a fortiori* van recentere datum dan het overleg in de Ministerraad dat op 7 mei 2021 plaatsgehad heeft.

Uit het voorgaande blijkt dat de om advies voorgelegde tekst nog vatbaar is voor wijzigingen die niet voortvloeien uit het advies van de afdeling Wetgeving: zo zouden daarin wijzigingen aangebracht kunnen worden naar aanleiding van de openbare raadpleging, de adviezen van de Gegevensbeschermingsautoriteiten, van het Controleorgaan op de politionele informatie en van het Vast Comité I en na afloop van het overleg dat binnen het Interministerieel Comité en het Overlegcomité moet plaatsvinden.

‡ Aangezien het om een voorontwerp van wet gaat, wordt onder "rechtsgrond" de overeenstemming met de hogere rechtsnormen verstaan.

[1] Dit blijkt ook uit de brief met de adviesaanvraag.

‡LW-BEHVMBJEH-GJDIBQW‡

Ook al is de afdeling Wetgeving ertoe gehouden om over een wetgevend voorontwerp of over een ontwerp van besluit advies uit te brengen zelfs indien de verplichte voorafgaande vormvereisten niet vervuld zijn,[2] dienen aan haar evenwel, om haar in staat te stellen haar taak naar behoren te vervullen, definitieve ontwerpteksten voorgelegd te worden, niet alleen om een onnodig onderzoek te vermijden van een tekst die naderhand nog gewijzigd zal worden, maar ook om te vermijden dat een ontwerp ten gevolge van wijzigingen die niet het gevolg zijn van haar advies, opnieuw om advies voorgelegd dient te worden.[3]

De stellers van het voorontwerp worden verzocht zich voortaan te houden aan de regel die aldus in herinnering gebracht is.

REIKWIJDTE EN CONTEXT VAN HET VOORONTWERP

A. EUROPEES RECHT EN EUROPESE RECHTSPRAAK EN INTERNE RECHTSPRAAK

1.1. Bij een arrest van 8 april 2014 van de grote kamer in antwoord op prejudiciële vragen vanwege het Hooggerechtshof van Ierland en het Grondwettelijk Hof van Oostenrijk[4] heeft het Hof van Justitie van de Europese Unie (hierna "het Hof van Justitie") richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 'betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG' ongeldig verklaard.

Naar aanleiding van dat arrest van het Hof van Justitie heeft het Grondwettelijk Hof bij arrest nr. 84/2015 van 11 juni 2015 de vernietiging uitgesproken van de wet van 30 juli 2013 'houdende wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90*decies* van het Wetboek van strafvordering', welke wet strekte tot de gedeeltelijke omzetting van richtlijn 2006/24/EG.

Dat arrest van het Grondwettelijk Hof steunt op de volgende motivering:

> "B.10.1. Zoals het Hof van Justitie heeft opgemerkt in de punten 56 en 57 van zijn arrest, schrijft de richtlijn voor om alle verkeersgegevens betreffende vaste en mobiele telefonie, internettoegang, e-mail over het internet en internettelefonie te bewaren, waardoor zij algemeen van toepassing is op alle personen en alle elektronische communicatiemiddelen, zonder onderscheid op basis van het doel, namelijk zware criminaliteit bestrijden, dat de Uniewetgever wilde nastreven.

[2] Uit artikel 84, § 3, tweede lid, van de wetten 'op de Raad van State', gecoördineerd op 12 januari 1973, volgt dat, wanneer het advies gevraagd wordt binnen een termijn van dertig of zestig dagen dan wel van vijf werkdagen, het gegeven wordt "zelfs indien de voorgeschreven vormvereisten niet zijn vervuld".

[3] Zie in deze zin advies 39.690/3, dat op 8 februari 2006 gegeven is over een voorontwerp dat geleid heeft tot de wet van 20 juli 2006 'betreffende de oprichting en de werking van het Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten', http://www.raadvst-consetat.be/dbx/adviezen/39690.pdf.

[4] HvJ (grote kamer), arrest *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources e.a.,* 8 april 2014, C-293/12, ECLI:EU:C:2014:238 en HvJ (grote kamer), arrest *Kärntner Landesregierung e.a. v. Oostenrijk*, C-594/12, ECLI:EU:C:2014:238, hierna het arrest "*Digital Rights*").

‡LW-BEHVMBJEH-GJDIBQW‡

De bestreden wet verschilt op dat punt niet van de richtlijn. Zoals in B.8 is vermeld, zijn immers de categorieën van gegevens die moeten worden bewaard identiek aan die welke zijn opgesomd in de richtlijn, terwijl geen enkel onderscheid wordt gemaakt met betrekking tot de betrokken personen of de bijzondere regels die moeten worden bepaald op basis van het doel van bestrijding van de inbreuken beschreven in artikel 126, § 2, van de wet van 13 juni 2005, dat bij de bestreden wet werd vervangen. Net zoals het Hof van Justitie heeft vastgesteld met betrekking tot de richtlijn (punt 58), is de wet dus ook van toepassing op personen voor wie er geen enkele aanwijzing bestaat dat hun gedrag - zelfs maar indirect of van ver - een verband vertoont met de in de bestreden wet opgesomde inbreuken. Op dezelfde wijze is de wet, zonder enige uitzondering, ook van toepassing op personen van wie de communicaties onder het beroepsgeheim vallen.

B.10.2. Niet méér dan het geval is voor de richtlijn, vereist het bestreden artikel 5 enig verband tussen de gegevens die moeten worden bewaard en een bedreiging van de openbare veiligheid. Het beperkt evenmin de bewaring van de desbetreffende gegevens tot een bepaalde periode of een bepaalde geografische zone of nog tot een kring van personen die betrokken kunnen zijn bij een door de wet beoogde inbreuk, of die zouden kunnen helpen, door het bewaren van de gegevens, bij het voorkomen, opsporen of vervolgen van die inbreuken.

B.10.3. Ook al worden de autoriteiten die gemachtigd zijn tot toegang tot de bewaarde gegevens, opgesomd in artikel 126, § 5, 3°, van de wet van 13 juni 2005, vervangen bij artikel 5 van de bestreden wet, toch wordt bij de wet geen enkele materiële of procedurele voorwaarde vastgelegd met betrekking tot die toegang.

B.10.4. Wat ten slotte de bewaarperiode van de gegevens betreft, maakt de wet geen enkel onderscheid tussen de categorieën van gegevens op basis van hun eventuele nut voor de nagestreefde doelstelling, of naar gelang van de betrokken personen.

B.11. Om dezelfde redenen als die welke het Hof van Justitie van de Europese Unie ertoe hebben gebracht de 'Dataretentierichtlijn' ongeldig te verklaren, dient te worden vastgesteld dat de wetgever, met de aanneming van artikel 5 van de bestreden wet, de grenzen heeft overschreden die worden opgelegd door de eerbiediging van het evenredigheidsbeginsel in het licht van de artikelen 7, 8 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie.

Het voormelde artikel 5 schendt bijgevolg de artikelen 10 en 11 van de Grondwet, in samenhang gelezen met die bepalingen. Het enige middel in de zaak nr. 5856 en het eerste middel in de zaak nr. 5859 zijn gegrond.

B.12. Wegens hun ondeelbaar karakter met artikel 5, dienen ook de artikelen 1 tot 4, 6 en 7 van de bestreden wet van 30 juli 2013, en dus de wet in haar geheel, te worden vernietigd."

1.2. De wetgever heeft aan die beide beslissingen gevolg gegeven door de wet van 29 mei 2016 'betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie' aan te nemen.[5]

[5] De afdeling Wetgeving heeft op 7 december 2015 advies 58.449/4 uitgebracht over een voorontwerp dat tot die wet van 29 mei 2016 geleid heeft, http://www.raadvst-consetat.be/dbx/adviezen/58449.pdf.

‡LW-BEHVMBJEH-GJDIBQW‡

De vernietiging van die wet is gevorderd bij vier beroepen die ingesteld zijn bij het Grondwettelijk Hof, dat bij zijn arrest nr. 96/2018 van 19 juli 2018 aan het Hof van Justitie de volgende prejudiciële vragen gesteld heeft:

"1. Dient artikel 15, lid 1, van de richtlijn 2002/58/EG, in samenhang gelezen met het recht op veiligheid, gewaarborgd bij artikel 6 van het Handvest van de grondrechten van de Europese Unie, en het recht op eerbiediging van de persoonsgegevens, zoals gewaarborgd bij de artikelen 7, 8 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, in die zin te worden geïnterpreteerd dat het zich verzet tegen een nationale regeling zoals die welke in het geding is, die voorziet in een algemene verplichting voor de operatoren en aanbieders van elektronische communicatiediensten om de verkeers- en locatiegegevens in de zin van de richtlijn 2002/58/EG, die door hen worden gegenereerd of verwerkt in het kader van het aanbieden van die diensten, te bewaren, nationale regeling die niet alleen ten doel heeft het onderzoeken, opsporen en vervolgen van feiten van zware criminaliteit, maar ook het waarborgen van de nationale veiligheid, de verdediging van het grondgebied en van de openbare veiligheid, het onderzoeken, opsporen en vervolgen van andere feiten dan die van zware criminaliteit of het voorkomen van een verboden gebruik van de elektronische communicatiesystemen, of de verwezenlijking van een andere doelstelling die is geïdentificeerd bij artikel 23, lid 1, van de Verordening (EU) 2016/679 en die bovendien onderworpen is aan nader in die regeling opgenomen waarborgen op het vlak van de bewaring van de gegevens en van de toegang ertoe?

2. Dient artikel 15, lid 1, van de richtlijn 2002/58/EG, gelezen in samenhang met de artikelen 4, 7, 8, 11 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, in die zin te worden geïnterpreteerd dat het zich verzet tegen een nationale regeling zoals die welke in het geding is, die voorziet in een algemene verplichting voor de operatoren en aanbieders van elektronische communicatiediensten om de verkeers- en locatiegegevens in de zin van de richtlijn 2002/58/EG, die door hen worden gegenereerd of verwerkt in het kader van het aanbieden van die diensten, te bewaren, indien die regeling mede tot doel heeft om de op de overheid rustende positieve verplichtingen ingevolge de artikelen 4 en 8 van het Handvest te bewerkstelligen om te voorzien in een wettelijk kader dat een effectief strafrechtelijk onderzoek en een daadwerkelijke bestraffing van seksueel misbruik van minderjarigen mogelijk maakt en het effectief mogelijk maakt om de pleger van het misdrijf te identificeren, ook wanneer gebruik wordt gemaakt van elektronische communicatiemiddelen?

3. Zou het Grondwettelijk Hof, indien het op grond van het antwoord verstrekt op de eerste of de tweede prejudiciële vraag tot de conclusie zou komen dat de bestreden wet één of meer van de uit de in die vragen vermelde bepalingen voortvloeiende verplichtingen schendt, de gevolgen van de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie tijdelijk kunnen handhaven teneinde rechtsonzekerheid te voorkomen en het mogelijk te maken dat de voorheen verzamelde en bewaarde gegevens alsnog kunnen gebruikt worden voor de door de wet beoogde doeleinden?"

In datzelfde arrest heeft het Grondwettelijk hof beslist om

"het onderzoek van de zaken voorts op [te schorten] totdat het Hof van Justitie uitspraak zal hebben gedaan in de zaken C-207/16 *Ministerio Fiscal* en C-623/17 *Privacy International / Secretary of State for Foreign and Commonwealth Affairs e.a.*".

‡LW-BEHVMBJEH-GJDIBQW‡

1.3.1. Op die prejudiciële vragen en op andere vragen die aan het Hof van Justitie voorgelegd waren door de Raad van State van Frankrijk heeft dat Hof geantwoord in een arrest dat op 6 oktober 2020 uitgesproken is in grote kamer[6] (hierna het arrest "*La Quadrature du Net*").

1.3.2. Wat de eerste twee prejudiciële vragen betreft die door het Grondwettelijk Hof gesteld zijn, heeft het Hof van Justitie zijn antwoord als volgt gemotiveerd in zijn arrest:

> "108. Wat in het bijzonder de verwerking en de opslag van verkeersgegevens door aanbieders van elektronischecommunicatiediensten betreft, blijkt uit artikel 6 en de overwegingen 22 en 26 van Richtlijn 2002/58 dat een dergelijke verwerking slechts is toegestaan voor zover en zolang dat nodig is voor de marketing en de facturering van de diensten en voor de levering van diensten met toegevoegde waarde. Zodra die periode is verstreken, moeten de verwerkte en opgeslagen gegevens worden gewist of geanonimiseerd. Wat de andere locatiegegevens dan de verkeersgegevens betreft, bepaalt artikel 9, lid 1, van Richtlijn 2002/58 dat die gegevens slechts onder bepaalde voorwaarden mogen worden verwerkt nadat zij zijn geanonimiseerd of wanneer de gebruikers of abonnees daarvoor hun toestemming hebben gegeven (arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 86 en aldaar aangehaalde rechtspraak).
>
> 109. Met de vaststelling van Richtlijn 2002/58 heeft de Uniewetgever dus de in de artikelen 7 en 8 van het Handvest neergelegde rechten geconcretiseerd, zodat de gebruikers van elektronischecommunicatiemiddelen in beginsel erop mogen vertrouwen dat hun communicatie en de daarmee verband houdende gegevens anoniem blijven en niet mogen worden vastgelegd, tenzij zij daarin hebben toegestemd.
>
> 110. Artikel 15, lid 1, van Richtlijn staat 2002/58 staat de lidstaten echter toe, te voorzien in uitzonderingen op de in artikel 5, lid 1, van deze richtlijn geformuleerde principeverplichting om de vertrouwelijkheid van de persoonsgegevens te waarborgen, en op de met name in de artikelen 6 en 9 van deze richtlijn vermelde overeenkomstige verplichtingen, indien dat in een democratische samenleving een noodzakelijke, redelijke en proportionele maatregel vormt om de nationale veiligheid, de landsverdediging en de openbare veiligheid te waarborgen, of om strafbare feiten of onbevoegd gebruik van het elektronischecommunicatiesysteem te voorkomen, te onderzoeken, op te sporen en te vervolgen. Daartoe kunnen de lidstaten onder meer wettelijke maatregelen treffen om gegevens gedurende een beperkte periode te bewaren indien dat om een van die redenen gerechtvaardigd is.
>
> 111. De mogelijkheid om af te wijken van de in de artikelen 5, 6 en 9 van Richtlijn 2002/58 vastgestelde rechten en verplichtingen kan echter niet rechtvaardigen dat de uitzondering op de principeverplichting tot waarborging van de vertrouwelijkheid van de elektronische communicatie en van de daarmee verband houdende gegevens en, in het bijzonder, op het verbod om deze gegevens op te slaan de regel wordt (zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punten 89 en 104).

[6] HvJ (grote kamer), arrest *La Quadrature du Net e. a. v. Premier ministre e.a.,* 6 oktober 2020, C-511/18, ECLI:EU:C:2020:791 en HvJ (grote kamer), arrest *French Data network e.a*., C-512/18 en HvJ (grote kamer), arrest *Ordre des barreaux francophones et germanophone e. a.*, C-520/18.

‡LW-BEHVMBJEH-GJDIBQW‡

112. Met betrekking tot de doelstellingen die een beperking van de met name in de artikelen 5, 6 en 9 van Richtlijn 2002/58 vastgestelde rechten en verplichtingen kunnen rechtvaardigen, heeft het Hof reeds geoordeeld dat de in artikel 15, lid 1, eerste zin, van deze richtlijn gegeven opsomming van doelstellingen exhaustief is, zodat een op grond van die bepaling vastgestelde wettelijke maatregel daadwerkelijk en strikt moet berusten op een van die doelstellingen (zie in die zin arrest van 2 oktober 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, punt 52 en aldaar aangehaalde rechtspraak).

113. Bovendien volgt uit artikel 15, lid 1, derde zin, van Richtlijn 2002/58 dat de lidstaten slechts wettelijke maatregelen ter beperking van de omvang van de in de artikelen 5, 6 en 9 van deze richtlijn bedoelde rechten en plichten mogen nemen voor zover deze maatregelen in overeenstemming zijn met de algemene beginselen van het Unierecht, waaronder het evenredigheidsbeginsel, en met de door het Handvest gewaarborgde grondrechten. In dit verband heeft het Hof reeds geoordeeld dat de door een lidstaat bij een nationale regeling aan aanbieders van elektronischecommunicatiediensten opgelegde verplichting om de verkeersgegevens te bewaren teneinde de bevoegde nationale autoriteiten in voorkomend geval toegang tot die gegevens te kunnen geven, niet alleen vragen doet rijzen betreffende de eerbiediging van de artikelen 7 en 8 van het Handvest, die betrekking hebben op, respectievelijk, de bescherming van het privéleven en de bescherming van persoonsgegevens, maar ook betreffende de eerbiediging van artikel 11 van het Handvest, dat betrekking heeft op de vrijheid van meningsuiting (zie in die zin arresten van 8 april 2014, *Digital Rights Ireland e.a.*, C-293/12 en C-594/12, EU:C:2014:238, punten 25 en 70, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punten 91 en 92 en aldaar aangehaalde rechtspraak).

114. Bij de uitlegging van artikel 15, lid 1, van Richtlijn 2002/58 moet derhalve zowel het belang van het door artikel 7 van het Handvest gewaarborgde recht op bescherming van het privéleven als dat van het door artikel 8 van het Handvest gewaarborgde recht op bescherming van persoonsgegevens, zoals dat blijkt uit de rechtspraak van het Hof, in aanmerking worden genomen. Hetzelfde geldt voor het recht op vrijheid van meningsuiting, aangezien dit in artikel 11 van het Handvest gewaarborgde grondrecht een van de wezenlijke grondslagen is van een democratische en pluralistische samenleving, die behoort tot de waarden waarop de Unie volgens artikel 2 VEU is gebaseerd (zie in die zin arresten van 6 maart 2001, *Connolly/Commissie*, C-274/99 P, EU:C:2001:127, punt 39, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 93 en aldaar aangehaalde rechtspraak).

115. In dit verband dient te worden gepreciseerd dat de bewaring van verkeers- en locatiegegevens als zodanig behalve een uitzondering op het in artikel 5, lid 1, van Richtlijn 2002/58 gestelde verbod op de opslag van die gegevens door anderen dan de gebruikers, ook een inmenging in de in de artikelen 7 en 8 van het Handvest verankerde grondrechten op eerbiediging van het privéleven en bescherming van persoonsgegevens vormt, waarbij niet van belang is of de gegevens betreffende het privéleven al dan niet gevoelig zijn en of de betrokkenen door die inmenging enig nadeel hebben ondervonden [zie in die zin advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punten 124 en 126 en aldaar aangehaalde rechtspraak; zie naar analogie, met betrekking tot artikel 8 EVRM, EHRM, 30 januari 2020, *Breyer tegen Duitsland*, CE:ECHR:2020:0130JUD005000112, § 81].

‡LW-BEHVMBJEH-GJDIBQW‡

116. Het is ook irrelevant of de bewaarde gegevens vervolgens al dan niet worden gebruikt (zie naar analogie, met betrekking tot artikel 8 EVRM, EHRM, 16 februari 2000, *Amann t. Zwisterland*, CE:ECHR:2000:0216JUD002779895, § 69, en 13 februari 2020, *Trjakovski en Chipovski t. Noord-Macedonië*, CE:ECHR:2020:0213JUD005320513, § 51), aangezien de toegang tot die gegevens, ongeacht het latere gebruik ervan, op zichzelf al een inmenging vormt in de in het voorgaande punt genoemde grondrechten [zie in die zin advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punten 124 en 126].

117. Deze conclusie is des te meer gerechtvaardigd daar verkeers- en locatiegegevens informatie kunnen prijsgeven over een groot aantal aspecten van het privéleven van de betrokken personen, waaronder ook gevoelige informatie, zoals seksuele geaardheid, politieke opvattingen, religieuze, filosofische, maatschappelijke of andersoortige overtuigingen en gezondheid, terwijl dergelijke gegevens bovendien in het Unierecht bijzondere bescherming genieten. Uit deze gegevens, in hun geheel beschouwd, kunnen zeer precieze conclusies worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren. In het bijzonder kan aan de hand van deze gegevens het profiel van de betrokken personen worden bepaald, informatie die vanuit het oogpunt van het recht op bescherming van het privéleven even gevoelig is als de inhoud zelf van de communicatie (zie in die zin arresten van 8 april 2014, *Digital Rights*, C-293/12 en C-594/12, EU:C:2014:238, punt 27, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 99).

118. De bewaring van verkeers- en locatiegegevens voor politiële doeleinden kan dus om te beginnen op zichzelf afbreuk doen aan het in artikel 7 van het Handvest verankerde recht op eerbiediging van communicatie en de gebruikers van elektronischecommunicatiemiddelen ontmoedigen om hun door artikel 11 van het Handvest gewaarborgde vrijheid van meningsuiting uit te oefenen (zie in die zin arresten van 8 april 2014, *Digital Rights*, C-293/12 en C-594/12, EU:C:2014:238, punt 28, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 101). Dit laatste geldt in het bijzonder voor personen van wie de communicatie naar nationaal recht onder het beroepsgeheim valt, en voor klokkenluiders van wie de activiteiten worden beschermd door Richtlijn (EU) 2019/1937 van het Europees Parlement en de Raad van 23 oktober 2019 inzake de bescherming van personen die inbreuken op het Unierecht melden (*PB* 2019, L 305, blz. 17). Dat ontmoedigende effect is bovendien des te ernstiger omdat de bewaarde gegevens talrijk en gevarieerd zijn.

119. Bovendien is het zo dat, gelet op de aanzienlijke hoeveelheid verkeers- en locatiegegevens die continu kunnen worden bewaard op grond van een algemene en ongedifferentieerde bewaringsmaatregel, en op het gevoelige karakter van de informatie die deze gegevens kunnen prijsgeven, het enkele feit dat die gegevens door aanbieders van elektronischecommunicatiediensten worden bewaard, risico's van misbruik en onrechtmatige toegang tot de gegevens inhoudt.

120. Het feit dat het de lidstaten op grond van artikel 15, lid 1, van Richtlijn 2002/58 is toegestaan om te voorzien in de in punt 110 van het onderhavige arrest bedoelde uitzonderingen, heeft ermee te maken dat de in de artikelen 7, 8 en 11 van het Handvest verankerde rechten geen absolute gelding hebben, maar moeten worden beschouwd in relatie tot hun functie in de samenleving (zie in die zin arrest van 16 juli 2020, *Facebook Ireland en Schrems*, C-311/18, EU:C:2020:559, punt 172 en aldaar aangehaalde rechtspraak).

‡LW-BEHVMBJEH-GJDIBQW‡

121. Zoals blijkt uit artikel 52, lid 1, van het Handvest, staat het Handvest immers beperkingen op de uitoefening van die rechten toe, mits deze beperkingen bij wet worden gesteld, de wezenlijke inhoud van die rechten eerbiedigen en, met inachtneming van het evenredigheidsbeginsel, noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen.

122. Bij de uitlegging van artikel 15, lid 1, van Richtlijn 2002/58 in het licht van het Handvest moet derhalve ook rekening worden gehouden met het belang van de door de artikelen 3, 4, 6 en 7 van het Handvest gewaarborgde rechten en met dat van de doelstellingen van bescherming van de nationale veiligheid en bestrijding van ernstige criminaliteit, die bijdragen tot de bescherming van de rechten en vrijheden van anderen.

123. Zo heeft ingevolge artikel 6 van het Handvest, waaraan de Conseil d'État en het Grondwettelijk Hof refereren, eenieder niet alleen recht op vrijheid, maar ook op veiligheid, en waarborgt deze bepaling rechten die overeenstemmen met die welke worden gewaarborgd door artikel 5 EVRM (zie in die zin arresten van 15 februari 2016, *N.*, C-601/15 PPU, EU:C:2016:84, punt 47; 28 juli 2016, *JZ*, C-294/16 PPU, EU:C:2016:610, punt 48, en 19 september 2019, *Rayonna prokuratura Lom*, C-467/18, EU:C:2019:765, punt 42 en aldaar aangehaalde rechtspraak).

124. Voorts zij eraan herinnerd dat artikel 52, lid 3, van het Handvest beoogt te zorgen voor de nodige samenhang tussen de in het Handvest vervatte rechten en de daarmee corresponderende, door het EVRM gewaarborgde rechten, zonder de autonomie van het Unierecht en van het Hof van Justitie van de Europese Unie aan te tasten. Bijgevolg dient bij de uitlegging van het Handvest rekening te worden gehouden met de overeenkomstige rechten van het EVRM, die het minimale beschermingsniveau bepalen [zie in die zin arresten van 12 februari 2019, *TC*, C-492/18 PPU, EU:C:2019:108, punt 57, en 21 mei 2019, *Commissie/Hongarije* (*Vruchtgebruik op landbouwgrond*), C-235/17, EU:C:2019:432, punt 72 en aldaar aangehaalde rechtspraak].

125. Artikel 5 EVRM, waarin het 'recht op vrijheid' en het 'recht op veiligheid' zijn verankerd, beoogt volgens de rechtspraak van het EHRM eenieder te beschermen tegen willekeurige en ongerechtvaardigde vrijheidsontneming (zie in die zin EHRM, 18 maart 2008, *Ladent t. Polen*, CE:ECHR:2008:0318JUD001103603, § § 45 en 46; 29 maart 2010, *Medvedyev e.a. t. Frankrijk*, CE:ECHR:2010:0329JUD000339403, § § 76 en 77, en 13 december 2012, *El-Masri t. 'The former Yugoslav Republic of Macedonia* ', CE:ECHR:2012:1213JUD003963009, § 239). Die bepaling ziet echter op vrijheidsontneming door overheidsinstanties, zodat artikel 6 van het Handvest niet aldus kan worden uitgelegd dat het de overheid een verplichting oplegt om specifieke maatregelen te nemen teneinde bepaalde strafbare handelingen tegen te gaan.

126. Wat daarentegen in het bijzonder de door het Grondwettelijk Hof genoemde effectieve bestrijding betreft van strafbare handelingen waarvan met name minderjarigen en andere kwetsbare personen het slachtoffer zijn, moet worden beklemtoond dat uit artikel 7 van het Handvest positieve verplichtingen voor de overheid kunnen voortvloeien om juridische maatregelen te nemen ter bescherming van het privéleven en het familie- en gezinsleven [zie in die zin arrest van 18 juni 2020, *Commissie/Hongarije* (*Transparantie van verenigingen*), C-78/18, EU:C:2020:476, punt 123 en aldaar aangehaalde rechtspraak van het EHRM). Dergelijke verplichtingen kunnen ook uit dat artikel voortvloeien ten aanzien van de bescherming van iemands woning en communicatie, en uit de artikelen 3 en 4 van het Handvest ten aanzien van de bescherming van iemands lichamelijke en geestelijke integriteit en het verbod op folteringen en onmenselijke en vernederende behandelingen.

‡LW-BEHVMBJEH-GJDIBQW‡

127. Gelet op die verschillende positieve verplichtingen is het noodzakelijk de diverse op het spel staande belangen en rechten met elkaar te verzoenen.

128. Het EHRM heeft namelijk geoordeeld dat de positieve verplichtingen die voortvloeien uit de artikelen 3 en 8 EVRM, waarin rechten zijn gewaarborgd die corresponderen met de in de artikelen 4 en 7 van het Handvest gewaarborgde rechten, met name impliceren dat materiële en procedurele bepalingen moeten worden vastgesteld en praktische maatregelen moeten worden genomen die het mogelijk maken om criminaliteit gericht tegen personen effectief te bestrijden door middel van doeltreffend onderzoek en doeltreffende vervolging, hetgeen des te belangrijker is wanneer het lichamelijke en geestelijke welzijn van een kind wordt bedreigd. De bevoegde autoriteiten dienen daarbij echter de wettelijk voorgeschreven procedures en de overige waarborgen die de omvang van de strafrechtelijke onderzoeksbevoegdheden beperken, alsmede de overige vrijheden en rechten volledig in acht te nemen. Met name dient er volgens het EHRM een wettelijk kader te worden ingevoerd dat het mogelijk maakt de verschillende belangen en rechten die moeten worden beschermd, met elkaar te verzoenen (EHRM, 28 oktober 1998, *Osman t. Verenigd Koninkrijk*, CE:ECHR:1998:1028JUD002345294, §§ 115 en 116; 4 maart 2004, *M.C. t. Bulgarij*e, CE:ECHR:2003:1204JUD003927298, § 151; 24 juni 2004, *Von Hannover t. Duitsland*, CE:ECHR:2004:0624JUD005932000, §§ 57 en 58, en 2 december 2008, *K.U. t. Finland*, CE:ECHR:2008:1202JUD 000287202, §§ 46, 48 en 49).

129. Wat de eerbiediging van het evenredigheidsbeginsel betreft, staat in artikel 15, lid 1, eerste zin, van Richtlijn 2002/58 te lezen dat de lidstaten een maatregel waarbij wordt afgeweken van het beginsel van vertrouwelijkheid van de communicatie en van de daarmee verband houdende verkeersgegevens kunnen treffen wanneer een dergelijke maatregel 'in een democratische samenleving noodzakelijk, redelijk en proportioneel is' in het licht van de in die bepaling genoemde doelstellingen. In overweging 11 van deze richtlijn wordt gepreciseerd dat een dergelijke maatregel 'strikt' evenredig moet zijn aan het nagestreefde doel.

130. In dit verband zij eraan herinnerd dat de bescherming van het grondrecht op eerbiediging van het privéleven volgens vaste rechtspraak van het Hof vereist dat de uitzonderingen op de bescherming van de persoonsgegevens en de beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven. Bovendien kan een doelstelling van algemeen belang niet worden nagestreefd zonder rekening te houden met het feit dat deze doelstelling moet worden verzoend met de door de maatregel aangetaste grondrechten, zulks via een evenwichtige afweging tussen de doelstelling en de op het spel staande belangen en rechten [zie in die zin arresten van 16 december 2008, *Satakunnan Markkinapörssi en Satamedia*, C-73/07, EU:C:2008:727, punt 56; 9 november 2010, *Volker und Markus Schecke en Eifert*, C-92/09 en C-93/09, EU:C:2010:662, punten 76, 77 en 86, en 8 april 2014, *Digital Rights Ireland e.a.*, C-293/12 en C-594/12, EU:C:2014:238, punt 52; advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 140].

‡LW-BEHVMBJEH-GJDIBQW‡

131. Meer bepaald volgt uit de rechtspraak van het Hof dat bij de beoordeling of de lidstaten een beperking van de omvang van de met name in de artikelen 5, 6 en 9 van Richtlijn 2002/58 bedoelde rechten en plichten kunnen rechtvaardigen, moet worden bepaald wat de ernst is van de inmenging die een dergelijke beperking meebrengt, en moet worden nagegaan of het belang van de met die beperking nagestreefde doelstelling van algemeen belang in verhouding staat tot die ernst (zie in die zin arrest van 2 oktober 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, punt 55 en aldaar aangehaalde rechtspraak).

132. Om aan het evenredigheidsvereiste te voldoen, dient een regeling duidelijke en nauwkeurige regels te bevatten over de reikwijdte en de toepassing van de betrokken maatregel, zodat degenen van wie de persoonsgegevens aan de orde zijn, over voldoende waarborgen beschikken dat die gegevens doeltreffend worden beschermd tegen het risico van misbruik. Die regeling moet wettelijk verbindend zijn naar intern recht en in het bijzonder aangeven in welke omstandigheden en onder welke voorwaarden een maatregel die voorziet in de verwerking van dergelijke gegevens kan worden genomen, en aldus waarborgen dat de inmenging tot het strikt noodzakelijke wordt beperkt. De noodzaak om over dergelijke waarborgen te beschikken is des te groter wanneer de persoonsgegevens op geautomatiseerde wijze worden verwerkt, met name wanneer er een aanzienlijk risico bestaat dat deze gegevens op onrechtmatige wijze zullen worden geraadpleegd. Deze overwegingen gelden in het bijzonder wanneer het gaat om de bescherming van een bijzondere categorie persoonsgegevens, te weten gevoelige gegevens [zie in die zin arresten van 8 april 2014, *Digital Rights Ireland e.a.*, C-293/12 en C-594/12, EU:C:2014:238, punten 54 en 55, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 117; advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 141].

133. Een regeling die voorziet in de bewaring van persoonsgegevens, moet derhalve steeds beantwoorden aan objectieve criteria die een verband leggen tussen de te bewaren gegevens en het nagestreefde doel [zie in die zin advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 191 en aldaar aangehaalde rechtspraak, en arrest van 3 oktober 2019, *A e.a.*, C-70/18, EU:C:2019:823, punt 63].

- Wettelijke maatregelen die voorzien in de preventieve bewaring van verkeers- en locatiegegevens ten behoeve van de bescherming van de nationale veiligheid

134. Het Hof heeft zich in zijn arresten betreffende de uitlegging van Richtlijn 2002/58 nog niet specifiek gebogen over de doelstelling van bescherming van de nationale veiligheid, waaraan is gerefereerd door de verwijzende rechters en de regeringen die opmerkingen hebben ingediend.

135. In dit verband moet om te beginnen worden opgemerkt dat de nationale veiligheid volgens artikel 4, lid 2, VEU tot de uitsluitende verantwoordelijkheid van elke lidstaat behoort. Deze verantwoordelijkheid strookt met het grote belang dat wordt gehecht aan de bescherming van de essentiële staatsfuncties en de fundamentele belangen van de samenleving, en omvat het voorkomen en bestrijden van activiteiten die de fundamentele constitutionele, politieke, economische of sociale structuren van een land ernstig kunnen destabiliseren en, met name, een rechtstreekse bedreiging kunnen vormen voor de samenleving, de bevolking of de staat als zodanig, zoals terroristische activiteiten.

‡LW-BEHVMBJEH-GJDIBQW‡

136. Het belang van de doelstelling van bescherming van de nationale veiligheid, gelezen in het licht van artikel 4, lid 2, VEU, overstijgt dat van de andere doelstellingen die worden genoemd in artikel 15, lid 1, van Richtlijn 2002/58, met name de doelstellingen van bestrijding van - zelfs ernstige - criminaliteit in het algemeen, en van bescherming van de openbare veiligheid. Bedreigingen als die waaraan in het voorgaande punt wordt gerefereerd, verschillen door hun aard en hun bijzondere ernst immers van het algemene risico dat zich - zelfs ernstige - spanningen of wanordelijkheden zullen voordoen die de openbare veiligheid ondermijnen. Mits aan de overige in artikel 52, lid 1, van het Handvest geformuleerde vereisten wordt voldaan, kan de doelstelling van bescherming van de nationale veiligheid derhalve maatregelen rechtvaardigen die ernstigere inmengingen in de grondrechten met zich brengen dan die welke door die andere doelstellingen zouden kunnen worden gerechtvaardigd.

137. In situaties als die welke in de punten 135 en 136 van het onderhavige arrest zijn beschreven, verzet artikel 15, lid 1, van Richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, zich derhalve in beginsel niet tegen een wettelijke maatregel op grond waarvan de bevoegde autoriteiten aan aanbieders van elektronischecommunicatiediensten een bevel kunnen opleggen om de verkeers- en locatiegegevens van alle gebruikers van elektronischecommunicatiemiddelen gedurende een beperkte periode te bewaren, wanneer er voldoende concrete aanwijzingen zijn dat de betrokken lidstaat wordt geconfronteerd met een ernstige bedreiging van de nationale veiligheid als bedoeld in de punten 135 en 136 van het onderhavige arrest, en die bedreiging werkelijk en actueel of voorzienbaar is. Ook al heeft een dergelijke maatregel zonder onderscheid betrekking op alle gebruikers van elektronischecommunicatiemiddelen, zonder dat er op het eerste gezicht enig verband in de zin van de in punt 133 van het onderhavige arrest bedoelde rechtspraak tussen die gebruikers en een bedreiging voor de nationale veiligheid van de betrokken lidstaat lijkt te bestaan, geoordeeld moet worden dat het bestaan van een dergelijke bedreiging op zichzelf dat verband aantoont.

138. Het bevel om preventief de gegevens te bewaren van alle gebruikers van elektronischecommunicatiemiddelen, mag echter slechts worden opgelegd voor een periode die niet langer is dan strikt noodzakelijk. Het valt weliswaar niet uit te sluiten dat het aan aanbieders van elektronischecommunicatiemiddelen opgelegde bevel tot bewaring van die gegevens kan worden verlengd wegens het voortduren van een dergelijke bedreiging, maar dit neemt niet weg dat elk bevel slechts mag worden gegeven voor een voorzienbare periode. Een dergelijke gegevensbewaring moet bovendien zijn onderworpen aan beperkingen en zijn omgeven met strikte waarborgen die ervoor zorgen dat de persoonsgegevens van de betrokken personen doeltreffend worden beschermd tegen het risico van misbruik. Die bewaring mag derhalve geen stelselmatig karakter hebben.

139. Gelet op de ernst van de inmenging in de in de artikelen 7 en 8 van het Handvest verankerde grondrechten die een dergelijke algemene en ongedifferentieerde bewaring van gegevens met zich brengt, dient te worden gewaarborgd dat de toepassing van die maatregel daadwerkelijk beperkt blijft tot situaties waarin de nationale veiligheid ernstig wordt bedreigd, zoals de in de punten 135 en 136 van het onderhavige arrest bedoelde situaties. Daartoe is het van wezenlijk belang dat een beslissing waarbij aan aanbieders van elektronischecommunicatiediensten een bevel tot een dergelijke gegevensbewaring wordt opgelegd, effectief kan worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij het doel van die toetsing is om na te gaan of een van die situaties zich voordoet en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien.

‡LW-BEHVMBJEH-GJDIBQW‡

- Wettelijke maatregelen die voorzien in de preventieve bewaring van verkeers- en locatiegegevens ten behoeve van de bestrijding van criminaliteit en de bescherming van de openbare veiligheid

140. Als het gaat om de doelstelling strafbare feiten te voorkomen, te onderzoeken, op te sporen en te vervolgen, kunnen overeenkomstig het evenredigheidsbeginsel enkel de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen voor de openbare veiligheid een rechtvaardiging vormen voor ernstige inmengingen in de in de artikelen 7 en 8 van het Handvest verankerde grondrechten, zoals die welke voortvloeien uit de bewaring van verkeers- en locatiegegevens. De doelstelling strafbare feiten in het algemeen te voorkomen, te onderzoeken, op te sporen en te vervolgen, kan derhalve enkel niet-ernstige inmengingen in die grondrechten rechtvaardigen [zie in die zin arresten van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 102, en 2 oktober 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, punten 56 en 57; advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 149].

141. Een nationale regeling die voorziet in de algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens ten behoeve van de bestrijding van zware criminaliteit, gaat verder dan strikt noodzakelijk is en kan niet worden beschouwd als een regeling die in een democratische samenleving gerechtvaardigd is, zoals artikel 15, lid 1, van Richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, eist (zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 107).

142. Gezien het gevoelige karakter van de informatie die verkeers- en locatiegegevens kunnen prijsgeven, is de vertrouwelijkheid van deze gegevens immers essentieel voor het recht op eerbiediging van het privéleven. Mede gelet op het in punt 118 van het onderhavige arrest bedoelde ontmoedigende effect dat de bewaring van die gegevens kan hebben op de uitoefening van de in de artikelen 7 en 11 van het Handvest verankerde grondrechten, en op de ernst van de inmenging die een dergelijke bewaring met zich brengt, is het in een democratische samenleving dan ook van belang dat deze bewaring, zoals het bij Richtlijn 2002/58 ingevoerde stelsel eist, de uitzondering en niet de regel vormt en dat de betrokken gegevens niet stelselmatig en continu kunnen worden bewaard. Deze conclusie geldt zelfs met betrekking tot de doelstellingen van bestrijding van zware criminaliteit en voorkoming van ernstige bedreigingen voor de openbare veiligheid en het belang dat aan deze doelstellingen moet worden toegekend.

143. Voorts heeft het Hof benadrukt dat een regeling die voorziet in de algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens, de elektronische communicatie van vrijwel de gehele bevolking bestrijkt, zonder dat enig onderscheid wordt gemaakt, enige beperking wordt gesteld of enige uitzondering wordt gemaakt op basis van het met de regeling beoogde doel. Een dergelijke regeling betreft algemeen alle personen die gebruikmaken van elektronischecommunicatiediensten, zonder dat die personen zich - zelfs maar indirect - in een situatie bevinden die aanleiding kan zijn om strafvervolging in te stellen, wat in strijd is met het in punt 133 van het onderhavige arrest in herinnering gebrachte vereiste. Zij is dus zelfs van toepassing op personen voor wie er geen enkele aanwijzing bestaat dat hun gedrag - zelfs maar indirect of van ver - verband houdt met die doelstelling van bestrijding van zware misdrijven, en vereist met name niet dat er een verband is tussen de te bewaren gegevens en een bedreiging voor de openbare veiligheid (zie in die zin arresten van 8 april 2014, *Digital Rights*, C-293/12 en C-594/12, EU:C:2014:238, punten 57 en 58, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 105).

‡LW-BEHVMBJEH-GJDIBQW‡

144. Zoals het Hof reeds heeft geoordeeld, beperkt een dergelijke regeling met name de bewaring niet tot gegevens die betrekking hebben op een bepaalde periode en/of een bepaalde geografische zone en/of een kring van bepaalde personen die op een of andere wijze betrokken kunnen zijn bij zware criminaliteit, of op personen voor wie de bewaring van de gegevens om andere redenen zou kunnen helpen bij het bestrijden van zware criminaliteit (zie in die zin arresten van 8 april 2014, *Digital Rights*, C-293/12 en C-594/12, EU:C:2014:238, punt 59, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 106).

145. Zelfs de positieve verplichtingen die, naargelang van het geval, voor de lidstaten kunnen voortvloeien uit de artikelen 3, 4 en 7 van het Handvest en, zoals in de punten 126 en 128 van het onderhavige arrest is opgemerkt, betrekking hebben op de invoering van regels die een effectieve bestrijding van strafbare feiten mogelijk maken, kunnen geen inmengingen rechtvaardigen die zo ernstig zijn als de inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten van vrijwel de gehele bevolking die een regeling die voorziet in de bewaring van verkeers- en locatiegegevens met zich brengt, zonder dat de gegevens van de betrokken personen, althans indirect, een verband met het nagestreefde doel aan het licht kunnen brengen.

146. Daarentegen kunnen, overeenkomstig hetgeen in de punten 142 tot en met 144 van het onderhavige arrest is vastgesteld, en gelet op de noodzaak om de op het spel staande rechten en belangen met elkaar te verzoenen, de doelstellingen van bestrijding van zware criminaliteit, voorkoming van ernstige bedreigingen voor de openbare veiligheid en, *a fortiori*, bescherming van de nationale veiligheid - gezien het belang ervan in het licht van de in het voorgaande punt in herinnering gebrachte positieve verplichtingen waaraan met name het Grondwettelijk Hof heeft gerefereerd - de bijzonder ernstige inmenging rechtvaardigen die een gerichte bewaring van verkeers- en locatiegegevens met zich brengt.

147. Zoals het Hof reeds heeft geoordeeld, staat artikel 15, lid 1, van Richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, derhalve niet eraan in de weg dat een lidstaat een regeling vaststelt op grond waarvan verkeers- en locatiegegevens preventief gericht kunnen worden bewaard ten behoeve van de bestrijding van zware criminaliteit, de voorkoming van ernstige bedreigingen voor de openbare veiligheid en de bescherming van de nationale veiligheid, op voorwaarde dat die bewaring, wat de categorieën te bewaren gegevens, de betrokken communicatiemiddelen, de betrokken personen en de duur van de bewaring betreft, tot het strikt noodzakelijke wordt beperkt (zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 108).

148. De noodzakelijke afbakening van een dergelijke gegevensbewaringsmaatregel kan met name worden verricht aan de hand van de categorieën betrokken personen, aangezien artikel 15, lid 1, van Richtlijn 2002/58 zich niet verzet tegen een regeling die is gebaseerd op objectieve factoren waarmee kan worden gemikt op de personen van wie de verkeers- en locatiegegevens, althans indirect, een verband met ernstige strafbare feiten aan het licht kunnen brengen, waarmee op de een of andere wijze kan worden bijgedragen tot de bestrijding van zware criminaliteit of waarmee een ernstig risico voor de openbare veiligheid of een risico voor de nationale veiligheid kan worden voorkomen (zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 111).

‡LW-BEHVMBJEH-GJDIBQW‡

149. In dit verband moet worden gepreciseerd dat de personen op wie aldus wordt gemikt, met name diegenen kunnen zij[n] die eerder in het kader van de toepasselijke nationale procedures en op basis van objectieve factoren zijn geïdentificeerd als personen die een bedreiging vormen voor de openbare veiligheid of de nationale veiligheid van de betrokken lidstaat.

150. Een maatregel die voorziet in de bewaring van verkeers- en locatiegegevens, kan ook worden afgebakend aan de hand van een geografisch criterium wanneer de bevoegde nationale autoriteiten op basis van objectieve factoren van mening zijn dat er in een of meer geografische gebieden sprake is van een situatie die wordt gekenmerkt door een hoog risico dat zware misdrijven worden voorbereid of gepleegd (zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 111). Het kan daarbij met name gaan om plekken waar veel zware criminaliteit plaatsvindt, om plaatsen waar er een verhoogd risico is op zware misdrijven, zoals plekken of faciliteiten die regelmatig door een zeer groot aantal personen worden bezocht, of om strategische plekken, zoals vliegvelden, stations of tolzones.

151. Om ervoor te zorgen dat de inmenging die de in de punten 147 tot en met 150 van het onderhavige arrest beschreven maatregelen inzake gerichte gegevensbewaring met zich brengen, in overeenstemming is met het evenredigheidsbeginsel, mogen die maatregelen niet langer gelden dan strikt noodzakelijk is in het licht van het ermee beoogde doel en van de omstandigheden waardoor zij worden gerechtvaardigd, met dien verstande dat zij eventueel kunnen worden verlengd mocht de noodzaak van een dergelijke bewaring blijven bestaan.

- *Wettelijke maatregelen die voorzien in de preventieve bewaring van IP-adressen en gegevens inzake de burgerlijke identiteit ten behoeve van de bestrijding van criminaliteit en de bescherming van de openbare veiligheid*

152. Opgemerkt dient te worden dat IP-adressen weliswaar behoren tot de verkeersgegevens, maar los van een bepaalde communicatie worden gegenereerd en primair dienen om via de aanbieders van elektronischecommunicatiediensten de natuurlijke persoon te identificeren die eigenaar is van een eindapparaat waarvandaan via het internet wordt gecommuniceerd. Voor zover bij e-mailverkeer en internettelefonie uitsluitend de IP-adressen van de bron van de communicatie en niet die van de ontvanger ervan worden bewaard, geven die adressen als zodanig geen enkele informatie prijs over de derden die in contact zijn geweest met de persoon die aan de basis ligt van de communicatie. Deze categorie gegevens is dan ook van mindere gevoelige aard dan de andere verkeersgegevens.

153. Aangezien IP-adressen echter onder meer kunnen worden gebruikt om de volledige zoekgeschiedenis van een internetgebruiker te traceren en dus om een volledig beeld te krijgen van diens online activiteit, kan aan de hand van die gegevens een gedetailleerd profiel van de betrokkene worden opgesteld. De voor een dergelijke tracking noodzakelijke bewaring en analyse van IP-adressen vormen dan ook ernstige inmengingen in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten van de internetgebruiker, die een ontmoedigend effect als bedoeld in punt 118 van het onderhavige arrest kunnen hebben.

154. Om de op het spel staande rechten en belangen met elkaar te verzoenen, zoals de in punt 130 van het onderhavige arrest aangehaalde rechtspraak verlangt, moet echter in aanmerking worden genomen dat in het geval van een online gepleegd strafbaar feit het IP-adres het enige onderzoeksmiddel kan zijn met behulp waarvan de persoon kan worden geïdentificeerd aan wie dat adres was toegewezen op het moment waarop dat feit werd gepleegd. Bovendien lijkt de bewaring van IP-adressen door aanbieders van elektronischecommunicatiediensten na afloop van de periode waarvoor deze adressen

‡LW-BEHVMBJEH-GJDIBQW‡

werden toegewezen, in beginsel niet noodzakelijk te zijn met het oog op de facturering van die diensten, met als gevolg dat, zoals verschillende regeringen hebben aangevoerd in de door hen bij het Hof ingediende opmerkingen, het opsporen van online gepleegde strafbare feiten onmogelijk kan blijken zonder gebruik te maken van een wettelijke maatregel als bedoeld in artikel 15, lid 1, van Richtlijn 2002/58. Zoals die regeringen hebben betoogd, kan dit met name het geval zijn bij zeer ernstige strafbare feiten op het gebied van kinderpornografie, zoals het online verwerven, verspreiden, uitzenden of ter beschikking stellen van kinderpornografie in de zin van artikel 2, onder *c)*, van richtlijn 2011/93/EU van het Europees Parlement en de Raad van 13 december 2011 ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie, en ter vervanging van kaderbesluit 2004/68/JBZ van de Raad (*PB* 2011, L 335, blz. 1).

155. In deze omstandigheden moet worden vastgesteld dat, ook al zou een wettelijke maatregel die voorziet in de bewaring van de IP-adressen van alle natuurlijke personen die eigenaar zijn van eindapparatuur die internettoegang mogelijk maakt, personen betreffen bij wie op het eerste gezicht een verband met de nagestreefde doelstellingen in de zin van de in punt 133 van het onderhavige arrest aangehaalde rechtspraak ontbreekt, en ook al moeten internetgebruikers, zoals in punt 109 van het onderhavige arrest is vastgesteld, op grond van de artikelen 7 en 8 van het Handvest erop kunnen vertrouwen dat hun identiteit in beginsel niet wordt onthuld, een wettelijke maatregel die voorziet in de algemene en ongedifferentieerde bewaring van uitsluitend de aan de bron van een verbinding toegewezen IP-adressen, in beginsel niet in strijd is met artikel 15, lid 1, van Richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, voor zover die mogelijkheid afhankelijk wordt gesteld van de strikte naleving van de materiële en procedurele voorwaarden die het gebruik van die gegevens dienen te regelen.

156. Gelet op het feit dat die bewaring een ernstige inmenging inhoudt in de grondrechten die zijn verankerd in de artikelen 7 en 8 van het Handvest, kunnen enkel de bestrijding van zware criminaliteit en het voorkomen van ernstige bedreigingen van de openbare veiligheid, alsmede de bescherming van de nationale veiligheid, die inmenging rechtvaardigen. Bovendien mag de bewaartermijn niet langer zijn dan strikt noodzakelijk is gelet op het nagestreefde doel. Tot slot moet een dergelijke maatregel voorzien in strikte voorwaarden en waarborgen met betrekking tot het gebruik van die gegevens, met name in de vorm van het in kaart brengen van de online communicatie en de online activiteiten van de betrokken personen.

157. Wat ten slotte de gegevens betreffende de burgerlijke identiteit van de gebruikers van elektronischecommunicatiemiddelen betreft, moet worden opgemerkt dat met die gegevens alleen noch de datum, het tijdstip, de duur en de ontvangers van de communicatie kunnen worden achterhaald, noch de plaats waar die communicatie heeft plaatsgevonden of het aantal malen dat in een specifieke periode met bepaalde personen is gecommuniceerd. Die gegevens verschaffen dus, afgezien van de contactgegevens van de betrokken gebruikers, zoals hun adres, geen informatie over wat die personen hebben gecommuniceerd en dus over hun privéleven. De inmenging die de bewaring van die gegevens met zich brengt, kan derhalve niet als 'ernstig' worden aangemerkt (zie in die zin arrest van 2 oktober 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, punten 59 en 60).

158. Hieruit volgt dat, overeenkomstig hetgeen is uiteengezet in punt 140 van het onderhavige arrest, wettelijke maatregelen die betrekking hebben op de verwerking van die gegevens als zodanig, in het bijzonder op de bewaring van en de toegang tot die gegevens met als enige doel de betrokken gebruiker te identificeren, zonder dat de gegevens in verband kunnen worden gebracht met informatie over de tot stand gebrachte

‡LW-BEHVMBJEH-GJDIBQW‡

communicatie, kunnen worden gerechtvaardigd door de in artikel 15, lid 1, eerste zin, van [de] richtlijn genoemde doelstelling strafbare feiten in het algemeen te voorkomen, te onderzoeken, op te sporen en te vervolgen (zie in die zin arrest van 2 oktober 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, punt 62).

159. Gelet op de noodzaak om de op het spel staande rechten en belangen met elkaar te verzoenen, moet in deze omstandigheden om de in de punten 131 en 158 van het onderhavige arrest uiteengezette redenen worden geoordeeld dat, ook al bestaat er geen verband tussen alle gebruikers van elektronischecommunicatiemiddelen en de nagestreefde doelstellingen, artikel 15, lid 1, van Richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 2, van het Handvest, zich niet verzet tegen een wettelijke maatregel op grond waarvan aanbieders van elektronischecommunicatiediensten verplicht zijn om de gegevens inzake de burgerlijke identiteit van alle gebruikers van elektronischecommunicatiemiddelen gedurende een niet nader bepaalde periode te bewaren ten behoeve van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten en het waarborgen van de openbare veiligheid, zonder dat het daarbij hoeft te gaan om ernstige strafbare feiten of om ernstige bedreigingen en verstoringen van de openbare veiligheid.

- *Wettelijke maatregelen die voorzien in de spoedbewaring van verkeers- en locatiegegevens ten behoeve van de bestrijding van zware criminaliteit*

160. Met betrekking tot de verkeers- en locatiegegevens die door aanbieders van elektronischecommunicatiediensten worden verwerkt en opgeslagen op grond van de artikelen 5, 6 en 9 van Richtlijn 2002/58 dan wel op grond van krachtens artikel 15, lid 1, van deze richtlijn vastgestelde wettelijke maatregelen als beschreven in de punten 134 tot en met 159 van het onderhavige arrest, dient te worden opgemerkt dat deze gegevens in beginsel moeten worden gewist of geanonimiseerd na het verstrijken van de wettelijke termijnen waarbinnen zij overeenkomstig de nationale bepalingen tot omzetting van die Richtlijn moeten worden verwerkt en opgeslagen.

161. Gedurende die verwerking en opslag kunnen zich evenwel situaties voordoen die het noodzakelijk maken om de betrokken gegevens ook na het verstrijken van die termijnen te bewaren teneinde ernstige strafbare feiten of verstoringen van de nationale veiligheid op te helderen, en dit niet alleen wanneer die feiten of verstoringen reeds konden worden vastgesteld, maar ook wanneer er na een objectief onderzoek van alle relevante omstandigheden een redelijk vermoeden bestaat dat dergelijke feiten zijn gepleegd of dat de nationale veiligheid wordt bedreigd.

162. In dit verband zij erop gewezen dat het op 23 november 2001 onder auspiciën van de Raad van Europa gesloten Cybercrimeverdrag (Serie Europese Verdragen - nr. 185), dat door alle 27 lidstaten is ondertekend en door 25 lidstaten is geratificeerd, en dat tot doel heeft de bestrijding van door middel van een computersysteem begane strafbare feiten te vergemakkelijken, in artikel 14 bepaalt dat de verdragsluitende partijen ten behoeve van specifieke strafrechtelijke onderzoeken of procedures bepaalde maatregelen moeten nemen met betrekking tot reeds opgeslagen verkeersgegevens, zoals de spoedbewaring van die gegevens. Met name is in artikel 16, lid 1, van dit verdrag bepaald dat de verdragsluitende partijen de wetgevende en andere maatregelen moeten nemen die nodig zijn om hun bevoegde autoriteiten in staat te stellen de spoedbewaring te bevelen of op soortgelijke wijze de spoedbewaring te bewerkstelligen van verkeersgegevens die zijn opgeslagen door middel van een computersysteem, in het bijzonder wanneer er redenen zijn om te vermoeden dat die gegevens vatbaar zijn voor verlies of wijziging.

‡LW-BEHVMBJEH-GJDIBQW‡

163. In een situatie als bedoeld in punt 161 van het onderhavige arrest staat het de lidstaten, gelet op de in punt 130 van het onderhavige arrest genoemde noodzaak om de op het spel staande rechten en belangen met elkaar te verzoenen, vrij om in een op grond van artikel 15, lid 1, van Richtlijn 2002/58 vastgestelde wettelijke regeling te voorzien in de mogelijkheid om via een aan effectieve rechterlijke toetsing onderworpen beslissing van de bevoegde autoriteit aan aanbieders van elektronischecommunicatiediensten een bevel op te leggen tot spoedbewaring van de in hun handen zijnde verkeers- en locatiegegevens gedurende een bepaalde periode.

164. Aangezien het doel van een dergelijke spoedbewaring niet meer overeenkomt met de doelen waarvoor de gegevens oorspronkelijk zijn vergaard en bewaard, en aangezien ingevolge artikel 8, lid 2, van het Handvest iedere verwerking van gegevens bepaalde doelen moet dienen, moeten de lidstaten in hun wetgeving duidelijk maken voor welk doel spoedbewaring van gegevens mogelijk is. Gelet op het feit dat een dergelijke bewaring een ernstige inmenging inhoudt in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten, kunnen enkel de bestrijding van zware criminaliteit en, *a fortiori*, de bescherming van de nationale veiligheid die inmenging rechtvaardigen. Om ervoor te zorgen dat de inmenging die een dergelijke maatregel met zich brengt, tot het strikt noodzakelijke wordt beperkt, moet bovendien om te beginnen de bewaarplicht uitsluitend gelden voor verkeers- en locatiegegevens die kunnen helpen bij het ophelderen van het betrokken ernstige strafbare feit of de betrokken verstoring van de nationale veiligheid. Bovendien mag de bewaartermijn niet langer zijn dan strikt noodzakelijk, zij het dat die termijn kan worden verlengd wanneer de omstandigheden en het met de betrokken maatregel beoogde doel dit rechtvaardigen.

165. In dit verband moet worden gepreciseerd dat een dergelijke spoedbewaring niet moet worden beperkt tot de gegevens van personen op wie een concrete verdenking rust dat zij een strafbaar feit hebben gepleegd of de nationale veiligheid in gevaar hebben gebracht. Mits daarbij het kader in acht wordt genomen dat is ingesteld bij artikel 15, lid 1, van Richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, en gelet op de overwegingen in punt 133 van het onderhavige arrest, kan een dergelijke maatregel naar keuze van de wetgever en binnen de grenzen van het strikt noodzakelijke worden uitgebreid tot verkeers- en locatiegegevens die betrekking hebben op andere personen dan die welke ervan worden verdacht een ernstig misdrijf of handelingen die een gevaar vormen voor de nationale veiligheid te hebben voorbereid of gepleegd, op voorwaarde dat op basis van objectieve en niet-discriminatoire factoren kan worden geoordeeld dat die gegevens kunnen helpen bij het ophelderen van een dergelijk misdrijf of een dergelijke verstoring van de nationale veiligheid. In dit verband kan bijvoorbeeld worden gedacht aan de gegevens van het slachtoffer van het misdrijf of van personen uit de sociale of professionele omgeving van de betrokkene, of aan de gegevens betreffende bepaalde geografische gebieden, zoals de plaatsen waar het misdrijf of de handeling die een gevaar heeft gevormd voor de nationale veiligheid, is voorbereid of gepleegd. Bovendien moet aan de bevoegde autoriteiten toegang tot de aldus bewaarde gegevens worden verleend met inachtneming van de voorwaarden die voortvloeien uit de arresten waarin Richtlijn 2002/58 is uitgelegd (zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punten 118-121 en aldaar aangehaalde rechtspraak).

166. Hieraan moet nog worden toegevoegd dat, zoals met name uit de punten 115 en 133 van het onderhavige arrest volgt, de toegang tot verkeers- en locatiegegevens die door aanbieders van elektronischecommunicatiediensten worden bewaard op grond van een krachtens artikel 15, lid 1, van Richtlijn 2002/58 vastgestelde maatregel, in beginsel enkel kan worden gerechtvaardigd door de doelstelling van algemeen belang met het oog waarop de verplichting tot bewaring van die gegevens aan die aanbieders is opgelegd.

‡LW-BEHVMBJEH-GJDIBQW‡

Hieruit volgt met name dat in geen geval toegang tot dergelijke gegevens mag worden verleend met het oog op de vervolging en bestraffing van een gewoon strafbaar feit, wanneer de bewaring van die gegevens haar rechtvaardiging vindt in de doelstelling van bestrijding van zware criminaliteit of, a fortiori, de doelstelling van bescherming van de nationale veiligheid. Overeenkomstig het evenredigheidsbeginsel zoals dit is verduidelijkt in punt 131 van het onderhavige arrest, kan daarentegen de toegang tot gegevens die zijn bewaard met het oog op de bestrijding van zware criminaliteit, worden gerechtvaardigd door de doelstelling van bescherming van de nationale veiligheid, [mits] de in het voorgaande punt bedoelde materiële en procedurele voorwaarden voor een dergelijke toegang in acht worden genomen.

167. In zoverre staat het de lidstaten vrij om in hun wetgeving te bepalen dat met inachtneming van diezelfde materiële en procedurele voorwaarden toegang tot verkeers- en locatiegegevens kan worden verleend met het oog op de bestrijding van zware criminaliteit of de bescherming van de nationale veiligheid, wanneer die gegevens door een aanbieder zijn bewaard in overeenstemming met de artikelen 5, 6 en 9 of met artikel 15, lid 1, van Richtlijn 2002/58."

Met betrekking tot de eerste en de tweede prejudiciële vraag die het Grondwettelijk Hof aan het Hof van Justitie voorgelegd had, heeft dat Hof in het *dictum* van dat arrest voor recht verklaard:

"Artikel 15, lid 1, van Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), zoals gewijzigd bij Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, moet aldus worden uitgelegd dat het zich verzet tegen wettelijke maatregelen die voor de in die bepaling genoemde doeleinden preventief voorzien in een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens. Artikel 15, lid 1, van Richtlijn 2002/58, zoals gewijzigd bij Richtlijn 2009/136, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten, verzet zich daarentegen niet tegen wettelijke maatregelen

– die het mogelijk maken om ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronischecommunicatiediensten een bevel tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens op te leggen in situaties waarin de betrokken lidstaat wordt geconfronteerd met een werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid, wanneer de beslissing waarbij dat bevel wordt opgelegd, effectief kan worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij het doel van die toetsing is om na te gaan of een van die situaties zich voordoet en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien, en wanneer dat bevel slechts kan worden opgelegd voor een periode die niet langer is dan strikt noodzakelijk, maar die kan worden verlengd indien die bedreiging voortduurt;

– die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een gerichte bewaring van verkeers- en locatiegegevens, die op basis van objectieve en niet-discriminatoire factoren wordt afgebakend aan de hand van categorieën betrokken personen of aan de hand van een geografisch criterium, voor een periode die niet langer is dan strikt noodzakelijk, maar die kan worden verlengd;

‡LW-BEHVMBJEH-GJDIBQW‡

– die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de IP-adressen die zijn toegewezen aan de bron van een verbinding, voor een periode die niet langer is dan strikt noodzakelijk;

– die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van criminaliteit en de bescherming van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronischecommunicatiemiddelen, en

– die het mogelijk maken om ten behoeve van de bestrijding van zware criminaliteit en, *a fortiori*, de bescherming van de nationale veiligheid via een aan effectieve rechterlijke toetsing onderworpen beslissing van de bevoegde autoriteit aan aanbieders van elektronischecommunicatiediensten een bevel op te leggen tot spoedbewaring van de in hun handen zijnde verkeers- en locatiegegevens gedurende een bepaalde periode,

mits die maatregelen, door het gebruik van duidelijke en nauwkeurige regels, verzekeren dat de betrokken gegevens slechts worden bewaard indien aan de daarvoor geldende materiële en procedurele voorwaarden wordt voldaan, en dat de betrokken personen beschikken over effectieve waarborgen tegen het risico van misbruik. [...]"

1.3.3. Met betrekking tot de derde prejudiciële vraag van het Grondwettelijk Hof heeft het Hof van Justitie voor recht verklaard:

"Een nationale rechterlijke instantie mag geen bepaling van haar nationale recht toepassen die haar machtigt om de werking in de tijd te beperken van de door haar op grond van dit recht uit te spreken onwettigverklaring van een nationale wettelijke regeling waarbij ten behoeve van met name de bescherming van de nationale veiligheid en de bestrijding van criminaliteit aan aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens wordt opgelegd die onverenigbaar is met artikel 15, lid 1, van Richtlijn 2002/58, zoals gewijzigd bij Richtlijn 2009/136, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten. Op grond van artikel 15, lid 1, uitgelegd in het licht van het doeltreffendheidsbeginsel, dient de nationale strafrechter informatie en bewijzen die door middel van een met het Unierecht onverenigbare algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens zijn verkregen, in het kader van een strafrechtelijke procedure tegen personen die worden verdacht van strafbare handelingen buiten beschouwing te laten indien die personen niet in de gelegenheid zijn om doeltreffend commentaar te leveren op die informatie en die bewijzen, die betrekking hebben op een gebied waarvan de rechter geen kennis heeft en een doorslaggevende invloed kunnen hebben op de beoordeling van de feiten."

1.4. Naar aanleiding van arrest *La Quadrature du Net* van het Hof van Justitie heeft het Grondwettelijk Hof zich in zijn arrest nr. 57/2021 van 22 april 2021 uitgesproken over de beroepen die gericht waren tegen de wet van 29 mei 2016.

‡LW-BEHVMBJEH-GJDIBQW‡

1.4.1. In dat arrest citeert het Grondwettelijk Hof eerst twee andere beslissingen van het Hof van Justitie, namelijk:

1° het arrest van 2 oktober 2018 in zake *Ministerio Fiscal* (C-207/16) (hierna het arrest *Ministerio Fiscal*), waarin het Hof van Justitie voor recht verklaard heeft:

> "Artikel 15, lid 1, van Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), zoals gewijzigd bij Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009, gelezen in samenhang met de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie, moet aldus worden uitgelegd dat de toegang van overheidsinstanties tot de identificatiegegevens van houders van met een gestolen mobiele telefoon geactiveerde simkaarten - zoals hun naam, voornaam en, in voorkomend geval, adres - geen zodanig ernstige inmenging in de door die artikelen van het Handvest gewaarborgde grondrechten van laatstgenoemden oplevert dat die toegang – op het gebied van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten – moet worden beperkt tot de bestrijding van zware criminaliteit."

In dat arrest heeft het Hof van Justitie voor zijn beslissing op volgende overwegingen gesteund:

> "Ten gronde
>
> 48. Met zijn twee vragen, die samen moeten worden onderzocht, wenst de verwijzende rechter in wezen te vernemen of artikel 15, lid 1, van Richtlijn 2002/58, gelezen in samenhang met de artikelen 7 en 8 van het Handvest, aldus moet worden uitgelegd dat de toegang van overheidsinstanties tot de identificatiegegevens van de houders van met een gestolen mobiele telefoon geactiveerde simkaarten - zoals hun naam, voornaam en, in voorkomend geval, adres - een zodanig ernstige inmenging in de door die artikelen van het Handvest gewaarborgde grondrechten van deze laatsten vormt dat die toegang, wat het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten betreft, zou moeten worden beperkt tot de bestrijding van zware criminaliteit en, zo ja, aan de hand van welke criteria de ernst van het betrokken delict moet worden beoordeeld.
>
> 49. In dit verband blijkt uit de verwijzingsbeslissing dat, zoals de advocaat-generaal in punt 38 van zijn conclusie in wezen heeft opgemerkt, het verzoek om een prejudiciële beslissing er niet toe strekt om uit te maken of de aanbieders van elektronische-communicatiediensten de in het hoofdgeding aan de orde zijnde persoonsgegevens hebben bewaard met inachtneming van de voorwaarden van artikel 15, lid 1, van Richtlijn 2002/58, gelezen in samenhang met de artikelen 7 en 8 van het Handvest. Zoals uit punt 46 van het onderhavige arrest blijkt, betreft het verzoek uitsluitend de vraag of en in welke mate het doel dat met de in het hoofdgeding aan de orde zijnde nationale regeling wordt nagestreefd, kan rechtvaardigen dat overheidsinstanties zoals de gerechtelijke politie toegang hebben tot dergelijke gegevens, en gaat het verzoek niet over de andere toegangsvoorwaarden die uit voormeld artikel 15, lid 1, voortvloeien.
>
> 50. De verwijzende rechter vraagt zich in het bijzonder af welke elementen in aanmerking moeten worden genomen bij de beoordeling of delicten waarvoor politiediensten in het kader van een onderzoek toegang kan worden verleend tot persoonsgegevens die door aanbieders van elektronische-communicatiediensten worden bewaard, voldoende ernstig zijn om de inmenging die een dergelijke toegang betekent in

‡LW-BEHVMBJEH-GJDIBQW‡

de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten, zoals uitgelegd door het Hof in zijn arrest van 8 april 2014, Digital Rights Ireland e.a. (C-293/12 en C-594/12, EU:C:2014:238), en in het arrest Tele2 Sverige en Watson e.a., te rechtvaardigen.

51. Wat betreft de vraag of sprake is van inmenging in die grondrechten, zij eraan herinnerd dat, zoals de advocaat-generaal in de punten 76 en 77 van zijn conclusie heeft aangegeven, de toegang van overheidsinstanties tot dergelijke gegevens inmenging in het in artikel 7 van het Handvest neergelegde grondrecht op eerbiediging van het privéleven vormt, zelfs al kan die inmenging om bepaalde redenen niet als 'ernstig' worden aangemerkt en zonder dat van belang is of de informatie over het privéleven al dan niet gevoelig is en of de betrokkenen door die inmenging enig nadeel hebben ondervonden. Een dergelijke toegang vormt tevens inmenging in het door artikel 8 van het Handvest gewaarborgde grondrecht op bescherming van persoonsgegevens, aangezien die toegang een verwerking van persoonsgegevens is [zie in die zin advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punten 124 en 126 en aldaar aangehaalde rechtspraak].

52. Wat betreft de doelstellingen die een rechtvaardiging kunnen vormen voor een nationale regeling als die in het hoofdgeding, die de toegang van overheidsinstanties tot door aanbieders van elektronische-communicatiediensten bewaarde gegevens regelt en die aldus afwijkt van het beginsel van de vertrouwelijkheid van elektronische communicatie, zij eraan herinnerd dat de in artikel 15, lid 1, eerste zin, van Richtlijn 2002/58 gegeven opsomming van doelstellingen exhaustief is, zodat die toegang daadwerkelijk en strikt op een van die doelstellingen moet berusten (zie in die zin arrest Tele2 Sverige en Watson e.a., punten 90 en 115).

53. Aangaande de doelstelling strafbare feiten te voorkomen, te onderzoeken, op te sporen en te vervolgen, dient te worden geconstateerd dat het daarbij volgens de bewoordingen van artikel 15, lid 1, eerste zin, van Richtlijn 2002/58 evenwel niet alleen over de bestrijding van ernstige delicten maar over 'strafbare feiten' in het algemeen gaat[.]

54. Stellig heeft het Hof in dit verband geoordeeld dat ter zake van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, alleen de bestrijding van zware criminaliteit kan rechtvaardigen dat overheidsinstanties toegang krijgen tot door aanbieders van elektronische-communicatiediensten bewaarde persoonsgegevens waaruit, in hun geheel beschouwd, precieze conclusies kunnen worden getrokken over het privéleven van de betrokken personen (zie in die zin arrest Tele2 Sverige en Watson e.a., punt 99).

55. Het Hof heeft die uitlegging echter gemotiveerd met de overweging dat de met een toegangsregeling nagestreefde doelstelling in verhouding moet staan tot de ernst van de inmenging in de betrokken grondrechten die deze ingreep meebrengt (zie in die zin arrest Tele2 Sverige en Watson e.a., punt 115).

56. Volgens het evenredigheidsbeginsel kan ter zake van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, ernstige inmenging immers slechts worden gerechtvaardigd door de doelstelling om - eveneens 'ernstige' - criminaliteit te bestrijden.

57. Is de inmenging die een dergelijke toegang veroorzaakt daarentegen niet ernstig, dan kan die toegang worden gerechtvaardigd door de doelstelling van het voorkomen, onderzoeken, opsporen en vervolgen van 'strafbare feiten' in het algemeen.

‡LW-BEHVMBJEH-GJDIBQW‡

58. Allereerst moet dus worden uitgemaakt of in casu, gelet op de omstandigheden van de onderhavige zaak, de inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten die zou voortvloeien uit het feit dat aan de gerechtelijke politie toegang tot de in het hoofdgeding aan de orde zijnde gegevens wordt verleend, als 'ernstig' moet worden beschouwd.

59. In dit verband heeft het verzoek in het hoofdgeding, waarmee de gerechtelijke politie in een strafrechtelijk onderzoek via rechterlijke toestemming toegang wil verkrijgen tot door aanbieders van elektronischecommunicatiediensten bewaarde persoonsgegevens, louter tot doel de houders te identificeren van de simkaarten die gedurende een periode van twaalf dagen met het IMEI-nummer van de gestolen mobiele telefoon zijn geactiveerd. Zoals in punt 40 van het onderhavige arrest is uiteengezet, strekt dat verzoek er enkel toe om toegang te verkrijgen tot de telefoonnummers die overeenstemmen met die simkaarten en tot de civiele-identiteitsgegevens van de houders van die kaarten, zoals hun naam, voornaam en, in voorkomend geval, adres. Zoals zowel de Spaanse regering als het openbaar ministerie ter terechtzitting heeft bevestigd, gaat het daarbij echter niet over de communicatie die met de gestolen mobiele telefoon tot stand is gebracht of over de locatie van die telefoon.

60. Met de via het toegangsverzoek in het hoofdgeding beoogde gegevens is het dus blijkbaar alleen mogelijk om, gedurende een bepaalde periode, de met de gestolen mobiele telefoon geactiveerde simkaart(en) in verband te brengen met de civiele identiteit van de houders van die simkaarten. Zonder aanvullende gegevens over de communicatie die met die simkaarten tot stand is gebracht en over de locatie, kan met die gegevens noch de datum, het uur, de duur of de ontvanger van de met de betrokken simkaart(en) verrichte oproepen worden achterhaald, noch waar die communicatie heeft plaatsgevonden of hoe vaak in een gegeven periode met bepaalde personen is gecommuniceerd. Uit die gegevens kunnen dus geen nauwkeurige conclusies over het privéleven van de betrokken personen worden getrokken.

61. In die omstandigheden kan de toegang tot de in het verzoek in het hoofdgeding bedoelde gegevens niet worden aangemerkt als een 'ernstige' inmenging in de grondrechten van de personen waarop de gegevens betrekking hebben.

62. Zoals uit de punten 53 tot en met 57 van dit arrest blijkt, kan de inmenging die een dergelijke gegevenstoegang zou veroorzaken dus worden gerechtvaardigd door de in artikel 15, lid 1, eerste zin, van Richtlijn 2002/58 vermelde doelstelling om 'strafbare feiten' in het algemeen te voorkomen, te onderzoeken, op te sporen en te vervolgen, zonder dat deze strafbare feiten als 'ernstig' moeten worden aangemerkt.

63. Gelet op het voorgaande dient op de gestelde vragen te worden geantwoord dat artikel 15, lid 1, van Richtlijn 2002/58, gelezen in samenhang met de artikelen 7 en 8 van het Handvest, aldus moet worden uitgelegd dat de toegang van overheidsinstanties tot de identificatiegegevens van houders van met een gestolen mobiele telefoon geactiveerde simkaarten - zoals hun naam, voornaam en, in voorkomend geval, adres - geen zodanig ernstige inmenging in de door die artikelen van het Handvest gewaarborgde grondrechten van laatstgenoemden oplevert dat die toegang - op het gebied van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten – moet worden beperkt tot de bestrijding van zware criminaliteit."

‡LW-BEHVMBJEH-GJDIBQW‡

2° Het arrest van 6 oktober 2020 in zake *Privacy International* (C-623/17), (hierna het arrest *Privacy International*), uitgesproken in grote kamer, waarin het Hof van Justitie voor recht verklaard heeft:

"Artikel 15, lid 1, van Richtlijn 2002/58, zoals gewijzigd bij Richtlijn 2009/136, gelezen in het licht van artikel 4, lid 2, VEU en de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, moet aldus worden uitgelegd dat het zich verzet tegen een nationale regeling op grond waarvan een overheidsorgaan ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten kan opleggen."

Dat arrest steunt op volgende overwegingen:

"Tweede vraag

50. Met zijn tweede vraag wenst de verwijzende rechter in wezen te vernemen of artikel 15, lid 1, van Richtlijn 2002/58, gelezen in het licht van artikel 4, lid 2, VEU en de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, aldus moet worden uitgelegd dat het zich verzet tegen een nationale regeling op grond waarvan een overheidsorgaan ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten kan opleggen.

51. Om te beginnen zij eraan herinnerd dat section 94 van de wet van 1984 volgens de informatie in het verzoek om een prejudiciële beslissing de Secretary of State de mogelijkheid biedt om aanbieders van elektronischecommunicatiediensten door middel van aanwijzingen de verplichting op te leggen om bulkcommunicatiegegevens door te zenden aan de veiligheids- en inlichtingendiensten, indien hij dit noodzakelijk acht in het belang van de nationale veiligheid of de betrekkingen met een buitenlandse regering. Deze gegevens omvatten verkeers- en locatiegegevens alsmede informatie over de gebruikte diensten, in de zin van section 21, leden 4 en 6, RIPA. Deze laatste bepaling ziet onder meer op de gegevens die nodig zijn om de bron en de bestemming van een communicatie te identificeren, de datum, het tijdstip, de duur en de aard van die communicatie te bepalen, het gebruikte materiaal te identificeren en de eindapparatuur en de communicatie te lokaliseren. Tot die gegevens behoren met name de naam en het adres van de gebruiker, het telefoonnummer van de beller en het gebelde nummer, het bron- en het doel-IP-adres en de adressen van de bezochte websites.

52. Een dergelijke verstrekking van gegevens door middel van doorzending betreft alle gebruikers van elektronischecommunicatiemiddelen, zonder dat wordt gespecificeerd of die doorzending wel of niet in real time moet plaatsvinden. De doorgezonden gegevens worden volgens de informatie in het verzoek om een prejudiciële beslissing door de veiligheids- en inlichtingendiensten bewaard en blijven ter beschikking van deze diensten ten behoeve van hun activiteiten, net zoals de andere databases van deze diensten. Met name kunnen de aldus verworven gegevens, waarop automatische bulkverwerking en -analyse worden toegepast, worden onderworpen aan kruiscontroles met andere databases die verschillende categorieën bulkpersoonsgegevens bevatten, of buiten die diensten worden bekendgemaakt, ook aan derde staten. Tot slot is voor die bewerkingen geen voorafgaande toestemming van een rechterlijke instantie of een onafhankelijk bestuursorgaan vereist en geldt er geen verplichting om de betrokkenen te informeren.

‡LW-BEHVMBJEH-GJDIBQW‡

53. Zoals met name uit de overwegingen 6 en 7 van Richtlijn 2002/58 volgt, heeft deze richtlijn tot doel om de gebruikers van elektronischecommunicatiediensten te beschermen tegen de gevaren die de nieuwe technologieën en, met name, de steeds grotere mogelijkheden van geautomatiseerde opslag en verwerking van gegevens voor de persoonsgegevens en de persoonlijke levenssfeer van die gebruikers meebrengen. Zoals in overweging 2 van Richtlijn 2002/58 wordt verklaard, beoogt deze richtlijn in het bijzonder de volledige eerbiediging van de in de artikelen 7 en 8 van het Handvest bedoelde rechten te waarborgen. Dienaangaande blijkt uit de toelichting bij het voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie [COM(2000) 385 definitief], waaruit Richtlijn 2002/58 is voortgekomen, dat de Uniewetgever heeft willen 'zorgen voor een hoge mate van bescherming van de persoonsgegevens en van de persoonlijke levenssfeer voor alle elektronischecommunicatiediensten, ongeacht de gebruikte technologie'.

54. Daartoe bepaalt artikel 5, lid 1, van Richtlijn 2002/58 dat '[d]e lidstaten [...] via nationale wetgeving het vertrouwelijke karakter van de communicatie en de daarmee verband houdende verkeersgegevens via openbare communicatienetwerken en via openbare elektronischecommunicatiediensten [garanderen]'. In diezelfde bepaling wordt benadrukt dat de lidstaten 'met name het afluisteren, aftappen, opslaan of anderszins onderscheppen of controleren van de communicatie en de daarmee verband houdende verkeersgegevens door anderen dan de gebruikers [verbieden], indien de betrokken gebruikers daarin niet hebben toegestemd, tenzij dat bij wet is toegestaan overeenkomstig artikel 15, lid 1,' en gepreciseerd dat '[d]it lid [...] de technische opslag die nodig is voor het overbrengen van informatie onverlet [laat], onverminderd het vertrouwelijkheidsbeginsel'.

55. Artikel 5, lid 1, legt aldus het beginsel van vertrouwelijkheid van zowel de elektronische communicatie als de daarmee verband houdende verkeersgegevens vast en impliceert met name dat het anderen dan de gebruikers in beginsel moet worden verboden die communicatie en die gegevens op te slaan, indien de gebruikers daarin niet hebben toegestemd. Gelet op haar algemene bewoordingen, bestrijkt die bepaling noodzakelijkerwijs elke voor andere doeleinden dan het overbrengen van informatie uitgevoerde bewerking die derden in staat stelt om kennis te nemen van de communicatie en de daarmee verband houdende gegevens.

56. Het in artikel 5, lid 1, van Richtlijn 2002/58 neergelegde verbod op het onderscheppen van de communicatie en de daarmee verband houdende verkeersgegevens omvat dus elke vorm van beschikbaarstelling door aanbieders van elektronischecommunicatiediensten van verkeers- en locatiegegevens aan overheidsinstanties, zoals veiligheids- en inlichtingendiensten, alsmede de bewaring van de beschikbaar gestelde gegevens door die instanties, ongeacht het latere gebruik van die gegevens.

57. Met de vaststelling van Richtlijn 2002/58 heeft de Uniewetgever dus de in de artikelen 7 en 8 van het Handvest neergelegde rechten geconcretiseerd, zodat de gebruikers van elektronischecommunicatiemiddelen in beginsel erop mogen vertrouwen dat hun communicatie en de daarmee verband houdende gegevens anoniem blijven en niet mogen worden vastgelegd, tenzij zij daarin hebben toegestemd (arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, punt 109).

58. Artikel 15, lid 1, van Richtlijn […] 2002/58 staat de lidstaten echter toe, te voorzien in uitzonderingen op de in artikel 5, lid 1, van deze richtlijn geformuleerde principeverplichting om de vertrouwelijkheid van de persoonsgegevens te waarborgen, en op de met name in de artikelen 6 en 9 van deze richtlijn vermelde overeenkomstige

‡LW-BEHVMBJEH-GJDIBQW‡

verplichtingen, indien dat in een democratische samenleving een noodzakelijke, redelijke en proportionele maatregel vormt om de nationale veiligheid, de landsverdediging en de openbare veiligheid te waarborgen, of om strafbare feiten of onbevoegd gebruik van het elektronischecommunicatiesysteem te voorkomen, te onderzoeken, op te sporen en te vervolgen. Daartoe kunnen de lidstaten onder meer wettelijke maatregelen treffen om gegevens gedurende een beperkte periode te bewaren indien dat om een van die redenen gerechtvaardigd is.

59. De mogelijkheid om af te wijken van de in de artikelen 5, 6 en 9 van Richtlijn 2002/58 vastgestelde rechten en verplichtingen kan echter niet rechtvaardigen dat de uitzondering op de principeverplichting tot waarborging van de vertrouwelijkheid van de elektronische communicatie en van de daarmee verband houdende gegevens en, in het bijzonder, op het verbod om deze gegevens op te slaan de regel wordt (zie in die zin arresten van 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punten 89 en 104, en 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, punt 111).

60. Bovendien volgt uit artikel 15, lid 1, derde zin, van Richtlijn 2002/58 dat de lidstaten slechts wettelijke maatregelen ter beperking van de omvang van de in de artikelen 5, 6 en 9 van deze richtlijn bedoelde rechten en plichten mogen nemen voor zover deze maatregelen in overeenstemming zijn met de algemene beginselen van het Unierecht, waaronder het evenredigheidsbeginsel, en met de door het Handvest gewaarborgde grondrechten. In dit verband heeft het Hof reeds geoordeeld dat de door een lidstaat bij een nationale regeling aan aanbieders van elektronischecommunicatiediensten opgelegde verplichting om de verkeersgegevens te bewaren teneinde de bevoegde nationale autoriteiten in voorkomend geval toegang tot die gegevens te kunnen geven, niet alleen vragen doet rijzen betreffende de eerbiediging van de artikelen 7 en 8 van het Handvest, die betrekking hebben op, respectievelijk, de bescherming van het privéleven en de bescherming van persoonsgegevens, maar ook betreffende de eerbiediging van artikel 11 van het Handvest, dat betrekking heeft op de vrijheid van meningsuiting (zie in die zin arresten van 8 april 2014, Digital Rights Ireland e.a., C-293/12 en C-594/12, EU:C:2014:238, punten 25 en 70, en 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punten 91 en 92 en aldaar aangehaalde rechtspraak).

61. Diezelfde vragen rijzen ook voor andere vormen van gegevensverwerking, zoals de doorzending van gegevens aan anderen dan de gebruikers of de toegang tot die gegevens met het oog op het gebruik ervan [zie naar analogie advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punten 122 en 123 en aldaar aangehaalde rechtspraak].

62. Bij de uitlegging van artikel 15, lid 1, van Richtlijn 2002/58 moet derhalve zowel het belang van het door artikel 7 van het Handvest gewaarborgde recht op bescherming van het privéleven als dat van het door artikel 8 van het Handvest gewaarborgde recht op bescherming van persoonsgegevens, zoals dat blijkt uit de rechtspraak van het Hof, in aanmerking worden genomen. Hetzelfde geldt voor het recht op vrijheid van meningsuiting, aangezien dit in artikel 11 van het Handvest gewaarborgde grondrecht een van de wezenlijke grondslagen is van een democratische en pluralistische samenleving, die behoort tot de waarden waarop de Unie overeenkomstig artikel 2 VEU is gebaseerd (zie in die zin arresten van 6 maart 2001, Connolly/Commissie, C-274/99 P, EU:C:2001:127, punt 39, en 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 93 en aldaar aangehaalde rechtspraak).

‡LW-BEHVMBJEH-GJDIBQW‡

63. De in de artikelen 7, 8 en 11 van het Handvest verankerde rechten hebben echter geen absolute gelding, maar moeten worden beschouwd in relatie tot hun functie in de samenleving (zie in die zin arrest van 16 juli 2020, Facebook Ireland en Schrems, C-311/18, EU:C:2020:559, punt 172 en aldaar aangehaalde rechtspraak).

64. Zoals blijkt uit artikel 52, lid 1, van het Handvest, staat het Handvest immers beperkingen op de uitoefening van die rechten toe, mits deze beperkingen bij wet worden gesteld, de wezenlijke inhoud van die rechten eerbiedigen en, met inachtneming van het evenredigheidsbeginsel, noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen.

65. Hieraan dient te worden toegevoegd dat het vereiste dat elke beperking op de uitoefening van grondrechten bij wet wordt gesteld, inhoudt dat de rechtsgrond die de inmenging in die rechten toestaat, zelf de reikwijdte van de beperking op de uitoefening van het betrokken recht moet bepalen (arrest van 16 juli 2020, Facebook Ireland en Schrems, C-311/18, EU:C:2020:559, punt 175 en aldaar aangehaalde rechtspraak).

66. Wat de eerbiediging van het evenredigheidsbeginsel betreft, staat in artikel 15, lid 1, eerste zin, van Richtlijn 2002/58 te lezen dat de lidstaten een maatregel waarbij wordt afgeweken van het beginsel van vertrouwelijkheid van de communicatie en van de daarmee verband houdende verkeersgegevens kunnen treffen wanneer een dergelijke maatregel 'in een democratische samenleving noodzakelijk, redelijk en proportioneel is' in het licht van de in die bepaling genoemde doelstellingen. In overweging 11 van deze richtlijn wordt gepreciseerd dat een dergelijke maatregel 'strikt' evenredig moet zijn aan het nagestreefde doel.

67. In dit verband zij eraan herinnerd dat de bescherming van het grondrecht op eerbiediging van het privéleven volgens vaste rechtspraak van het Hof vereist dat de uitzonderingen op de bescherming van de persoonsgegevens en de beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven. Bovendien kan een doelstelling van algemeen belang niet worden nagestreefd zonder rekening te houden met het feit dat deze doelstelling moet worden verzoend met de door de maatregel aangetaste grondrechten, zulks via een evenwichtige afweging tussen de doelstelling en de op het spel staande belangen en rechten [zie in die zin arresten van 16 december 2008, Satakunnan Markkinapörssi en Satamedia, C-73/07, EU:C:2008:727, punt 56; 9 november 2010, Volker und Markus Schecke en Eifert, C-92/09 en C-93/09, EU:C:2010:662, punten 76, 77 en 86, en 8 april 2014, Digital Rights Ireland e.a., C-293/12 en C-594/12, EU:C:2014:238, punt 52; advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 140].

68. Om aan het evenredigheidsvereiste te voldoen, dient een regeling duidelijke en nauwkeurige regels te bevatten over de reikwijdte en de toepassing van de betrokken maatregel, zodat degenen van wie de persoonsgegevens aan de orde zijn, over voldoende waarborgen beschikken dat die gegevens doeltreffend worden beschermd tegen het risico van misbruik. Die regeling moet wettelijk verbindend zijn naar intern recht en in het bijzonder aangeven in welke omstandigheden en onder welke voorwaarden een maatregel die voorziet in de verwerking van dergelijke gegevens kan worden genomen, en aldus waarborgen dat de inmenging tot het strikt noodzakelijke wordt beperkt. De noodzaak om over dergelijke waarborgen te beschikken is des te groter wanneer de persoonsgegevens op geautomatiseerde wijze worden verwerkt, met name wanneer er een aanzienlijk risico bestaat dat deze gegevens op onrechtmatige wijze zullen worden geraadpleegd. Deze overwegingen gelden in het bijzonder wanneer het gaat om de bescherming van een bijzondere categorie persoonsgegevens, te weten gevoelige gegevens [zie in die zin arresten van 8 april 2014, Digital Rights Ireland e.a., C-293/12 en C-594/12,

‡LW-BEHVMBJEH-GJDIBQW‡

EU:C:2014:238, punten 54 en 55, en 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 117; advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 141].

69. Wat de vraag betreft of een nationale regeling als die van het hoofdgeding voldoet aan de vereisten van artikel 15, lid 1, van Richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, dient te worden opgemerkt dat de doorzending van verkeers- en locatiegegevens aan anderen dan de gebruikers, zoals de veiligheids- en inlichtingendiensten, afwijkt van het vertrouwelijkheidsbeginsel. Wanneer die bewerking, zoals in casu, op algemene en ongedifferentieerde wijze wordt uitgevoerd, heeft zij tot gevolg dat de afwijking van de principeverplichting tot waarborging van de vertrouwelijkheid van de gegevens de regel wordt, terwijl het bij richtlijn 2002/58 ingevoerde stelsel eist dat die afwijking de uitzondering blijft.

70. Voorts vormt de doorzending van verkeers- en locatiegegevens aan een derde volgens vaste rechtspraak van het Hof een inmenging in de in de artikelen 7 en 8 van het Handvest verankerde grondrechten, ongeacht het latere gebruik van die gegevens. In dit verband is het van weinig belang of de gegevens betreffende het privéleven al dan niet gevoelig zijn en of de betrokkenen door die inmenging enig nadeel hebben ondervonden [zie in die zin advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punten 124 en 126 en aldaar aangehaalde rechtspraak, en arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, punten 115 en 116].

71. De inmenging die de doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten vormt in het door artikel 7 van het Handvest gewaarborgde recht, moet als bijzonder ernstig worden beschouwd, met name gelet op het gevoelige karakter van de informatie die deze gegevens kunnen prijsgeven, en op de mogelijkheid om aan de hand van deze gegevens het profiel van de betrokken personen te bepalen, informatie die even gevoelig is als de inhoud zelf van de communicatie. Die inmenging kan bovendien bij de betrokken personen het gevoel opwekken dat hun privéleven constant in de gaten wordt gehouden (zie naar analogie arresten van 8 april 2014, Digital Rights Ireland e.a., C-293/12 en C-594/12, EU:C:2014:238, punten 27 en 37, en 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punten 99 en 100).

72. Tevens moet worden opgemerkt dat de doorzending van verkeers- en locatiegegevens aan overheidsinstanties voor veiligheidsdoeleinden op zichzelf afbreuk kan doen aan het in artikel 7 van het Handvest verankerde recht op eerbiediging van communicatie, en de gebruikers van elektronischecommunicatiemiddelen kan ontmoedigen om hun door artikel 11 van het Handvest gewaarborgde vrijheid van meningsuiting uit te oefenen. Dit laatste geldt in het bijzonder voor personen van wie de communicatie naar nationaal recht onder het beroepsgeheim valt, en voor klokkenluiders van wie de activiteiten worden beschermd door Richtlijn (EU) 2019/1937 van het Europees Parlement en de Raad van 23 oktober 2019 inzake de bescherming van personen die inbreuken op het Unierecht melden (PB 2019, L 305, blz. 17). Dat ontmoedigende effect is bovendien des te ernstiger omdat de bewaarde gegevens talrijk en gevarieerd zijn (zie in die zin arresten van 8 april 2014, Digital Rights Ireland e.a., C-293/12 en C-594/12, EU:C:2014:238, punt 28; 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 101, en 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, punt 118).

‡LW-BEHVMBJEH-GJDIBQW‡

73. Ten slotte is het zo dat, gelet op de aanzienlijke hoeveelheid verkeers- en locatiegegevens die continu kunnen worden bewaard op grond van een algemene bewaringsmaatregel, en op het gevoelige karakter van de informatie die deze gegevens kunnen prijsgeven, het enkele feit dat die gegevens door aanbieders van elektronischecommunicatiediensten worden bewaard, risico's van misbruik en onrechtmatige toegang tot de gegevens inhoudt.

74. Wat de doelstellingen betreft die dergelijke inmengingen kunnen rechtvaardigen, meer in het bijzonder de in het hoofdgeding aan de orde zijnde doelstelling van bescherming van de nationale veiligheid, moet om te beginnen worden opgemerkt dat de nationale veiligheid volgens artikel 4, lid 2, VEU tot de uitsluitende verantwoordelijkheid van elke lidstaat behoort. Deze verantwoordelijkheid strookt met het grote belang dat wordt gehecht aan de bescherming van de essentiële staatsfuncties en de fundamentele belangen van de samenleving, en omvat het voorkomen en bestrijden van activiteiten die de fundamentele constitutionele, politieke, economische of sociale structuren van een land ernstig kunnen destabiliseren en, met name, een rechtstreekse bedreiging kunnen vormen voor de samenleving, de bevolking of de staat als zodanig, zoals terroristische activiteiten (arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, punt 135).

75. Het belang van de doelstelling van bescherming van de nationale veiligheid, gelezen in het licht van artikel 4, lid 2, VEU, overstijgt dat van de andere doelstellingen die worden genoemd in artikel 15, lid 1, van Richtlijn 2002/58, met name de doelstellingen van bestrijding van - zelfs ernstige - criminaliteit in het algemeen, en van bescherming van de openbare veiligheid. Bedreigingen als die waaraan in het voorgaande punt wordt gerefereerd, verschillen door hun aard en hun bijzondere ernst immers van het algemene risico dat zich - zelfs ernstige - spanningen of wanordelijkheden zullen voordoen die de openbare veiligheid ondermijnen. Mits aan de overige in artikel 52, lid 1, van het Handvest geformuleerde vereisten wordt voldaan, kan de doelstelling van bescherming van de nationale veiligheid derhalve maatregelen rechtvaardigen die ernstigere inmengingen in de grondrechten met zich brengen dan die welke door die andere doelstellingen zouden kunnen worden gerechtvaardigd (arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, punt 136).

76. Om te voldoen aan het in punt 67 van het onderhavige arrest in herinnering gebrachte evenredigheidsvereiste, dat verlangt dat uitzonderingen op de bescherming van persoonsgegevens en beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven, dient een nationale regeling die een inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten met zich brengt, evenwel in overeenstemming te zijn met de eisen die voortvloeien uit de in de punten 65, 67 en 68 van het onderhavige arrest aangehaalde rechtspraak.

77. Wat in het bijzonder de toegang van een autoriteit tot persoonsgegevens betreft, mag een regeling zich niet ertoe beperken te eisen dat de toegang tot deze gegevens wordt verleend voor het met die regeling beoogde doel, maar moet zij ook de materiële en procedurele voorwaarden voor dit gebruik bepalen [zie naar analogie advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 192 en aldaar aangehaalde rechtspraak].

‡LW-BEHVMBJEH-GJDIBQW‡

78. Een nationale regeling die de toegang tot locatie- en verkeersgegevens regelt, moet dus aan de hand van objectieve criteria bepalen in welke omstandigheden en onder welke voorwaarden aan de bevoegde nationale autoriteiten toegang tot de betrokken gegevens moet worden verleend, aangezien een algemene toegang tot alle bewaarde gegevens, los van enig - zelfs maar indirect - verband met het nagestreefde doel, niet kan worden geacht tot het strikt noodzakelijke te zijn beperkt, (zie in die zin arrest van 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 119 en aldaar aangehaalde rechtspraak).

79. Die vereisten zijn a fortiori van toepassing op een wettelijke maatregel als aan de orde in het hoofdgeding, op grond waarvan de bevoegde nationale autoriteit aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten kan opleggen. Een dergelijke doorzending heeft immers tot gevolg dat die gegevens ter beschikking worden gesteld aan overheidsinstanties [zie naar analogie advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 212].

80. Het feit dat de doorzending van de verkeers- en locatiegegevens geschiedt op algemene en ongedifferentieerde wijze, betekent dat die doorzending algemeen alle personen betreft die gebruikmaken van elektronischecommunicatiediensten, dat wil zeggen zelfs personen voor wie er geen enkele aanwijzing bestaat dat hun gedrag - zelfs maar indirect of van ver - een verband vertoont met de doelstelling van bescherming van de nationale veiligheid. Met name is er geen enkel verband vereist tussen de gegevens die moeten worden doorgezonden en een bedreiging van de nationale veiligheid (zie in die zin arresten van 8 april 2014, Digital Rights Ireland e.a., C-293/12 en C-594/12, EU:C:2014:238, punten 57 en 58, en 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 105). Gelet op het feit dat de doorzending van dergelijke gegevens aan overheidsinstanties - overeenkomstig de vaststelling in punt 79 van het onderhavige arrest - gelijkstaat aan het verlenen van toegang tot deze gegevens, moet worden geoordeeld dat een regeling die de algemene en ongedifferentieerde doorzending van gegevens aan overheidsinstanties mogelijk maakt, een algemene toegang tot die gegevens impliceert.

81. Daaruit volgt dat een nationale regeling die aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten oplegt, verder gaat dan strikt noodzakelijk is en niet kan worden beschouwd als een regeling die in een democratische samenleving gerechtvaardigd is, zoals artikel 15, lid 1, van Richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, eist.

82. Gelet op een en ander moet op de tweede vraag worden geantwoord dat artikel 15, lid 1, van Richtlijn 2002/58, gelezen in het licht van artikel 4, lid 2, VEU en de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, aldus moet worden uitgelegd dat het zich verzet tegen een nationale regeling op grond waarvan een overheidsorgaan ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten kan opleggen."

1.4.2. Na die twee beslissingen van het Hof van Justitie aangehaald te hebben, geeft het Grondwettelijk Hof de motivering en het dictum weer van het arrest *La Quadrature du Net* van het Hof van Justitie, in antwoord op de in zijn arrest nr. 96/2018 gestelde prejudiciële vragen.

‡LW-BEHVMBJEH-GJDIBQW‡

Vervolgens motiveert het Grondwettelijk Hof zijn beslissing als volgt:

"B.15. Uit het voormelde arrest van het Hof van Justitie van 6 oktober 2020 in zake *La Quadrature du Net e.a.*, blijkt dat artikel 15, lid 1, van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8 en 11 alsook van artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, aldus moet worden uitgelegd dat het zich verzet tegen wettelijke maatregelen die voor de in dat artikel 15, § 1, genoemde doeleinden preventief voorzien in een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens, behalve in de in het voormelde arrest beschreven beperkte gevallen.

In zoverre zij principieel en zonder beperking tot die gevallen voorziet in een algemene en ongedifferentieerde bewaring, door de operatoren en aanbieders van elektronische communicatiediensten, van de identificatiegegevens, de toegangs- en verbindingsgegevens, alsook van de communicatiegegevens beoogd in artikel 126, § 3, van de wet van 13 juni 2005, schendt de bestreden wet bijgevolg artikel 15, lid 1, van de richtlijn 2002/58/EG, gelezen in het licht van de voormelde bepalingen van het Handvest van de grondrechten van de Europese Unie, en in samenhang met de artikelen 10 en 11 van de Grondwet.

B.16.1. In het dictum van het voormelde arrest van 6 oktober 2020, in zake *La Quadrature du Net e.a.*, preciseert het Hof van Justitie echter dat artikel 15, lid 1, van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8 en 11 alsook van artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, zich niet verzet tegen verschillende soorten wettelijke maatregelen die het Hof opsomt. Toelaatbaar zijn aldus, met name, wettelijke maatregelen 'die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de IP-adressen die zijn toegewezen aan de bron van een verbinding, voor een periode die niet langer is dan strikt noodzakelijk', of nog wettelijke maatregelen 'die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van criminaliteit en de bescherming van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronischecommunicatiemiddelen'. Die wettelijke maatregelen moeten, 'door het gebruik van duidelijke en nauwkeurige regels, verzekeren dat de betrokken gegevens slechts worden bewaard indien aan de daarvoor geldende materiële en procedurele voorwaarden wordt voldaan, en dat de betrokken personen beschikken over effectieve waarborgen tegen het risico van misbruik'.

B.16.2. Op grond van die preciseringen van het Hof van Justitie betoogt de Ministerraad in zijn aanvullende memories dat de bestreden wet in elk geval niet dient te worden vernietigd in zoverre zij voorziet in de algemene en ongedifferentieerde verplichting tot bewaring, door de operatoren en aanbieders van elektronischecommunicatiediensten, van de IP-adressen die zijn toegewezen aan de bron van een verbinding, enerzijds, en van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronischecommunicatiemiddelen, anderzijds.

De Ministerraad besluit daaruit dat, in voorkomend geval, enkel het tweede en het derde lid van artikel 126, § 3, van de wet van 13 juni2005 dienen te worden vernietigd, waarin respectievelijk de verbindings- en locatiegegevens en de communicatiegegevens worden beoogd. Hij is van mening dat het eerste lid van het voormelde artikel 126, § 3, waarin de identificatiegegevens worden beoogd, daarentegen niet dient te worden vernietigd, net zomin als de andere bepalingen van de bestreden wet, aangezien zij de nodige waarborgen bevatten op het vlak van bewaring van en toegang tot de gegevens.

‡LW-BEHVMBJEH-GJDIBQW‡

B.17. Te dezen dient te worden vastgesteld dat de bestreden wet, wat het beginsel zelf ervan betreft, berust op een verplichting tot algemene en ongedifferentieerde bewaring van alle gegevens beoogd in artikel 126, § 3, van de wet van 13 juni 2005, en dat zij, in het algemeen, zoals in B.3 en B.4 is vermeld, ruimere doelstellingen nastreeft dan de bestrijding van zware criminaliteit of het risico van aantasting van de openbare veiligheid.

Het onderscheid dat bij artikel 126, § 3, van de wet van 13 juni2005 wordt gemaakt tussen drie categorieën van gegevens (te weten: identificatiegegevens, toegangs- en verbindingsgegevens, alsook communicatiegegevens) heeft slechts een weerslag op het startpunt van de bewaringstermijn van de gegevens - in elk geval twaalf maanden -, en eventueel op de mogelijkheden voor de gemachtigde instanties om toegang tot die gegevens te hebben (zie artikel 46*bis* van het Wetboek van strafvordering en artikel 126, § 2, van de wet van 13 juni 2005). Die categorisering stemt daarenboven niet overeen met het onderscheid dat door het Hof van Justitie in zijn arrest van 6 oktober 2020 wordt gemaakt voor wat betreft de verschillende categorieën van gegevens die het voorwerp kunnen uitmaken van een verplichting tot algemene en ongedifferentieerde bewaring, mits verscheidene voorwaarden in acht worden genomen (te weten, te dezen: de IP-adressen die zijn toegewezen aan de bron van een verbinding en de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronischecommunicatiemiddelen).

B.18. Bij het arrest van het Hof van Justitie van 6 oktober 2020 wordt een verandering van gezichtspunt opgelegd ten opzichte van de keuze die de wetgever heeft gemaakt: de verplichting tot bewaring van gegevens met betrekking tot elektronische communicatie moet de uitzondering zijn, en niet de regel. De regeling waarbij in een dergelijke verplichting wordt voorzien, moet daarenboven onderworpen zijn aan duidelijke en nauwkeurige regels over de reikwijdte en de toepassing van de betrokken maatregel, waarbij een minimum aan vereisten worden opgelegd (punt 133). Die regeling moet waarborgen dat de inmenging tot het strikt noodzakelijke wordt beperkt en moet steeds 'beantwoorden aan objectieve criteria die een verband leggen tussen de te bewaren gegevens en het nagestreefde doel' (punten 132 en 133).

B.19. Het staat aan de wetgever een regeling tot stand te brengen waarbij de beginselen in acht worden genomen die van toepassing zijn inzake bescherming van persoonsgegevens, in het licht van de rechtspraak van het Hof van Justitie, en, in voorkomend geval, rekening te houden met de door dat Hof aangebrachte preciseringen wat betreft de verschillende soorten wettelijke maatregelen die verenigbaar worden geacht met artikel 15, lid 1, van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8, 11 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie. In het bijzonder staat het, in die context, ook aan de wetgever tussen de verschillende soorten aan bewaring onderworpen gegevens het onderscheid te maken dat geboden is, zodat wordt gewaarborgd dat, voor elk soort gegeven, de inmenging tot het strikt noodzakelijke wordt beperkt.

B.20. Rekening houdend met hetgeen voorafgaat, dienen de artikelen 2, b), 3 tot 11 en 14 van de bestreden wet, die onlosmakelijk met elkaar verbonden zijn, te worden vernietigd."

Om die redenen beslist het Grondwettelijk Hof in zijn arrest nr. 57/2021 van 22 april 2021 de artikelen 2, b), 3 tot 11 en 14 van de wet van 29 mei 2016 te vernietigen zonder de gevolgen ervan gedurende een bepaalde periode te handhaven. Voor het overige verwerpt het Hof het beroep.

‡LW-BEHVMBJEH-GJDIBQW‡

1.5. Het voorliggende voorontwerp strekt ertoe gevolg te geven aan dat arrest van het Grondwettelijk Hof van 22 april 2021 evenals aan de rechtspraak van het Hof van Justitie waarop dat arrest gebaseerd is, meer bepaald het arrest *La Quadrature du Net*.

2. Gelet op wat voorafgaat, moet het voorontwerp meer in het bijzonder onderzocht worden in het licht van artikel 15 van richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 dat als volgt luidt:

> "Toepassing van een aantal bepalingen van Richtlijn 95/46/EG
>
> 1. De lidstaten kunnen wettelijke maatregelen treffen ter beperking van de reikwijdte van de in de artikelen 5 en 6, artikel 8, leden 1, 2, 3 en 4, en artikel 9 van deze richtlijn bedoelde rechten en plichten, indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale, d.w.z. de staatsveiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronische-communicatiesysteem als bedoeld in artikel 13, lid 1, van Richtlijn 95/46/EG. Daartoe kunnen de lidstaten o.a. wetgevingsmaatregelen treffen om gegevens gedurende een beperkte periode te bewaren om de redenen die in dit lid worden genoemd. Alle in dit lid bedoelde maatregelen dienen in overeenstemming te zijn met de algemene beginselen van het Gemeenschapsrecht, met inbegrip van de beginselen als bedoeld in artikel 6, leden 1 en 2, van het Verdrag betreffende de Europese Unie.
>
> 1*bis*. Lid 1 is niet van toepassing op de uit hoofde van Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken[7] te bewaren gegevens voor de in artikel 1, lid 1, van die richtlijn bedoelde doeleinden.
>
> 1*ter*. Aanbieders zetten interne procedures op voor de afhandeling van verzoeken om toegang tot persoonsgegevens van gebruikers op de grondslag van nationale bepalingen die overeenkomstig lid 1 zijn aangenomen. Zij verstrekken aan de bevoegde nationale instantie op verzoek gegevens over deze procedures, het aantal ontvangen verzoeken, de aangevoerde wettelijke motivering en hun antwoord.
>
> 2. Het bepaalde in hoofdstuk III van Richtlijn 95/46/EG inzake beroep op de rechter, aansprakelijkheid en sancties geldt voor de nationale bepalingen die uit hoofde van deze richtlijn worden aangenomen en ten aanzien van de individuele rechten die uit deze richtlijn voortvloeien.
>
> 3. De Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens, ingesteld bij artikel 29 van Richtlijn 95/46/EG, voert de in artikel 30 van die richtlijn vermelde taken ook uit ten aanzien van aangelegenheden die onder de onderhavige richtlijn vallen, namelijk de bescherming van de fundamentele rechten en vrijheden en van rechtmatige belangen in de sector elektronische communicatie."

[7] *Voetnoot 1 van de geciteerde richtlijn:* PB L 105 van 13.4.2006, blz. 54.

‡LW-BEHVMBJEH-GJDIBQW‡

3. Aangezien de bepalingen van de wet van 29 mei 2016 en daarvóór de bepalingen van de wet van 30 juli 2013 vernietigd zijn, worden ze, wat het interne recht betreft, geacht nooit te hebben bestaan en worden de bepalingen die bij die wetten zijn opgeheven of gewijzigd opnieuw toepasselijk zoals ze gelden, ongeacht de wijzigingen die bij de twee voormelde wetten aangebracht zijn.

4. Het is in die context dat de stellers van het voorontwerp derhalve een regeling voor gegevensbewaring willen invoeren om de doelstellingen te bereiken die het Hof van Justitie en het Grondwettelijk Hof legitiem hebben geacht en die in overeenstemming is met het dictum en de motivering van de beslissingen van die hoge rechtscolleges, in het bijzonder met de uit die beslissingen voortvloeiende grenzen en criteria inzake het bewaren van verkeers- en locatiegegevens door de operatoren die actief zijn in de sector van de elektronische communicatie alsook inzake de toegang tot die gegevens door de overheden.

B. BEPALINGEN INGEVOERD BIJ DE ONTWORPEN TEKST OM TEGEMOET TE KOMEN AAN DE VEREISTEN WAARAAN VOLGENS DE ARRESTEN VAN HET HOF VAN JUSTITIE EN VAN HET GRONDWETTELIJK HOF ALSOOK VOLGENS DE RELEVANTE RECENTE RECHTSPRAAK VAN HET EUROPEES HOF VOOR DE RECHTEN VAN DE MENS VOLDAAN MOET ZIJN

Vooraf wijst de afdeling Wetgeving erop dat haar adiëring per definitie beperkt is tot de ontworpen tekst en dat het haar gelet op het voorgaande niet toekomt te onderzoeken of het geheel van het Belgisch positief recht, inzonderheid het gerechtelijk recht en het recht betreffende de inlichtingen- en veiligheidsdiensten, overeenkomstig met name de rechtspraak van het Europees Hof voor de Rechten van de Mens, het recht op eerbiediging van het privéleven kan waarborgen bij het verzamelen en het gebruiken van de gegevens waarvan dit ontwerp de bewaring regelt. Aldus hangt de vraag of de aaneenschakeling van de verzameling van, de bewaring van, de toegang tot en het gebruik van de betrokken gegevens verenigbaar is met de fundamentele rechten en vrijheden in kwestie af van andere geldende bepalingen, ongeacht of ze al dan niet een algemene strekking hebben, die niet aan de afdeling Wetgeving voorgelegd zijn.[8]

I.1. LERING VAN DE ARRESTEN *DIGITAL RIGHTS*, *MINISTERIO FISCAL* EN *LA QUADRATURE DU NET*

1.1. Uit de arresten inzake *Digital Rights, Ministerio Fiscal en La Quadrature du Net* evenals uit het daarop aansluitend arrest nr. 84/2015 van het Grondwettelijk Hof moet voornamelijk het volgende onthouden worden:

1° De bewaring van gegevens met de bedoeling dat de bevoegde nationale overheden eventueel tot die gegevens toegang hebben, vormt een inmenging in het fundamentele recht op eerbiediging van de persoonlijke levenssfeer en in de andere rechten die zijn neergelegd in de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie, met als verzwarende omstandigheid dat de overheden kennis moeten kunnen nemen van die gegevens.

[8] Zie in die zin advies 58.449/4.

‡LW-BEHVMBJEH-GJDIBQW‡

2° De wezenlijke inhoud van die rechten kan evenwel niet door die inmenging worden aangetast, wanneer het op grond van de toegang die de nationale overheden tot de betrokken gegevens krijgen niet mogelijk is om van de inhoud zelf van de elektronische communicatie kennis te nemen.

3° Die inmenging beantwoordt voorts aan een doelstelling van algemeen belang, wanneer ze de bestrijding van het internationale terrorisme, de bestrijding van de zware criminaliteit met het oog op de openbare veiligheid en het recht van eenieder op veiligheid tot doel heeft.

4° De vraag rijst dus of de beoogde inmenging evenredig is met het nagestreefde doel, namelijk of het gaat om maatregelen die absoluut noodzakelijk zijn om dat doel te bereiken. Wat dat betreft moet de regeling in kwestie "duidelijke en precieze regels betreffende de draagwijdte en de toepassing van de betrokken maatregel bevatten die minimale vereisten opleggen, zodat de personen van wie de gegevens zijn bewaard over voldoende garanties beschikken dat hun persoonsgegevens doeltreffend worden beschermd tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en elk onrechtmatig gebruik van deze gegevens".

In dat opzicht wordt niet aan dat evenredigheidsvereiste voldaan door een wetgeving die:

a) algemeen van toepassing is op alle personen, alle elektronische communicatiemiddelen en alle verkeersgegevens, zonder dat enig onderscheid wordt gemaakt, enige beperking wordt gesteld of enige uitzondering wordt gemaakt op basis van het doel zware criminaliteit te bestrijden;

b) niet bepaalt dat de personen van wie de gegevens bewaard worden zich, zelfs indirect, in een situatie moeten bevinden die aanleiding kan geven tot strafrechtelijke vervolging en geen uitzonderingen bevat, zodat zij zelfs van toepassing is op personen van wie de communicaties volgens de nationale rechtsregels onder het beroepsgeheim vallen;

c) geen enkel verband vereist tussen de gegevens die moeten worden bewaard en een bedreiging van de openbare veiligheid en met name de bewaring niet beperkt tot:

– hetzij gegevens die betrekking hebben op een bepaalde periode en/of een bepaalde geografische zone en/of een kring van bepaalde personen die op een of andere wijze betrokken kunnen zijn bij zware criminaliteit;

– hetzij personen voor wie de bewaring van de gegevens om andere redenen zou kunnen helpen bij het voorkomen, opsporen of vervolgen van zware criminaliteit;

d) "geen objectieve criteria bevat ter begrenzing van de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan met het oog op het voorkomen, opsporen of strafrechtelijk vervolgen van inbreuken die, gelet op de omvang en de ernst van de inmenging in de door de artikelen 7 en 8 van het Handvest erkende fundamentele rechten, voldoende ernstig kunnen worden geacht om een dergelijke inmenging te rechtvaardigen"; in dat opzicht kunnen er problemen rijzen op grond van een wetgeving die "geen materiële en

‡LW-BEHVMBJEH-GJDIBQW‡

procedurele voorwaarden bevat" en "niet uitdrukkelijk bepaalt dat deze toegang en het latere gebruik van de betrokken gegevens strikt gebonden zijn aan het doel, nauwkeurig afgebakende zware criminaliteit te voorkomen, op te sporen of strafrechtelijk te vervolgen"; dat geldt in het bijzonder wanneer de wetgeving "geen objectieve criteria bevat op basis waarvan het aantal personen dat de bewaarde gegevens mag raadplegen en vervolgens gebruiken, kan worden beperkt tot wat strikt noodzakelijk is voor de verwezenlijking van het nagestreefde doel" en "de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens niet onderworpen is aan enige voorafgaande controle door een rechterlijke instantie of een onafhankelijke administratieve instantie waarvan de beslissing beoogt om de toegang tot de gegevens en het gebruik ervan te beperken tot wat strikt noodzakelijk is ter verwezenlijking van het nagestreefde doel en die uitspraak doet op een gemotiveerd verzoek van deze autoriteiten, ingediend in het kader van procedures ter voorkoming, opsporing of vervolging van strafbare feiten";

e) voorziet in een algemene bewaartermijn van de gegevens "zonder dat enig onderscheid wordt gemaakt tussen (…) categorieën van gegevens naargelang van het nut ervan voor het nagestreefde doel of naargelang van de betrokken personen" en die niet preciseert "dat deze termijn op basis van objectieve criteria moet worden vastgesteld om te waarborgen dat hij beperkt is tot wat strikt noodzakelijk is". Daaruit kan afgeleid worden dat vereist is dat "deze inmenging nauwkeurig omkaderd is door bepalingen die kunnen waarborgen dat zij daadwerkelijk beperkt is tot het strikt noodzakelijke";

f) niet voorziet in "specifieke regels die aangepast zijn aan de enorme hoeveelheid gegevens die volgens deze richtlijn moeten worden bewaard, alsook aan het gevoelige karakter van deze gegevens en aan het risico dat zij op onrechtmatige wijze zullen worden geraadpleegd, en die met name ertoe strekken de bescherming en de beveiliging van de betrokken gegevens duidelijk en strikt te regelen om de volle integriteit en vertrouwelijkheid ervan te waarborgen"; dat geldt meer in het bijzonder wanneer de wetgeving niet van de operatoren vereist dat ze "via technische en organisatorische maatregelen een bijzonder hoog niveau van bescherming en beveiliging bieden" dat bovendien waarborgt dat "de gegevens na de bewaarperiode onherroepelijk worden vernietigd";

g) niet voorschrijft dat de gegevens in kwestie op het grondgebied van de Unie moeten worden bewaard, met als gevolg dat "niet ten volle is gewaarborgd dat een onafhankelijke autoriteit toezicht houdt op de inachtneming van de in de twee vorige punten bedoelde vereisten inzake bescherming en beveiliging, zoals uitdrukkelijk wordt voorgeschreven door artikel 8, lid 3, van het Handvest".

2. Specifiek wat betreft de strekking van artikel 15, lid 1, van richtlijn 2002/58/EG, gelezen in het licht van artikel 4, lid 2, VEU en van de artikelen 7, 8 en 11 van het Handvest van de grondrechten van de Europese Unie, moet uit de arresten *Ministerio Fiscal*, *Privacy International* en *La Quadrature du Net* voornamelijk het volgende onthouden worden:

‡LW-BEHVMBJEH-GJDIBQW‡

1° Niet toelaatbaar is een nationale regeling op grond waarvan een overheidsorgaan ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronische communicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten kan opleggen;

2° Toelaatbaar is een nationale wettelijke regeling die het mogelijk maakt om ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronische communicatiediensten een bevel tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens op te leggen in situaties waarin de betrokken lidstaat wordt geconfronteerd met een werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid, wanneer de beslissing waarbij dat bevel wordt opgelegd, effectief kan worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij het doel van die toetsing is om na te gaan of een van die situaties zich voordoet en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien, en wanneer dat bevel slechts kan worden opgelegd voor een periode die niet langer is dan strikt noodzakelijk, maar die kan worden verlengd indien die bedreiging voortduurt;

3° Toelaatbaar is een nationale wettelijke regeling die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorziet in een gerichte bewaring van verkeers- en locatiegegevens, die op basis van objectieve en niet-discriminatoire factoren wordt afgebakend aan de hand van categorieën betrokken personen of aan de hand van een geografisch criterium, voor een periode die niet langer is dan strikt noodzakelijk, maar die kan worden verlengd;

4° Toelaatbaar is een nationale wettelijke regeling die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorziet in een algemene en ongedifferentieerde bewaring van de IP-adressen die zijn toegewezen aan de bron van een verbinding, voor een periode die niet langer is dan strikt noodzakelijk;

5° Toelaatbaar is een nationale wettelijke regeling die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van criminaliteit en de bescherming van de openbare veiligheid voorziet in een algemene en ongedifferentieerde bewaring van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronische communicatiemiddelen;

6° Toelaatbaar is een nationale wettelijke regeling die het mogelijk maakt om ten behoeve van de bestrijding van zware criminaliteit en, *a fortiori*, de bescherming van de nationale veiligheid via een aan effectieve rechterlijke toetsing onderworpen beslissing van de bevoegde autoriteit aan aanbieders van elektronische communicatiediensten een bevel op te leggen tot spoedbewaring van de in hun handen zijnde verkeers- en locatiegegevens gedurende een bepaalde periode;

‡LW-BEHVMBJEH-GJDIBQW‡

7° Toelaatbaar is meer specifiek een wetgeving die de toegang van overheidsinstanties mogelijk maakt tot de identificatiegegevens van de houders van met een gestolen mobiele telefoon geactiveerde simkaarten – zoals hun naam, voornaam en, in voorkomend geval, adres – een dergelijke regeling levert weliswaar een inmenging in de grondrechten van laatstgenoemden op, maar het betreft geen zodanig ernstige inmenging dat die toegang – op het gebied van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten – moet worden beperkt tot de bestrijding van zware criminaliteit.

Wat de hiervoor vermelde punten 2° tot 6° betreft, zijn de betrokken wetgevingen enkel toelaatbaar als ze bovendien door het gebruik van duidelijke en nauwkeurige regels, verzekeren dat de betrokken gegevens slechts worden bewaard indien aan de daarvoor geldende materiële en procedurele voorwaarden wordt voldaan, en dat de betrokken personen beschikken over effectieve waarborgen tegen het risico van misbruik.

3. Ten slotte moet ook voor ogen gehouden worden dat het Hof van Justitie zich in zijn arrest *La Quadrature du Net* eveneens uitgesproken heeft over andere prejudiciële vragen[9-10] van de Raad van State van Frankrijk.

[9] In de zaak C-511/18 heeft de Raad van State van Frankrijk de volgende vragen gesteld:
"1) Moet de verplichting tot algemene en ongedifferentieerde bewaring, die rust op de aanbieders op grond van de permissieve bepalingen van artikel 15, lid 1, van richtlijn [2002/58/EG] van 12 juli 2002, in een context die wordt gekenmerkt door ernstige en aanhoudende bedreigingen voor de nationale veiligheid, en met name door terreurgevaar, worden beschouwd als een inmenging die wordt gerechtvaardigd door het recht op veiligheid als gewaarborgd door artikel 6 van het Handvest van de grondrechten van de Europese Unie, en door de vereisten van nationale veiligheid, waarvoor de verantwoordelijkheid krachtens artikel 4 van het Verdrag betreffende de Europese Unie uitsluitend op de lidstaten rust?
2) Dient de richtlijn van 12 juli 2002, gelezen in het licht van het Handvest van de grondrechten van de Europese Unie, aldus te worden uitgelegd dat zij het mogelijk maakt om wetgevende maatregelen te nemen, zoals maatregelen voor het in real time opvragen van verkeers- en locatiegegevens van welbepaalde personen, die weliswaar van invloed zijn op de rechten en verplichtingen van de aanbieders van een elektronische communicatiedienst, maar hun geen specifieke verplichting opleggen tot bewaring van hun gegevens?
3) Moet de richtlijn van 12 juli 2002, gelezen in het licht van het Handvest van de grondrechten van de Europese Unie, aldus worden uitgelegd dat zij de regelmatigheid van de procedures voor het opvragen van verbindingsgegevens in alle gevallen afhankelijk stelt van het vereiste om de betrokken personen te informeren wanneer dergelijke informatie het onderzoek van de bevoegde autoriteiten niet langer in gevaar kan brengen, dan wel dat dergelijke procedures als regelmatig kunnen worden beschouwd gelet op alle andere bestaande procedurele waarborgen, aangezien deze waarborgen de doeltreffendheid van het recht op beroep garanderen?"

[10] In de zaak C-512/18, heeft de Raad van State van Frankrijk de volgende vragen gesteld:
"1) Moet de verplichting tot algemene en ongedifferentieerde bewaring, die rust op de aanbieders op grond van de permissieve bepalingen van artikel 15, lid 1, van richtlijn [2002/58/EG] van 12 juli 2002, met name gelet op de waarborgen en controles die vervolgens gelden voor zowel het opvragen als het gebruiken van die verbindingsgegevens, worden beschouwd als een inmenging die wordt gerechtvaardigd door het recht op veiligheid als gewaarborgd door artikel 6 van het Handvest van de grondrechten van de Europese Unie en door de vereisten van nationale veiligheid, waarvoor de verantwoordelijkheid krachtens artikel 4 van het Verdrag betreffende de Europese Unie uitsluitend op de lidstaten rust?
2) Moeten de bepalingen van richtlijn [2000/31/EG] van 8 juni 2000, gelezen tegen de achtergrond van de artikelen 6, 7, 8 en 11 alsook van artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, aldus worden uitgelegd dat zij toestaan dat een staat een nationale regeling invoert die de personen van wie de activiteit erin bestaat online toegang tot communicatiediensten aan het publiek aan te bieden, en de natuurlijke of rechtspersonen die, zelfs gratis, met het oog op de terbeschikkingstelling aan het publiek door het aanbieden van online communicatiediensten aan het publiek zorgen voor de opslag van door de afnemers van die diensten aangeleverde signalen, geschriften, beelden, geluiden of berichten van om het even welke aard, verplicht om gegevens te bewaren die het mogelijk maken om eenieder te identificeren die heeft bijgedragen tot de creatie van de inhoud of van om het even welke inhoud van de diensten waarvan zij aanbieder zijn, zodat de gerechtelijke autoriteit

‡LW-BEHVMBJEH-GJDIBQW‡

In die context heeft het Hof van Justitie in dat arrest het volgende voor recht gezegd:

> "Artikel 15, lid 1, van richtlijn 2002/58, zoals gewijzigd bij richtlijn 2009/136, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten, moet aldus worden uitgelegd dat het zich niet verzet tegen een nationale regeling die aanbieders van elektronischecommunicatiediensten verplicht om, ten eerste, met name verkeers- en locatiegegevens op geautomatiseerde wijze te analyseren en in real time op te vragen, en, ten tweede, technische gegevens over de locatie van de gebruikte eindapparatuur in real time op te vragen, wanneer
>
> – die geautomatiseerde analyse beperkt is tot situaties waarin de betrokken lidstaat wordt geconfronteerd met een werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid, en de toepassing van die analyse effectief kan worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij het doel van die toetsing is om na te gaan of er sprake is van een situatie die de genoemde maatregel rechtvaardigt en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien, en wanneer
>
> – het in real time verzamelen van verkeers- en locatiegegevens beperkt is tot personen ten aanzien van wie er een geldige reden bestaat om te vermoeden dat zij op de een of andere manier betrokken zijn bij terroristische activiteiten, en is onderworpen aan voorafgaande toetsing door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, om ervoor te zorgen dat een dergelijke maatregel slechts wordt toegestaan binnen de grenzen van het strikt noodzakelijke. In naar behoren gemotiveerde urgente gevallen dient die toetsing op korte termijn plaats te vinden."

4. Zoals de afdeling Wetgeving reeds in advies 58.449/4 opgemerkt heeft, moet in het licht van deze bewoordingen rekening gehouden worden met de afgebakende draagwijdte van de verschillende beslissingen van het Hof van Justitie en van het Grondwettelijk Hof.

Zo heeft de zaak *Digital Rights* betrekking op de bewaring van en de daaropvolgende toegang tot gegevens zoals bedoeld in richtlijn 2006/24/EU, namelijk de bewaring en de toegang tot gegevens "teneinde te garanderen dat die gegevens beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit". De strekking van het arrest van het Hof van Justitie en de gevolgtrekkingen die daaruit moeten worden gemaakt, hoe strikt deze ook zijn, hebben dus enkel betrekking op het bewaren van gegevens waarvan het uiteindelijke doel erin bestaat gedragingen en handelingen die zware overtredingen vormen, strafrechtelijk te bestraffen, wat per definitie geen lichte bestraffing kan zijn.

In de zaak *La Quadrature du Net* heeft het Hof van Justitie zich uitgesproken in een context waarin de bewuste bewaring naargelang van het geval de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid of de bestrijding van criminaliteit en de bescherming van de openbare veiligheid tot doel had. Het Hof heeft zich ook uitgesproken over het op geautomatiseerde wijze analyseren van gegevens in geval van een werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid en over het in real time verzamelen van

---

in voorkomend geval om mededeling ervan kan verzoeken om de regels inzake burgerlijke of strafrechtelijke aansprakelijkheid te doen naleven?"

‡LW-BEHVMBJEH-GJDIBQW‡

verkeers- en locatiegegevens dat zich beperkt tot personen ten aanzien van wie er een geldige reden bestaat om te vermoeden dat zij op de een of andere manier betrokken zijn bij terroristische activiteiten.

In de zaak *Ministerio Fiscal* heeft het Hof van Justitie zich uitgesproken over de toegang van overheidsinstanties tot de identificatiegegevens van de houders van met een gestolen mobiele telefoon geactiveerde simkaarten.

In het arrest *Privacy International* ten slotte werd aan het Hof van Justitie een vraag gesteld over een nationale regeling op grond waarvan een overheidsorgaan ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronische communicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten kan opleggen.

Bij het onderzoek van het voorontwerp van wet moet dus rekening gehouden worden met de omstandigheid dat de vereisten waaraan volgens de voormelde beslissingen voldaan moet zijn hoofdzakelijk te maken hebben met de bestrijding van de criminaliteit, waarbij het naargelang van het geval om al dan niet zware criminaliteit gaat, en met de bescherming van de nationale veiligheid, inzonderheid in gevallen waarin deze laatste ernstig bedreigd wordt, in het bijzonder door terroristische daden.

De strekking van dat arrest kan *a priori* niet worden uitgebreid tot een bewaring van gegevens of een toegang tot bewaarde gegevens die andere doeleinden zouden dienen, zoals het opsporen door een ombudsdienst van een persoon die kwaadwillige oproepen pleegt, de identificatie van de persoon die een hulpdienst belt of van de plaats van waaruit zo'n oproep wordt gedaan zodat de hulpdienst kan optreden en kan zorgen voor de bescherming van goederen en personen, of het opsporen buiten iedere strafrechtelijke context van een persoon van wie de verdwijning onrustwekkend is wanneer blijkt dat zijn leven in onmiddellijk gevaar zou kunnen zijn en zelfs niet tot de activiteiten van de inlichtingen- en veiligheidsdiensten.

Deze laatste gevallen moeten dus niet zozeer onderzocht worden in het licht van de voormelde rechtspraak, maar wel in het licht van artikel 15, lid 1, van richtlijn 2002/58/EG, in zoverre die bepaling andere afwijkingen toestaat dan die welke in de voornoemde arresten onderzocht zijn, alsook vanuit het oogpunt van de meer algemene aspecten van het recht op eerbiediging van het privéleven dat gewaarborgd wordt door artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, door artikel 7 van het Handvest van de grondrechten van de Europese Unie en door artikel 22 van de Grondwet[11], evenals in het licht van het recht op bescherming van persoonsgegevens, dat specifiek gewaarborgd wordt door artikel 8 van het Handvest van de grondrechten van de Europese Unie, en in het licht van de desbetreffende Europese regelgeving, zoals verordening (EU) 2016/679 van

[11] Zie onder meer L. TASSONE, "La protection des données dans la jurisprudence de la Cour européenne des droits de l'homme" in A. GROSJEAN (ed.), *Enjeux européens et mondiaux de la protection des données personnelles*, verzamelwerk, Larcier, coll. Création Information Communication, 53 e.v., en de verwijzingen aldaar; over de inlichtingen- en veiligheidsdiensten zie onder meer advies 42.178/2, op 19 februari 2007 gegeven over een voorontwerp dat ontstaan gegeven heeft aan de wet van 4 februari 2010 'betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten' *Parl.St.* Senaat 2006-07, nr. 3-2138/1, 279-297, http://www.raadvst-consetat.be/dbx/avis/42178.pdf.

‡LW-BEHVMBJEH-GJDIBQW‡

het Europees Parlement en de Raad van 27 april 2016 'betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)' (hierna "de AVG").

5. Wat meer bepaald de AVG betreft, levert het arrest *La Quadrature du Net* leringen op die onthouden moeten worden.

Zo heeft het Hof van Justitie in zijn arrest het volgende geoordeeld:

"193. Met de tweede vraag in zaak C-512/18 wenst de verwijzende rechter in wezen te vernemen of de bepalingen van richtlijn 2000/31, gelezen in het licht van de artikelen 6 tot en met 8 en 11 en artikel 52, lid 1, van het Handvest, aldus moeten worden uitgelegd dat zij zich verzetten tegen een nationale regeling waarbij aanbieders die het publiek online toegang verlenen tot communicatiediensten en aanbieders van opslagdiensten een verplichting tot algemene en ongedifferentieerde bewaring van met name de met die diensten verband houdende persoonsgegevens wordt opgelegd.

194. De verwijzende rechter, die van mening is dat dergelijke diensten binnen de werkingssfeer van richtlijn 2000/31 en niet binnen die van richtlijn 2002/58 vallen, stelt zich op het standpunt dat artikel 15, leden 1 en 2, van richtlijn 2000/31, gelezen in samenhang met de artikelen 12 en 14 van deze richtlijn, als zodanig geen principieel verbod op het bewaren van gegevens inzake de creatie van inhoud invoert waarvan slechts bij wijze van uitzondering zou kunnen worden afgeweken. Hij vraagt zich niettemin af of dit standpunt aanvaardbaar is, gelet op de noodzaak om de in de artikelen 6 tot en met 8 en 11 van het Handvest verankerde grondrechten te eerbiedigen.

195. De verwijzende rechter verduidelijkt voorts dat zijn vraag ziet op de bewaarplicht die is neergelegd in artikel 6 LCEN, gelezen in samenhang met decreet nr. 2011-219. Tot de gegevens die de betrokken aanbieders van diensten uit dien hoofde dienen te bewaren, behoren onder meer de gegevens betreffende de burgerlijke identiteit van de personen die van die diensten hebben gebruikgemaakt, zoals hun naam, voornaam, hun bijbehorende postadressen, hun bijbehorende e-mail- of accountadressen, hun wachtwoorden en, wanneer het ondertekenen van het contract of het aanmaken van het account plaatsvindt tegen betaling, de gebruikte betaalsoort, de betalingsreferentie, het bedrag en de datum en het tijdstip van de transactie.

196. Tot de te bewaren gegevens behoren ook de identificatoren van de abonnees, van de verbindingen en van de gebruikte eindapparatuur, de aan de inhoud toegekende identificatoren, de datum en het tijdstip van het begin en het einde van de verbindingen en verrichtingen, en de soorten protocollen die zijn gebruikt voor de verbinding met de dienst en voor de overdracht van de inhoud. De bewaartermijn voor die gegevens bedraagt één jaar en er kan om toegang tot die gegevens worden verzocht in het kader van strafrechtelijke en civielrechtelijke procedures, om de regels inzake civielrechtelijke of strafrechtelijke aansprakelijkheid te doen naleven, en in het kader van maatregelen voor het inwinnen van inlichtingen waarop artikel L. 851-1 CSI van toepassing is.

197. In dit verband moet worden opgemerkt dat richtlijn 2000/31 volgens artikel 1, lid 2, bepaalde nationale bepalingen nader tot elkaar brengt die van toepassing zijn op de diensten van de informatiemaatschappij in de zin van artikel 2, onder a).

‡LW-BEHVMBJEH-GJDIBQW‡

198. Tot die diensten behoren onder meer die welke op individueel verzoek van een afnemer van diensten en gewoonlijk tegen vergoeding worden verricht via elektronische apparatuur voor de verwerking en de opslag van gegevens op afstand, zoals diensten waarbij toegang wordt verschaft tot het internet of tot een communicatienetwerk, en opslagdiensten (zie in die zin arresten van 24 november 2011, Scarlet Extended, C‑70/10, EU:C:2011:771, punt 40; 16 februari 2012, SABAM, C‑360/10, EU:C:2012:85, punt 34; 15 september 2016, Mc Fadden, C‑484/14, EU:C:2016:689, punt 55, en 7 augustus 2018, SNB-REACT, C‑521/17, EU:C:2018:639, punt 42 en aldaar aangehaalde rechtspraak).

199. Artikel 1, lid 5, van richtlijn 2000/31 bepaalt evenwel dat deze richtlijn niet van toepassing is op kwesties in verband met diensten van de informatiemaatschappij die onder richtlijnen 95/46 en 97/66 vallen. Dienaangaande blijkt uit de overwegingen 14 en 15 van richtlijn 2000/31 dat de bescherming van het vertrouwelijke karakter van communicatie en van natuurlijke personen in verband met de verwerking van persoonsgegevens in het kader van de diensten van de informatiemaatschappij uitsluitend wordt beheerst door richtlijnen 95/46 en 97/66. Laatstgenoemde richtlijn stelt ter waarborging van de vertrouwelijkheid van communicatie in artikel 5 een verbod op iedere vorm van onderschepping of bewaking van berichten.

200. Vragen die verband houden met de bescherming van het vertrouwelijke karakter van communicatie en van persoonsgegevens moeten derhalve worden beoordeeld aan de hand van richtlijn 2002/58 en verordening 2016/679, die in de plaats zijn gekomen van, respectievelijk, richtlijn 97/66 en richtlijn 95/46, waarbij moet worden aangetekend dat de bescherming die richtlijn 2000/31 beoogt te verzekeren, hoe dan ook geen afbreuk mag doen aan de vereisten die voortvloeien uit richtlijn 2002/58 en verordening 2016/679 (zie in die zin arrest van 29 januari 2008, Promusicae, C‑275/06, EU:C:2008:54, punt 57).

201. De bewaarplicht die de in punt 195 van het onderhavige arrest bedoelde nationale regeling oplegt aan aanbieders die het publiek online toegang geven tot communicatiediensten en aanbieders van opslagdiensten, en die betrekking heeft op de met die diensten verband houdende persoonsgegevens, moet dus worden getoetst aan richtlijn 2002/58 of verordening 2016/679, zoals de advocaat-generaal in wezen heeft opgemerkt in punt 141 van zijn conclusie in de gevoegde zaken La Quadrature du Net e.a. (C-511/18 en C-512/18, EU:C:2020:6).

202. Afhankelijk van de vraag of de levering van de diensten waarop die nationale regeling betrekking heeft, al dan niet onder richtlijn 2002/58 valt, zal die levering derhalve ofwel worden beheerst door deze richtlijn, in het bijzonder door artikel 15, lid 1, ervan, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, ofwel door verordening 2016/679, in het bijzonder door artikel 23, lid 1, van deze verordening, gelezen in het licht van dezelfde bepalingen van het Handvest.

203. Zoals de Europese Commissie in haar schriftelijke opmerkingen heeft gesteld, valt *in casu* niet uit te sluiten dat sommige van de diensten waarop de in punt 195 van het onderhavige arrest bedoelde nationale regeling betrekking heeft, elektronischecommunicatiediensten in de zin van richtlijn 2002/58 zijn, hetgeen de verwijzende rechter dient na te gaan.

204. In dit verband moet worden opgemerkt dat richtlijn 2002/58 van toepassing is op elektronischecommunicatiediensten die voldoen aan de voorwaarden die vermeld staan in artikel 2, onder c), van richtlijn 2002/21, waarnaar artikel 2 van richtlijn 2002/58 verwijst en waarin een elektronischecommunicatiedienst wordt gedefinieerd als 'een gewoonlijk tegen vergoeding aangeboden dienst die geheel of hoofdzakelijk bestaat in het overbrengen van signalen via elektronischecommunicatienetwerken, waaronder

‡LW-BEHVMBJEH-GJDIBQW‡

telecommunicatiediensten en transmissiediensten op netwerken die voor omroep worden gebruikt'. Wat de door richtlijn 2000/31 bestreken diensten van de informatiemaatschappij als bedoeld in de punten 197 en 198 van het onderhavige arrest betreft, deze diensten zijn elektronischecommunicatiediensten indien zij geheel of hoofdzakelijk bestaan in het overbrengen van signalen via elektronischecommunicatienetwerken. (zie in die zin arrest van 5 juni 2019, Skype Communications, C‑142/18, EU:C:2019:460, punten 47 en 48).

205. Internettoegangsdiensten, waarop de in punt 195 van het onderhavige arrest bedoelde nationale regeling van toepassing lijkt te zijn, zijn derhalve elektronischecommunicatiediensten in de zin van richtlijn 2002/21, zoals in overweging 10 van deze richtlijn wordt bevestigd (zie in die zin arrest van 5 juni 2019, Skype Communications, C‑142/18, EU:C:2019:460, punt 37). Dit geldt ook voor webgebaseerde e-maildiensten, die mogelijk eveneens onder die nationale regeling vallen, aangezien die diensten technisch gezien kunnen worden beschouwd als diensten die geheel of hoofdzakelijk bestaan in het overbrengen van signalen via elektronischecommunicatienetwerken (zie in die zin arrest van 13 juni 2019, Google, C‑193/18, EU:C:2019:498, punten 35 en 38).

206. Wat de vereisten betreft die voortvloeien uit artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, zij verwezen naar alle vaststellingen en beoordelingen in het kader van de beantwoording van de eerste vraag in de zaken C‑511/18 en C‑512/18 en de eerste en de tweede vraag in zaak C‑520/18.

207. Wat de uit verordening 2016/679 voortvloeiende vereisten betreft, zij eraan herinnerd dat deze verordening, zoals blijkt uit overweging 10 ervan, met name een consistent en hoog niveau van bescherming van natuurlijke personen binnen de Unie beoogt te waarborgen en daartoe een coherente en homogene toepassing van de regels inzake bescherming van de grondrechten van deze personen in verband met de verwerking van persoonsgegevens binnen de gehele Unie wil verzekeren (zie in die zin arrest van 16 juli 2020, Facebook Ireland en Schrems, C‑311/18, EU:C:2020:559, punt 101).

208. Daartoe moeten bij elke verwerking van persoonsgegevens, behoudens de op grond van artikel 23 van verordening 2016/679 toegestane uitzonderingen, de in hoofdstuk II van deze verordening neergelegde beginselen inzake verwerking van persoonsgegevens en de in hoofdstuk III van deze verordening geregelde rechten van de betrokkene worden geëerbiedigd. In het bijzonder moet elke verwerking van persoonsgegevens ten eerste in overeenstemming zijn met de in artikel 5 van verordening 2016/679 geformuleerde beginselen, en ten tweede voldoen aan de in artikel 6 van deze verordening opgesomde rechtmatigheidsvoorwaarden (zie naar analogie, met betrekking tot richtlijn 95/46, arrest van 30 mei 2013, Worten, C‑342/12, EU:C:2013:355, punt 33 en aldaar aangehaalde rechtspraak).

209. Wat meer bepaald artikel 23, lid 1, van verordening 2016/679 betreft, moet worden opgemerkt dat deze bepaling – net als artikel 15, lid 1, van richtlijn 2002/58 – de lidstaten de mogelijkheid biedt om met het oog op de erin genoemde doelstellingen via wetgevingsmaatregelen de reikwijdte van de erin bedoelde verplichtingen en rechten te beperken, "op voorwaarde dat die beperking de wezenlijke inhoud van de grondrechten en fundamentele vrijheden onverlet laat en in een democratische samenleving een noodzakelijke en evenredige maatregel is ter waarborging van" het nagestreefde doel. Elke op die grondslag vastgestelde wettelijke maatregel moet met name voldoen aan de specifieke vereisten die zijn geformuleerd in artikel 23, lid 2, van verordening 2016/679.

‡LW-BEHVMBJEH-GJDIBQW‡

210. Artikel 23, leden 1 en 2, van verordening 2016/679 kan derhalve niet aldus worden uitgelegd dat het de lidstaten de bevoegdheid kan verlenen om afbreuk te doen aan de eerbiediging van de persoonlijke levenssfeer, in strijd met artikel 7 van het Handvest, of aan de andere door het Handvest geboden waarborgen (zie naar analogie, met betrekking tot richtlijn 95/46, arrest van 20 mei 2003, Österreichischer Rundfunk e.a., C‑465/00, C‑138/01 en C‑139/01, EU:C:2003:294, punt 91). Net zoals geldt voor artikel 15, lid 1, van richtlijn 2002/58, is het met name zo dat de bevoegdheid die artikel 23, lid 1, van verordening 2016/679 de lidstaten verleent, slechts kan worden uitgeoefend in overeenstemming met het evenredigheidsvereiste, dat verlangt dat uitzonderingen op de bescherming van persoonsgegevens en beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven (zie naar analogie, met betrekking tot richtlijn 95/46, arrest van 7 november 2013, IPI, C‑473/12, EU:C:2013:715, punt 39 en aldaar aangehaalde rechtspraak).

211. Bijgevolg gelden de vaststellingen die zijn gedaan in het kader van de beantwoording van de eerste vraag in de zaken C‑511/18 en C‑512/18 en van de eerste en de tweede vraag in zaak C‑520/18, en de beoordelingen die in dat kader zijn verricht, *mutatis mutandis* voor artikel 23 van verordening 2016/679."

Concluderend heeft het Hof van Justitie voor recht verklaard:

"Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000, betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt ('richtlijn inzake elektronische handel') moet aldus worden uitgelegd dat zij niet van toepassing is op de bescherming van het vertrouwelijke karakter van communicatie en van natuurlijke personen in verband met de verwerking van persoonsgegevens in het kader van de diensten van de informatiemaatschappij. Deze bescherming wordt, naargelang van het geval, beheerst door richtlijn 2002/58, zoals gewijzigd bij richtlijn 2009/136, of door verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG (algemene verordening gegevensbescherming) . Artikel 23, lid 1, van verordening 2016/679, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, moet aldus worden uitgelegd dat het zich verzet tegen een nationale regeling waarbij aanbieders die het publiek online toegang verlenen tot communicatiediensten en aanbieders van opslagdiensten een verplichting tot algemene en ongedifferentieerde bewaring van met name de met die diensten verband houdende persoonsgegevens wordt opgelegd."

6. Tot slot dient bijzondere aandacht besteed te worden aan het verzoek dat het Grondwettelijk Hof in arrest 57/2021 geformuleerd heeft.

Er wordt aan herinnerd dat het Grondwettelijk Hof het volgende heeft geoordeeld:

– Er is een verandering van gezichtspunt vereist ten opzichte van de keuze die de wetgever heeft gemaakt: de verplichting tot bewaring van gegevens met betrekking tot elektronische communicatie moet de uitzondering zijn, en niet de regel.

– De regeling waarbij in een dergelijke verplichting wordt voorzien, moet daarenboven onderworpen zijn aan duidelijke en nauwkeurige regels over de reikwijdte en de toepassing van de betrokken maatregel, waarbij een minimum aan vereisten worden opgelegd.

‡LW-BEHVMBJEH-GJDIBQW‡

– Die regeling moet waarborgen dat de inmenging tot het strikt noodzakelijke wordt beperkt en moet steeds "beantwoorden aan objectieve criteria die een verband leggen tussen de te bewaren gegevens en het nagestreefde doel".

Daartoe staat het aan de wetgever tussen de verschillende soorten aan bewaring onderworpen gegevens het onderscheid te maken dat geboden is, zodat wordt gewaarborgd dat, voor elk soort gegeven, de inmenging tot het strikt noodzakelijke wordt beperkt.

I.2. DE RECHTSPRAAK VAN HET EUROPEES HOF VOOR DE RECHTEN VAN DE MENS

Meer in het algemeen dient ook rekening gehouden te worden met het recht op eerbiediging van het privéleven, dat gewaarborgd wordt bij artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden en bij artikel 22 van de Grondwet.[12]

Uit de rechtspraak van het Europees Hof voor de Rechten van de Mens[13], meer in het bijzonder wat betreft het geheim toezicht op en de massale onderschepping van communicatie en de daarmee verband houdende gegevens, moet in wezen met de volgende beginselen rekening gehouden worden:

– 1° geheim toezicht op burgers kan slechts aanvaard worden voor zover het strikt noodzakelijk is voor de bescherming van de democratische instellingen. Wetsbepalingen waarbij bevoegdheden verleend worden inzake geheim toezicht op correspondentie, postzendingen en telecommunicatie, zijn, in een uitzonderlijke situatie zoals de bedreiging door complexe vormen van spionage en terrorisme, in een democratische samenleving noodzakelijk voor de nationale veiligheid en/of de bescherming van de openbare orde en het voorkomen van strafbare feiten;

– 2° de invoering van een dergelijke regeling moet echter "bij wet voorzien" en "noodzakelijk" zijn; in dit kader onderzoekt het Europees Hof voor de Rechten van de Mens of het nationaal juridisch kader een duidelijke definitie bevat van:

1. de redenen waarom massale onderschepping toegestaan kan worden;

2. de omstandigheden waarin de communicatie van een persoon onderschept mag worden;

3. De procedure voor het verlenen van een machtiging;

4. De procedure die gevolgd moet worden voor de selectie, het onderzoek en het gebruik van de onderschepte gegevens.

[12] Zie onder meer L. TASSONE, "*La protection des données dans la jurisprudence de la Cour européenne des droits de l'homme*" in Enjeux européens et mondiaux de la protection des données personnelles, A. Grosjean (ed.), Larcier, coll. Création Information Communication, 53 e.v., en de verwijzingen aldaar; over de inlichtingen- en veiligheidsdiensten zie onder meer advies 42.178/2.

[13] Zie onder meer het principearrest, EHRM, arrest-*Klass e.a. t. Duitsland*, 9 september 1978. Zie EHRM, arrest *Big Brother watch en anderen t. Verenigd Koninkrijk*, 25 mei 2021, 322 tot 364 voor een recente herinnering aan de rechtspraak ter zake en de beginselen die daaruit voortvloeien.

‡LW-BEHVMBJEH-GJDIBQW‡

5. De voorzorgen die genomen moeten worden voor het mededelen van die gegevens aan andere partijen.

6. De beperkingen die gelden voor de duur van de onderschepping en voor de termijn waarin de onderschepte gegevens bewaard mogen worden, alsook de omstandigheden waarin die gegevens gewist of vernietigd moeten worden.

7. De procedures en nadere regels met betrekking tot het toezicht, door een onafhankelijke instantie, op de naleving van de hierboven vermelde waarborgen en de bevoegdheden van die instantie in geval van niet-naleving;

8. De procedures voor het onafhankelijk toezicht achteraf op de naleving van de waarborgen en de bevoegdheden die aan de bevoegde instantie verleend worden voor het behandelen van gevallen van niet-naleving.

Het proces moet derhalve afgebakend worden met "end-to-end-waarborgen", die het mogelijk maken zich ervan te vergewissen dat de noodzaak en de proportionaliteit van de genomen maatregelen in elke fase van het toezichtproces beoordeeld worden, inzonderheid bij het onderscheppen van gegevens; die waarborgen[14] houden onder andere in dat

– voor onderscheppingsactiviteiten, althans voor massale onderscheppingsactiviteiten , van meet af aan, d.w.z. bij de omschrijving van de bedoeling en de omvang van de activiteit, een vergunning verleend moet zijn door een onafhankelijke instantie;

– de activiteiten moeten worden onderworpen aan een onafhankelijk toezicht en aan een onafhankelijke controle die achteraf uitgevoerd wordt.[15]

ONDERZOEK VAN HET VOORONTWERP

VOORAFGAANDE OPMERKING

Voordat enige andere opmerking gemaakt wordt, dient eraan herinnerd te worden dat het Grondwettelijk Hof in arrest nr. 57/2021, dat volgt op het arrest *La Quadrature du Net*, de wetgever verzocht heeft om van gezichtspunt te veranderen wat de bewaring van de desbetreffende gegevens betreft opdat die de uitzondering zou blijven en niet de regel zou worden, en dat voor die bewaring duidelijke en nauwkeurige regels over de reikwijdte en de toepassing van de betrokken maatregel zouden gelden en dat daarbij een minimum aan regels opgelegd zou worden, zodat de inmenging tot het strikt noodzakelijke beperkt wordt en

[14] Zie in dat verband onder meer EHRM, *arrest Big brother watch e. a. t. Verenigd Koninkrijk*, 25 mei 2021, 350.

[15] Het Europees Hof voor de Rechten van de Mens heeft in dat verband het volgende geoordeeld: "(…) qu'en ce qui concerne l'interception en masse, l'interception et la conservation des données de communication associées, ainsi que les recherches effectuées sur celles-ci, doivent être analysées au regard des mêmes garanties que celles applicables au contenu des communications, mais qu'il n'est pas nécessaire que les dispositions juridiques régissant le traitement des données de communication associées soient identiques en tous points à celles régissant le traitement du contenu des communications". Het Hof is hoe dan ook van mening dat het vereiste van een onafhankelijke vergunning voor beide categorieën geldt (zie in dit verband onder andere EHRM, *Big Brother watch e.a. t. Verenigd Koninkrijk*, 25 mei 2021, 363 en 364, en 417 en 418).

‡LW-BEHVMBJEH-GJDIBQW‡

beantwoordt aan objectieve criteria die een verband leggen tussen de te bewaren gegevens en het nagestreefde doel. Het Grondwettelijk Hof heeft gesuggereerd dat de wetgever daartoe tussen de verschillende soorten aan bewaring onderworpen gegevens het onderscheid zou maken dat geboden is.

Voorliggend voorontwerp strekt ertoe duidelijk tegemoet te komen aan dat arrest, door binnen de bakens te blijven die aldus door het Grondwettelijk Hof uitgezet zijn.

Het voorontwerp geeft echter aanleiding tot verscheidene algemene opmerkingen, met name op het stuk van de beperking tot het strikt noodzakelijke voor alle ontworpen regelingen inzake bewaring die opgezet worden per categorie van gegevens en per doeleinde, de duidelijkheid en de nauwkeurigheid van de ontworpen regelingen en hun verenigbaarheid met het legaliteitsbeginsel dat in artikel 22 van de Grondwet verankerd is, naast de bijzondere opmerkingen die vervolgens geformuleerd zullen worden.

ALGEMENE OPMERKINGEN

Het opleggen, aan de aanbieders van elektronischecommunicatiediensten, van een bevel tot een algemene en ongedifferentieerde bewaring van de verkeers- en locatiegegevens ter bescherming van de nationale veiligheid, in situaties waarin de Staat geconfronteerd wordt met een ernstige bedreiging van de nationale veiligheid die werkelijk en actueel of voorzienbaar blijkt

1. Er zij aan herinnerd dat volgens de lering van het arrest *La Quadrature du Net* ingestemd kan worden met een wettelijke regeling die het mogelijk maakt om aan de aanbieders van elektronische communicatiediensten een bevel te geven tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens ter bescherming van de nationale veiligheid in situaties waarin de Staat geconfronteerd wordt met een ernstige bedreiging van de nationale veiligheid die werkelijk en actueel of voorzienbaar blijkt.

De beslissing waarbij een dergelijk bevel opgelegd wordt, dient evenwel effectief getoetst te kunnen worden door een rechterlijke instantie of een onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij het doel van die toetsing erin bestaat na te gaan of een van die situaties zich voordoet en of voldaan is aan de voorwaarden en waarborgen waarin voorzien moet worden. Bovendien mag dat bevel slechts opgelegd worden voor een periode die niet langer is dan strikt noodzakelijk, maar die verlengd kan worden indien die bedreiging voortduurt.

2.1.1. Artikel 31 van voorliggend voorontwerp strekt ertoe in de wet van 30 november 1998 'houdende regeling van de inlichtingen– en veiligheidsdiensten', een artikel 18/17/1 in te voegen, luidende:

> "De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten en in geval van een reële, actuele of voorzienbare ernstige bedreiging van de nationale veiligheid, de medewerking vorderen van operatoren voor het algemeen en ongedifferentieerd bewaren van verkeers- en lokalisatiegegevens van elektronische communicatie die door hen wordt gegenereerd en verwerkt.

‡LW-BEHVMBJEH-GJDIBQW‡

De vordering wordt schriftelijk gedaan door het diensthoofd en vermeldt, naargelang het geval, de aard van het eensluidend advies van de commissie, de aard van het eensluidend advies van de voorzitter van de commissie of de aard van de toelating van de betrokken minister bedoeld in artikel 18/10, § 3, derde lid.

De machtiging van het diensthoofd wordt overgemaakt aan de bevoegde minister.

De betrokken inlichtingen- en veiligheidsdienst kan de medewerking vorderen van het Instituut bedoeld in artikel 2, 1° van de wet van 13 juni 2005 betreffende de elektronische communicatie, om de vordering aan alle betrokken operatoren over te maken.

Het diensthoofd kan bij schriftelijke beslissing vorderen dat personen van wie hij veronderstelt dat zij over de nodige technische deskundigheid beschikken, medewerking verlenen bij de tenuitvoerlegging van deze methode. De vordering vermeldt, naargelang het geval, de aard van de instemming van de commissie, de aard van de instemming van de voorzitter van de commissie of de aard van de toelating van de betrokken minister.

Eenieder die weigert de vereiste bewaring te verrichten, wordt gestraft met een geldboete van zesentwintig euro tot tienduizend euro.

De methode wordt toegestaan voor een periode die niet langer mag zijn dan 6 maanden onverminderd de procedure bedoeld in artikel 18/10, § 5.

De betrokken inlichtingen– en veiligheidsdienst brengt om de twee maanden bij de Commissie verslag uit over de evolutie van de dreiging. In dit verslag worden de elementen belicht die hetzij de handhaving van de algemene en ongedifferentieerde bewaring, hetzij de beëindiging ervan rechtvaardigen.

De Koning kan, op voorstel van de Minister van Justitie, de Minister van Defensie en de Minister bevoegd voor de elektronische communicatie, nadere regels voor de samenwerking met de operatoren bepalen."

2.1.2. Er dient vastgesteld te worden dat de ontworpen bepaling tegemoetkomt aan de vereisten van het Europees recht voor zover de mogelijkheid om aan de operatoren een bevel te geven daarbij alleen geboden wordt ter bescherming van de nationale veiligheid in situaties waarin de Staat geconfronteerd wordt met een ernstige bedreiging van de nationale veiligheid die reëel en actueel of voorzienbaar blijkt.

2.1.3. Met betrekking tot de duur van de operatie – die tot het strikt noodzakelijke beperkt moet worden – wordt in de in te voeren regeling bepaald dat:

– die duur beperkt wordt tot maximaal zes maanden, met dien verstande dat de betrokken inlichtingen- en veiligheidsdienst om de twee maanden bij de Commissie[16] een verslag aangaande de evolutie van de dreiging moet indienen waarvan het de bedoeling is dat daarin de elementen belicht worden die hetzij de handhaving van de algemene en ongedifferentieerde bewaring, hetzij de beëindiging ervan rechtvaardigen.

[16] Het gaat om de Commissie ingesteld bij artikel 43/1 van de wet van 30 november 1998.

‡LW-BEHVMBJEH-GJDIBQW‡

– die duur verlengd kan worden onder de strikte voorwaarden bepaald in artikel 18/10, § 5, van de wet van 30 november 1998.[17]

Met die regeling, die voortvloeit uit het in onderlinge samenhang lezen van het thans geldende artikel 18/10 en het ontworpen artikel 18/17/1 van de wet van 30 november 1998, kan aldus blijkbaar voldaan worden aan de vereisten die voortvloeien uit het Europees recht op dat punt.

2.1.4.1. Er doen zich evenwel moeilijkheden voor in verband met de vraag of de voorgenomen operatie onderworpen is aan:

– "de instemming vanwege een onafhankelijke autoriteit vanaf het begin - zodra de bedoeling en de reikwijdte van de operatie bepaald zijn" – overeenkomstig de rechtspraak van het Europees Hof voor de Rechten van de Mens, in het bijzonder het arrest *Big Brother watch*[18];

– "een effectieve toetsing", hetzij door een rechterlijke instantie, hetzij door een onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij het doel van die toetsing is om na te gaan of een van die situaties zich voordoet en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien" – volgens de bewoordingen van de rechtspraak van het Hof van Justitie.

2.1.4.2. Wat het arrest *Big Brother watch* betreft, heeft het Europees Hof voor de Rechten van de Mens, zoals eerder vermeld, het volgende geoordeeld:

> "(…) que l'interception en masse, l'interception et la conservation des données de communication associées, ainsi que les recherches effectuées sur celles-ci, doivent être analysées au regard des mêmes garanties que celles applicables au contenu des communications, mais qu'il n'est pas nécessaire que les dispositions juridiques régissant le traitement des données de communication associées soient identiques en tous points à celles régissant le traitement du contenu des communications ."

Het Hof gaat er hoe dan ook van uit dat het vereiste van een onafhankelijke machtiging voor die beide categorieën geldt.

---

[17] Die bepaling luidt als volgt:
"Het diensthoofd kan, op voorafgaand eensluidend advies van de commissie, de verlenging van de uitzonderlijke methode voor het verzamelen van gegevens machtigen voor een nieuwe termijn die niet langer mag zijn dan twee maanden te rekenen vanaf het verstrijken van de lopende methode, onverminderd zijn verplichting om de methode te beëindigen zodra de potentiële dreiging die haar rechtvaardigt weggevallen is, wanneer de methode niet langer nuttig is voor het doel waarvoor zij werd beslist of wanneer hij een onwettigheid vaststelt. In dat geval brengt het diensthoofd van de betrokken dienst zijn met redenen omklede beslissing om de methode te beëindigen ter kennis van de commissie.
Een tweede en elke volgende verlenging van de uitzonderlijke methode voor het verzamelen van gegevens is slechts mogelijk indien er bijzondere omstandigheden aanwezig zijn, die de verlenging van het gebruik van deze methode noodzaken. Deze bijzondere redenen worden in de beslissing opgenomen. Indien deze bijzondere omstandigheden niet voorhanden zijn, dient de methode te worden beëindigd.
De voorwaarden bepaald in de paragrafen 1 tot 3 zijn toepasselijk op de in deze paragraaf bepaalde wijzen van verlenging van de uitzonderlijke methode voor het verzamelen van gegevens."
Bovendien moet opgemerkt worden dat luidens artikel 18/10, § 1, van de wet van 30 november 1998 "[h]et diensthoofd (…) de uitzonderlijke methode [beëindigt] wanneer de ernstige potentiële dreiging die haar rechtvaardigt weggevallen is, wanneer de methode niet langer nuttig is voor het doel waarvoor zij werd ingesteld, of wanneer hij een onwettigheid heeft vastgesteld. Hij brengt zijn beslissing zo spoedig mogelijk ter kennis van de Commissie."

[18] Zie in dat verband, onder meer, EHRM, arrest *Big Brother watch e. a. t. Verenigd Koninkrijk*, 25 mei 2021, 350.

‡LW-BEHVMBJEH-GJDIBQW‡

Op een vraag in dat verband hebben de gemachtigden van de minister het volgende geantwoord met betrekking tot de strekking van het begrip "l'interception et la conservation des données de communication associées":

> "Door deze niet afzonderlijk te benoemen, impliceert het Hof volgens (…) dat haar conclusie enkel van toepassing is wanneer ook de bulk interceptie van de inhoud van communicatie georganiseerd wordt. Het Hof spreekt zich niet uit over de bewaring van enkel de meta-data, waarbij verondersteld mag worden dat deze maatregel minder intrusief is dan het bewaren van de inhoud van de communicatie.
>
> Minder intrusief, maar nog steeds intrusief. Daarom voorzien we de waarborg van de BIM-commissie die voorafgaandelijk toestemming moet geven in het geval van een ernstige dreiging tegen de nationale veiligheid, of een mechanisme dat in de wet beschreven staat dat ook betrekking heeft op de nationale veiligheid."

In het licht van de aldus verstrekte toelichtingen dient inderdaad vastgesteld te worden dat in het arrest *Big Brother watch* geen uitspraak gedaan wordt over een regeling die louter betrekking zou hebben op de bewaring van gegevens die verband houden met de inhoud van elektronische communicaties, maar wel over een regeling betreffende zowel het onderscheppen van de inhoud als de metagegevens, waarbij dat onderscheppen niet alleen betrekking had op de opslag en de bewaring van die gegevens, maar ook op de toegang tot en de analyse van die gegevens.[19]

Het lijkt dan ook een hachelijke zaak de lering van dat arrest, in het bijzonder de vereisten inzake de voorafgaande toetsing door een rechterlijke instantie of een onafhankelijke instelling, ook te laten gelden voor het mechanisme van de algemene en ongedifferentieerde bewaring dat in de ontworpen tekst in het vooruitzicht gesteld wordt.

Indien dat toch het geval zou zijn, dan zou erop gewezen moeten worden dat uit artikel 18/10, § 1, van de wet van 30 november 1998 blijkt dat het diensthoofd zijn beslissing slechts kan nemen op eensluidend advies van de commissie. Zo moet de commissie onderzoeken "of de wettelijke bepalingen voor het aanwenden van de uitzonderlijke methode voor het verzamelen van gegevens, alsook de in artikel 18/9 §§ 2 en 3, bepaalde principes van proportionaliteit en subsidiariteit, zijn nageleefd en (…) de door § 2 voorgeschreven vermeldingen" controleren.

Die commissie, waarvan in artikel 43/1, § 1 van de wet van 30 november 1998 bepaald wordt dat ze samengesteld is uit magistraten en in de uitoefening van haar controleopdrachten volledig onafhankelijk handelt, beantwoordt aan het begrip "onafhankelijke bestuurlijke autoriteit" in de zin van de hiervoor aangehaalde rechtspraak. Haar eensluidend advies is bindend: krachtens artikel 18/10, § 3, tweede lid, mag de geplande operatie niet verricht worden indien haar advies negatief is.

[19] Zie met betrekking tot de door het Europees Hof voor de Rechten van de Mens onderzochte regeling de punten 15 tot en met 17 van dat arrest.

‡LW-BEHVMBJEH-GJDIBQW‡

Niettemin luidt artikel 18/10, § 3, derde lid, van de wet van 30 november 1998 als volgt:

> "Indien de commissie geen advies uitbrengt binnen de termijn van vier dagen of zij de betrokken dienst meedeelt dat zij niet kan beraadslagen binnen die termijn overeenkomstig artikel 43, § 1, zevende lid, kan de betrokken dienst de bevoegde minister aanzoeken, die al dan niet toelating geeft om zo spoedig mogelijk de beoogde methode uit te voeren. De minister deelt zijn beslissing mee aan de voorzitters van de commissie en van het Vast Comité I."

In beide genoemde gevallen wordt de beslissing om de operatie toe te staan door de minister genomen indien de commissie geen advies uitbrengt. De minister is evenwel geen "onafhankelijke bestuurlijke autoriteit" waarvan de medewerking vereist zou zijn.[20]

2.1.4.3. In het licht van de opdrachten die bij de artikelen 43/2 en volgende van de wet van 30 november 1998 aan het Vast Comité I toevertrouwd worden, lijkt de in te voeren regeling geen moeilijkheden op te leveren in het licht van de door het Hof van Justitie vermelde controlevereisten.

2.2. Het ontworpen dispositief geeft in het licht van het grondwettelijk recht evenwel aanleiding tot een fundamentele opmerking.

Zo veronderstelt de "algemene en ongedifferentieerde" bewaring waarin het ontworpen artikel 18/17/1 voorziet, dat een bevel gegeven wordt aan alle operatoren die diensten voor elektronische communicatie leveren. Zelfs indien slechts bepaalde vooraf aangewezen operatoren verplicht zouden zijn om de gegevens in kwestie te bewaren, zou hen aldus niettemin het bevel gegeven worden om de verkeers- en locatiegegevens op een algemene en ongedifferentieerde wijze te bewaren.

Zelfs indien het om een in de tijd beperkt bevel zou gaan, vormt dergelijk bevel geen bestuurshandeling met individuele strekking, maar is het algemeen en abstract van aard, terwijl het aan de operatoren gericht is. Bijgevolg is de beslissing waarbij die "algemene en ongedifferentieerde" bewaring opgelegd wordt van verordenende aard.

Met betrekking tot het toekennen van een bevoegdheid van verordenende aard aan een overheid die geen politieke verantwoording verschuldigd is aan de betrokken wetgevende vergaderingen – dat wil zeggen aan een andere overheid dan de Koning die handelt met medeondertekening van een minister, of dan een minister – heeft de afdeling Wetgeving in het verleden er al meermaals op gewezen dat het toekennen van een reglementaire bevoegdheid aan ambtenaren of aan openbare instellingen of organen ervan, moeilijk in overeenstemming te brengen valt met de algemene principes van het Belgisch publiekrecht (artikelen 33 en 108 van de Grondwet), aangezien daardoor geraakt wordt aan het beginsel van de eenheid van de verordenende macht en ter zake iedere rechtstreekse parlementaire controle ontbreekt. Verordeningen van die aard ontberen daarenboven de waarborgen waarmee de klassieke regelgeving gepaard gaat, zoals die inzake bekendmaking. Als er in het verleden al uitzonderingen op het delegatieverbod van reglementaire bevoegdheid aan openbare instellingen

[20] Zie EHRM, arrest van 25 mei 2021, *Big Brother watch e.a. t. Verenigd Koninkrijk*, 377.

‡LW-BEHVMBJEH-GJDIBQW‡

aanvaardbaar geacht zijn door de afdeling Wetgeving, betrof het doorgaans delegaties met een beperkte draagwijdte of betreffende nevenaspecten en van een zodanig technische aard dat ervan uitgegaan mocht worden dat de instellingen die de betrokken reglementering dienden toe te passen, ook het best geplaatst waren om die reglementering uit te werken.[21]

De principiële beslissing om de algemene en ongedifferentieerde bewaring van de verkeers- en locatiegegevens van de elektronische communicatiemiddelen op te leggen, is uiteraard geen beslissing met een beperkte draagwijdte of betreffende nevenaspecten en ze is evenmin van een zodanig technische aard dat ze er gegrond redenen bestaan om de bevoegdheid daartoe op te dragen aan personeelsleden van de inlichtingen- en veiligheidsdiensten.

Onder voorbehoud van de opmerkingen 2.1.4.2 en 2.1.4.3 staat het uiteindelijk aan de Koning om een dergelijke algemene en abstracte beslissing te nemen.

De ontworpen tekst moet in het licht van deze opmerking herzien worden.

2.3. Het systeem dat bij voorliggend voorontwerp ingevoerd wordt, kan leiden tot een ander geval waarin tot een algemene en ongedifferentieerde bewaring van metagegevens beslist zou worden.

Het gaat om het geval bedoeld in het ontworpen artikel 126/1, § 3, eerste lid, 2°, van de wet van 13 juni 2005, dat voorziet in de bewaring van de gegevens inzake elektronische communicatie, bedoeld in paragraaf 2 van datzelfde artikel, in alle zones waar het algemeen dreigingsniveau, vastgesteld op basis van de wet van 10 juli 2006 'betreffende de analyse van de dreiging', ten minste niveau 3 bedraagt, overeenkomstig artikel 11 van het koninklijk besluit van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging, en zolang niveau 3 of 4 geldt.

Dat geval wordt aldus, overeenkomstig de bedoeling van de stellers van het voorontwerp, bepaald in het licht van de situaties waarin de gegevens op een gerichte wijze bewaard moeten worden en niet van situaties waarin een algemene en ongedifferentieerde bewaring van gegevens vereist wordt.

Uit het recent verleden is evenwel gebleken dat dreigingsniveau 3 voor het volledige grondgebied van het Rijk kan gelden en dat, in voorkomend geval, zelfs voor een relatief lange periode.

In het geval waarbij dreigingsniveau 3 voor het volledige grondgebied zou gelden, zou dat systeem dus neerkomen op een algemene en ongedifferentieerde bewaring van de metagegevens. Voorzichtigheidshalve moet er dus van uitgegaan worden dat voor deze specifieke situatie de beginselen betreffende de algemene en ongedifferentieerde bewaring toepassing vinden en niet die betreffende de gerichte bewaring.

[21] Zie in dat verband, onder andere, advies 69.160/4 d.d. 6 mei 2021 over een voorontwerp van wet 'tot invoering van bijkomende beveiligingsmaatregelen voor de verstrekking van mobiele 5G-diensten' en advies 69.166/4 d.d. 10 juni 2021 over voorontwerp van wet 'houdende omzetting van het Europees wetboek voor elektronische communicatie en wijziging van diverse bepalingen inzake elektronische communicatie'.

‡LW-BEHVMBJEH-GJDIBQW‡

Wat dat specifieke geval betreft, lijkt de ontworpen regeling te voldoen aan de eerder genoemde vereisten inzake het doel van de gegevensbewaring[22] en de beperking ervan in de tijd.[23]

De vraag rijst evenwel op welke manier voldaan zal worden aan het vereiste van de "effectieve toetsing" in de zin van de hiervoor aangehaalde rechtspraak.

De ontworpen tekst moet in het licht van die opmerking herzien en aangevuld worden.

De afgebakende en gerichte bewaring van verkeers- en locatiegegevens ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid

1. Er wordt aan herinnerd dat volgens de lering van het arrest *La Quadrature du Net* een gerichte bewaring van verkeers- en locatiegegevens, die op basis van objectieve en niet-discriminatoire factoren afgebakend wordt aan de hand van categorieën betrokken personen of aan de hand van een geografisch criterium, voor een periode die niet langer is dan strikt noodzakelijk, maar die verlengd kan worden, aanvaard kan worden ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid.

2. Voorliggend voorontwerp strekt ertoe een dergelijke bewaring te regelen door in de wet van 13 juni 2005 een nieuw artikel 126/1 in te voegen.

In essentie voorziet die bepaling in de bewaring van drie categorieën verkeers- en locatiegegevens die opgesomd worden in paragraaf 2 (de gegevens met betrekking tot de toegang en de verbinding, de communicatiegegevens en de gegevens van oproeppogingen zonder resultaat). De Koning wordt ermee belast te bepalen welke gegevens van die drie categorieën bewaard moeten worden en aan welke vereisten die gegevens moeten beantwoorden.

3. Naar luid van de ontworpen paragraaf 1, derde lid, van dat artikel worden die gegevens bewaard ten behoeve van de vrijwaring van de nationale veiligheid, de strijd tegen zware criminaliteit, de preventie van ernstige dreigingen van de openbare veiligheid, en de bescherming van de vitale belangen van een natuurlijke persoon.

[22] De regeling die bij de wet van 10 juli 2006 en het koninklijk besluit van 28 november 2006 ingevoerd is, is in de eerste plaats bedoeld om te gelden voor bedreigingen die verband houden met terrorisme en extremisme (zie artikel 3 van de wet van 10 juli 2006 en artikel 8, 1°, b) en c) van de wet van 30 november 1998). Overeenkomstig artikel 11, § 6, van het koninklijk besluit van 28 november 2006 stemt dreigingsniveau3 stemt overeen met een "ernstige" bedreiging, namelijk een bedreiging die "mogelijk en waarschijnlijk" is, terwijl dreigingsniveau 4 overeenkomt met een "zeer ernstige" bedreiging, namelijk een bedreiging die "ernstig en zeer nabij" is.

[23] In de betrokken zones is de gegevensbewaring van toepassing zolang daar dreigingsniveau 3 of 4 van kracht is.

‡LW-BEHVMBJEH-GJDIBQW‡

Die doeleinden stemmen uitdrukkelijk overeen met die vermeld in het arrest *La Quadrature du Net*, met uitzondering van "de bescherming van de vitale belangen van een natuurlijke persoon". Wat dat doeleinde betreft, valt evenwel op te merken dat het deel uitmaakt van een andere context dan die van de prejudiciële vragen waarop het Hof van Justitie geantwoord heeft in zijn arrest *La Quadrature du Net*.

Een dergelijk doeleinde kan hoe dan ook *a priori* geacht worden te vallen onder de bescherming van de openbare veiligheid en onder de positieve verplichtingen die in dat verband op de Lidstaten rusten ter bescherming van het leven en de veiligheid van personen.

Wat het doeleinde van de bewaring betreft, lijkt het ontworpen artikel 126/1 derhalve geen moeilijkheden op te leveren in het licht van de rechtspraak van het Hof van Justitie en het Grondwettelijk Hof.

4.1.1. Het richten van de betrokken bewaring steunt op het bepalen van verschillende categorieën van geografische zones die opgesomd worden in paragraaf 3 van het ontworpen artikel, namelijk:

1° de gerechtelijke arrondissementen waar gemiddeld minstens drie strafbare feiten zoals bedoeld in artikel 90*ter* van het Wetboek van Strafvordering per duizend inwoners per jaar vastgesteld zijn tijdens de drie jaren voorafgaand aan het lopende jaar, alsook de politiezones die dezelfde kenmerken vertonen maar gelegen zijn in een gerechtelijk arrondissement dat niet aan de voormelde voorwaarden voldoet;

2° de zones waar het dreigingsniveau, vastgesteld krachtens de wet van 10 juli 2006 ten minste niveau 3 is, en zolang in die zones ten minste dreigingsniveau 3 blijft bestaan;

3° de gebieden die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit; als tot die categorie behorend worden vermeld de havens, de spoorwegstations, de metro– en de pre-metrostations, de gebouwen bestemd voor allerlei diensten, zoals justitie, de lokale en de federale politie en douane en accijnzen; eveneens vermeld worden de gemeenten waar zich militaire domeinen bevinden, de gevangenissen en de transitiehuizen, de wapenkamers en schietstanden, de faciliteiten bedoeld in de regelgeving inzake de bescherming tegen ioniserende stralingen, de SEVESO-inrichtingen, de gemeenten waar zich kritieke infrastructuren bevinden, het ASTRID-netwerk, alsook de informatienetwerken en – systemen ter ondersteuning van het verlenen van essentiële diensten door operatoren van essentiële diensten;

4° de zones waar er een mogelijke ernstige bedreiging is voor de vitale belangen van het land of de essentiële behoeften van de bevolking; in dat verband worden vermeld de neutrale zones en de ministeriële kabinetten, de gebouwen die bestemd zijn voor rechtspersonen waarvan het economisch en wetenschappelijk potentieel beschermd moet worden en die opgenomen zijn in een lijst die jaarlijks door de staatsveiligheid en de algemene inlichtingen- en veiligheidsdienst opgesteld wordt op voorstel van de minister van Justitie en Defensie en door de Nationale Veiligheidsraad goedgekeurd wordt, de autosnelwegen en de bijhorende openbare parkeerterreinen, de wetgevende vergaderingen, de gemeentehuizen, de

‡LW-BEHVMBJEH-GJDIBQW‡

zetels van de provincieraden, het koninklijk paleis, de koninklijke domeinen, de gebouwen bestemd voor allerlei diensten zoals justitie, de lokale en de federale politie, alsook voor de Veiligheid van de Staat; eveneens vermeld worden de gemeenten waar zich militaire domeinen bevinden, de grensgemeenten, de ziekenhuizen en de Nationale Bank van België;

5° de zones waar er een mogelijk ernstige bedreiging bestaat voor de belangen van de internationale instellingen; in dat verband wordt melding gemaakt van de ambassades en diplomatieke vertegenwoordigingen, de gebouwen bestemd voor de Europese Unie en voor de NAVO, de kantoren van de instellingen van de Europese Economische Ruimte en de kantoren van de Verenigde Naties.

De autoriteiten die bevoegd zijn voor een van de aangelegenheden in verband met de bestemming van de zone worden ermee belast jaarlijks op de door de Koning vastgestelde datum aan de door de Koning aangewezen dienst de gegevens mee te delen die nodig zijn voor de concrete vaststelling van de geografische zones. Wanneer een geografische zone niet langer aan bedoeld criterium voldoet, zijn die autoriteiten er tevens toe gehouden deze dienst daarvan onverwijld in kennis stellen, zodat de verplichting tot bewaring zo spoedig mogelijk beëindigd kan worden. De lijst van de zones wordt elk jaar bijgewerkt en naar gelang van het geval ter beschikking gesteld van het Vast Comité I, door de inlichtingen- en veiligheidsdiensten, of van het Controleorgaan van de politionele informatie.

4.1.2. Voor de zones die behoren tot een van de categorieën die vermeld worden in de hiervoor geciteerde punten 3°, 4° en 5° wordt bepaald dat, bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie, en van de minister bevoegd voor de elektronische communicatie, na raadpleging van de bevoegde gegevensbeschermingsautoriteiten en van het Belgisch Instituut voor postdiensten en telecommunicatie (hierna "het Instituut"), door de Koning bijkomende zones bepaald kunnen worden, met dien verstande dat dit besluit om de drie jaar hernieuwd moet worden. Indien dat besluit binnen die termijn niet hernieuwd wordt, vervalt de verplichting tot bewaring wat de bijkomende geografische zones betreft, en dit tot een nieuw koninklijk besluit van kracht wordt.

Voorts wordt nog het volgende bepaald:

> "Categorieën van geografische zones kunnen enkel opgenomen worden ter vrijwaring van de nationale veiligheid, of indien er in deze zones op basis van objectieve en niet-discriminerende elementen kan worden vastgesteld dat er een situatie bestaat die wordt gekenmerkt door een hoog risico op het voorbereiden of plegen van daden van zware criminaliteit."

4.1.3. Bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie, en van de minister bevoegd voor elektronische communicatie, na raadpleging van de bevoegde gegevensbeschermingsautoriteiten en van het Instituut, kan de Koning bovendien bepalen welke technische parameters en gegevens de operatoren dienen te gebruiken om de gegevensopslag tot de bedoelde zones te beperken, de lijst opstellen van de verschillende autoriteiten die bevoegd zijn voor de aangelegenheden in kwestie, de procedures bepalen voor de mededeling van informatie door de bevoegde autoriteiten aan de door de Koning aangewezen dienst en de

‡LW-BEHVMBJEH-GJDIBQW‡

procedures voor de mededeling van informatie door deze dienst aan de betrokken operatoren en de termijn waarbinnen de operatoren jaarlijks de bewaring voor de betrokken zone ten uitvoer leggen.

4.1.4. Dienaangaande wordt jaarlijks een evaluatieverslag opgesteld dat gericht wordt aan de Kamer van Volksvertegenwoordigers en aan het Controleorgaan op de politionele informatie. Met betrekking tot de administratieve transparantie en de informatie van het publiek wordt in het ontworpen artikel 126/1, § 3, laatste lid, daarentegen het volgende bepaald:

> "De wet van 11 april 1994 betreffende de openbaarheid van bestuur en de wet van 5 augustus 2006 betreffende de toegang van het publiek tot milieu-informatie zijn niet van toepassing op de informatie, documenten of gegevens, in welke vorm ook, bedoeld in dit artikel, met uitzondering van de criminaliteitsstatistieken bedoeld in het eerste lid, punt 1°."

4.1.5. Concreet zullen de operatoren gehouden zijn tot het bewaren van de gegevens voor alle communicaties die vanuit of naar een van de voornoemde zones gevoerd worden. Van een eindgebruiker zullen alleen die gegevens bewaard worden die verwerkt of gegenereerd zijn wanneer hij zich in de betrokken zone bevond.

Hoe dan ook wordt in dat verband het volgende bepaald:

> "Indien de door de operator gebruikte technologie niet toelaat de bewaring van gegevens te beperken tot de in paragraaf 3 bedoelde zones, bewaart hij ten minste de gegevens die nodig zijn om de hele betrokken zone te bestrijken en beperkt hij de bewaring van gegevens buiten die zone tot wat strikt noodzakelijk is in het licht van de technische mogelijkheden."

4.2.1. Het aldus ingevoerde systeem doet op een aantal punten vragen rijzen.

4.2.2. In de eerste plaats heeft het Hof van Justitie, zoals in de bespreking van dit artikel gesteld wordt, in zijn arrest *La Quadrature du Net* geoordeeld dat voor de gerichte bewaring van gegevens gesteund kan worden op geografische criteria

> "wanneer de bevoegde nationale autoriteiten op basis van objectieve [en niet-discriminatoire] factoren van mening zijn dat er in een of meer geografische gebieden sprake is van een situatie die wordt gekenmerkt door een hoog risico dat zware misdrijven worden voorbereid of gepleegd (...). Het kan daarbij met name gaan om plekken waar veel zware criminaliteit plaatsvindt, om plaatsen waar er een verhoogd risico is op zware misdrijven, zoals plekken of faciliteiten die regelmatig door een zeer groot aantal personen worden bezocht, of om strategische plekken, zoals vliegvelden, stations of tolzones."[24]

Op te merken valt dat de stellers van het voorontwerp bij de keuze van de in aanmerking genomen zones getracht hebben om zich te beperken tot de tenuitvoerlegging van de criteria die door het Hof van Justitie vermeld zijn.

[24] Randnummer 150 van dat arrest.

‡LW-BEHVMBJEH-GJDIBQW‡

Tevens moet opgemerkt worden dat in de bespreking van dit artikel getracht wordt de redenen op te geven waarom, in het licht van de aldus ten uitvoer gelegde criteria, elk type zone in uiteindelijke opsomming opgenomen kon en moest worden.

Zulks neemt evenwel niet weg dat aldus een aanzienlijk aantal en een aanzienlijke verscheidenheid aan zones opgesomd worden, enerzijds, en dat, anderzijds, als men die zaken samen beschouwt, een vrij groot deel van het grondgebied gedekt wordt.

Voor bepaalde zones lijkt het niet voor de hand te liggen of ze al dan niet bestempeld kunnen worden als "plek waar veel zware criminaliteit plaatsvindt", als "plaats waar er een verhoogd risico is op zware misdrijven, doordat ze regelmatig door een zeer groot aantal personen bezocht worden", of nog als "strategische plek".

Dat is het geval met, bijvoorbeeld, de transitiehuizen bedoeld in de wet van 17 mei 2006 'betreffende de externe rechtspositie van de veroordeelden tot een vrijheidsstraf en de aan het slachtoffer toegekende rechten in het raam van de strafuitvoeringsmodaliteiten', de autosnelwegen in hun geheel, de gemeentehuizen of nog de zetels van de provincieraden.

De afdeling Wetgeving kan bijgevolg alleen maar akte nemen van de redenen die reeds opgegeven zijn en de stellers van het voorontwerp verzoeken de keuze van de betrokken zones nog nader te motiveren. Indien er voor elk type zone geen duidelijke, precieze en specifieke redenen opgegeven worden, zal met betrekking tot de ontworpen tekst onzekerheid blijven bestaan over de vraag of de voorgenomen regeling inzake bewaring tot het "strikt noodzakelijke" beperkt blijft.

De lijst van de betrokken zones moet bijgevolg opnieuw onderzocht worden.

4.2.3. De vraag rijst welke autoriteit verantwoordelijk is voor de afbakening van de omvang van elke zone, aangezien die omvang nauwkeurig bepaald en tot het strikt noodzakelijke ingeperkt moet worden in het licht van het arrest *La Quadrature du Net*.

Zo zal, volgens het systeem waarin de ontworpen tekst voorziet, de autoriteit bevoegd voor de aangelegenheid die verband houdt met de bestemming van de zone ermee belast worden jaarlijks aan de door de Koning aangewezen dienst de gegevens mee te delen die nodig zijn voor de concrete bepaling van de geografische zones. Wanneer een geografische zone niet langer aan bedoeld criterium voldoet, zal die autoriteit die dienst daarvan eveneens onverwijld in kennis moeten stellen, zodat de verplichting tot bewaring van de gegevens zo spoedig mogelijk beëindigd kan worden.[25]

Voorts wordt bepaald dat de door de Koning aangewezen dienst elk jaar en telkens wanneer hij van een wijziging in kennis gesteld wordt, de lijst bijwerkt van de geografische gebieden waar de gegevens bewaard moeten worden.

[25] De afdeling Wetgeving gaat ervan uit dat het daarbij bijvoorbeeld gaat om gevallen waarbij in gerechtelijke arrondissementen of politiezones bij aanvang van een nieuw jaar niet meer de minimale criminaliteitscijfers gehaald zouden worden die vereist zijn om als bewaringszone beschouwd te worden, of gevallen waarin een gebouw bestemd voor een welbepaald gebruik op grond waarvan het beschouwd wordt als een bewaringszone, bestemd wordt voor een ander gebruik waardoor de reden om het aldus te beschouwen zou komen te vervallen.

‡LW-BEHVMBJEH-GJDIBQW‡

In het ontworpen dispositief wordt evenwel niets voorgeschreven inzake de concrete en technische criteria die in aanmerking genomen moeten worden om de omvang van de zone te bepalen opdat de zones die tot eenzelfde categorie behoren volgens dezelfde methodologie bepaald zouden worden.[26] Het is de afdeling Wetgeving evenmin duidelijk welke overheid bevoegd is voor het bepalen van de omvang op zich of voor de wijziging ervan. In dat verband wordt alleen bepaald dat de door de Koning aangewezen dienst de lijst van de zones elk jaar en "telkens wanneer hij van een wijziging in kennis wordt gesteld" bijwerkt, wat veronderstelt dat inzake de wijziging van de lijst de beslissingsbevoegdheid toekomt aan de instanties die bevoegd zijn voor de aangelegenheid waarvoor die zone bestemd is, terwijl de Koning de lijst van die instanties kan vaststellen, maar Hij daartoe niet verplicht is.

Doordat het bepalen van de omvang van de zones en het opnemen van zones op de lijst of het schrappen van zones van de lijst van doorslaggevend belang zijn voor de verplichting die aan de operatoren opgelegd wordt om de daarmee verband houdende gegevens te bewaren, moeten al die beslissingen dan ook genomen, of op zijn minst goedgekeurd worden door één enkele overheid, om ervoor te zorgen dat het gelijkheidsbeginsel in acht genomen wordt, in het bijzonder wat betreft de personen wier gegevens bewaard zouden kunnen worden. Het gaat daarbij bovendien om handelingen met een algemene strekking en abstracte gevolgen; het gaat dus om verordenende handelingen die alleen gesteld mogen worden door een overheid die politieke verantwoording verschuldigd is aan het Parlement, namelijk de Koning, aangezien het *in casu* om de federale overheid gaat.[27-28]

4.2.4. Bij het ontworpen artikel 126/1, § 5, wordt de Koning ertoe gemachtigd met betrekking tot de drie categorieën van zones waarvan in het ontworpen artikel 126/1, § 3, eerste lid, 3°, 4° en 5°, sprake is de "bijkomende geografische zones" te bepalen.

Er wordt evenwel niet nader bepaald aan welke criteria de Koning daarbij uitvoering dient te geven.

De ontworpen paragraaf 6 luidt weliswaar als volgt :

> "De minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie en de minister brengen, na voorafgaand advies van het Coördinatiecomité voor Inlichtingen en Veiligheid, en van het Instituut en de bevoegde gegevensbeschermingsautoriteiten, jaarlijks een evaluatieverslag uit aan de Kamer van volksvertegenwoordigers over de toepassing van dit artikel en, in voorkomend geval, van het in paragraaf 5 bedoelde Koninklijk Besluit, teneinde na te gaan of het nodig is bepalingen aan te passen.

[26] Zo zou bijvoorbeeld niet aanvaard kunnen worden dat in de ene zone waarin een gemeentehuis, een ambassade of een ziekenhuis gelegen is ook de onmiddellijke omgeving tot die zone gerekend worden, terwijl in een andere zone waarin een gemeentehuis, een ambassade of een ziekenhuis gelegen is alleen het betrokken gebouw daartoe gerekend zou worden.

[27] In voorkomend geval en mits de berekeningsmethode vooraf door de wetgever of door de koning vastgesteld is, zouden één of meer ministers ermee belast kunnen worden die zones vast te stellen.

[28] Zie in dezelfde zin, advies 69.160/4, gegeven op 6 mei 2021.

‡LW-BEHVMBJEH-GJDIBQW‡

In dit evaluatieverslag wordt in het bijzonder nagegaan of de categorieën van geografische zones opgenomen in de wet en het in paragraaf 5, bedoelde koninklijk besluit nog steeds voldoen aan de criteria bedoeld in paragraaf 3, eerste lid, punten 3° tot 5° of het nog nodig is deze te handhaven dan wel of andere categorieën opgenomen moeten worden.

Categorieën van geografische zones kunnen enkel opgenomen worden ter vrijwaring van de nationale veiligheid, of indien er in deze zones op basis van objectieve en niet-discriminerende elementen kan worden vastgesteld dat er een situatie bestaat die wordt gekenmerkt door een hoog risico op het voorbereiden of plegen van daden van zware criminaliteit.

(...)."

De strekking van de beginselen die vastgelegd worden in het derde lid van die bepaling is evenwel niet helemaal duidelijk.

Zo vraagt de afdeling Wetgeving zich af of die beginselen voor de Koning bindend zullen zijn, wanneer uitvoering gegeven wordt aan de machtiging die aan Hem verleend wordt met het oog op de toevoeging van bepaalde types zones aan de drie voornoemde categorieën, dan wel of het gaat om een aan de toekomstige wetgever gericht verzoek, dat per definitie voor Hem niet bindend zou kunnen zijn.

Hoe dan ook impliceert het legaliteitsbeginsel dat verbonden is aan artikel 22 van de Grondwet, dat de machtiging die aan de Koning verleend wordt nauwkeurig genoeg afgebakend moet worden en dat de ontworpen tekst bijgevolg aldus gesteld moet worden dat de beginselen die in het ontworpen artikel 126/1, § 6, derde lid, vervat zijn op ondubbelzinnige wijze voor Hem gelden.

In dat verband volgt uit de uitleg van de gemachtigden van de minister dat, wanneer de Koning aan de betrokken machtiging uitvoering zal geven, Hij de criteria in acht zal moeten nemen die vermeld worden *in limine* van de bepalingen die in de drie betrokken categorieën zones voorzien. Zo zal, bij wijze van voorbeeld, wanneer overwogen wordt om een zone toe te voegen aan de categorie waarvan in de ontworpen paragraaf 3, eerste lid, 5°, sprake is, de Koning die toevoeging moeten kunnen verantwoorden in het licht van het bestaan van "een mogelijk ernstige bedreiging (...) voor de belangen van de op het nationale grondgebied gevestigde internationale instellingen". Deze regeling is aldus bedoeld om de aan de Koning verleende machtiging af te bakenen.

4.2.5. Het laatste lid van paragraaf 3 van de ontworpen artikel luidt als volgt:

"De wet van 11 april 1994 betreffende de openbaarheid van bestuur en de wet van 5 augustus 2006 betreffende de toegang van het publiek tot milieu-informatie zijn niet van toepassing op de informatie, documenten of gegevens, in welke vorm ook, bedoeld in dit artikel, met uitzondering van de criminaliteitsstatistieken bedoeld in het eerste lid, punt 1°."

4.2.5.1. Bij de ontworpen bepaling wordt de wet van 11 april 1994 'betreffende de openbaarheid van bestuur' aldus op uiterst algemene wijze niet-toepasselijk verklaard op "de informatie, documenten of gegevens, in welke vorm ook, bedoeld in [het ontworpen artikel 126/1]".

‡LW-BEHVMBJEH-GJDIBQW‡

In dat verband[29] dient rekening gehouden te worden met artikel 32 van de Grondwet, dat als volgt luidt:

> "Ieder heeft het recht elk bestuursdocument te raadplegen en er een afschrift van te krijgen, behoudens in de gevallen en onder de voorwaarden bepaald door de wet, het decreet of de regel bedoeld in artikel 134."

Hoewel de betrokken wetgever er bij artikel 32 van de Grondwet toe gemachtigd wordt te bepalen in welke gevallen het recht om elk bestuursdocument te raadplegen en daarvan een afschrift te krijgen niet geldt, moet met de uitzonderingen die aldus gemaakt worden, met inachtneming van het gelijkheidsbeginsel en het beginsel van niet-discriminatie een legitiem doel nagestreefd worden en moeten ze proportioneel blijven ten opzichte van het legitiem doel dat aldus nagestreefd wordt.

De wet van 11 april 1994 die de algemene regeling inzake de toegang tot bestuursdocumenten bevat, voorziet reeds in uitzonderingen op de toegang tot bepaalde documenten. Zo wordt in artikel 6, § 1, van die wet bepaald dat de administratieve overheid de vraag om inzage in, uitleg over of mededeling van een afschrift van een bestuursdocument afwijst, wanneer zij vastgesteld heeft dat het belang van de openbaarheid niet opweegt tegen de bescherming van onder andere de veiligheid van de bevolking of de openbare orde, of nog de veiligheid of de verdediging van het land. Bij die bepaling wordt een systeem ingesteld in het kader waarvan de toegang tot een bestuursdocument of de afgifte van een afschrift van dat document geval per geval geweigerd kan worden, maar wordt geen algemene regeling ingevoerd volgens welke het *a priori* verboden zou zijn toegang te verlenen tot een specifieke categorie documenten of volgens welke de toegang tot een welbepaald document *a priori* tot deze of gene categorie personen beperkt zou kunnen worden.

Met een dergelijk systeem van *a posteriori* te nemen individuele beslissingen kan ervoor gezorgd worden dat de openbare veiligheid, de openbare orde en de veiligheid en de verdediging van het land beschermd worden.

Een degelijke regeling, in het kader waarvan handelingen met individuele strekking gesteld kunnen worden waartegen in laatste instantie bij de afdeling Bestuursrechtspraak van de Raad van State beroep ingesteld kan worden, is aldus van dien aard dat daarmee de proportionaliteit gegarandeerd kan worden van de beperkingen die aan het recht op toegang tot bestuursdocumenten opgelegd worden.

De ontworpen tekst beperkt, daarentegen, op radicale wijze het recht op bestuurlijke transparantie met betrekking tot werkelijk alle "de informatie, documenten of gegevens, in welke vorm ook, bedoeld in [het ontworpen artikel 126/1]".

[29] Voor soortgelijke opmerkingen zie, *mutatis mutandis*, advies 69.160/4.

‡LW-BEHVMBJEH-GJDIBQW‡

De stellers van het voorontwerp moeten kunnen aantonen dat de verschillende behandeling die bij voorliggend dispositief ingevoerd wordt tussen degenen voor wie het *a priori* volstrekt niet mogelijk is om van de lijst met de gevoelige zones kennis te nemen en degenen die kennis wensen te nemen van andere gevoelige bestuursdocumenten op het stuk van de openbare veiligheid, de openbare orde en de veiligheid en de verdediging van het land, die vallen onder de regeling die ingevoerd is bij de wet van 11 april 1994, en in het bijzonder bij de artikel 6 van die wet, op een redelijke en objectieve verantwoording berust zodat die verschillende behandeling conform het gelijkheidsbeginsel en het niet-discriminatiebeginsel is.[30]

Hoe dan ook dient de ontworpen regeling in overeenstemming te blijven met het evenredigheidsbeginsel. Het feit dat de wet van 11 april 1994 niet van toepassing is op "de informatie, documenten of gegevens, in welke vorm ook, bedoeld in [het ontworpen artikel 126/1], met uitzondering van de criminaliteitsstatistieken bedoeld in het eerste lid, punt 1°" van dat artikel, lijkt overdreven wegens de zeer algemene bewoordingen waarin die bepaling gesteld is. Het verdient derhalve aanbeveling om de voorgenomen uitsluiting te beperken tot de categorieën van informatie, documenten of gegevens waarvoor die afwijkende regeling daadwerkelijk verantwoord is.

4.2.5.2. Voor zover de ontworpen bepaling voorziet in een afwijking van de wet van 5 augustus 2006 'betreffende de toegang van het publiek tot milieu-informatie' dienen in dat verband in principe, *mutatis mutandis*, dezelfde opmerkingen geformuleerd te worden als die welke in het vorige punt gemaakt zijn.

Er mag evenwel niet uit het oog verloren worden dat die wet strekt tot omzetting van richtlijn 2003/4/EG van het Europees Parlement en de Raad van 28 januari 2003 'inzake de toegang van het publiek tot milieu-informatie en tot intrekking van Richtlijn 90/313/EEG van de Raad'.

In het licht van het systeem dat ingevoerd is bij de artikelen 3 en 4 van die richtlijn, dat weliswaar alleen geldt voor "milieu-informatie", zoals gedefinieerd in artikel 2, 1°, van die richtlijn, kunnen afwijkingen van de mededelingsplicht alleen aanvaard worden als ze geval per geval toegestaan worden. Die afwijkingen kunnen inzonderheid ingegeven zijn door de noodzaak om de openbare veiligheid of nationale defensie[31] te garanderen, maar in een algemene regeling van voorafgaande uitsluiting mag niet voorzien worden.

4.2.5.3. De voorliggende bepaling moet in het licht van de voorgaande opmerkingen worden herzien.

[30] Zie GwH 19 december 2013, nr. 169/2013.

[31] Artikel 4, lid 2, van de richtlijn.

‡LW-BEHVMBJEH-GJDIBQW‡

4.3.1. Zoals hierboven is aangegeven, stelt de ontworpen bepaling het volgende:

> "Elke autoriteit die bevoegd is voor een van de in de punten 1 tot en met 5 bedoelde aangelegenheden deelt jaarlijks op de door de Koning vastgestelde datum aan de door de Koning aangewezen dienst de gegevens mee die nodig zijn voor de operationele tenuitvoerlegging van dit lid."

Die autoriteiten zijn voorts gehouden die dienst onverwijld in te lichten "wanneer een geografische zone niet langer aan het bedoelde criterium voldoet, (…) zodat de verplichting tot bewaring bedoeld in paragraaf 1 in deze zone zo spoedig mogelijk kan worden beëindigd".

Ten slotte kan de Koning – maar hij is daartoe dus niet verplicht – een lijst opstellen van de verschillende autoriteiten in kwestie.

In zoverre in zones gegevens worden bewaard die inhoudelijk aangelegenheden zouden betreffen waarvoor de gemeenschappen en de gewesten bevoegd zijn,[32] is deze bepaling problematisch: ze legt eenzijdig verplichtingen op aan die bevoegdheidsniveaus, voor wie die verplichtingen dus gelden, niet alleen in het kader van een aangelegenheid die onder federale bevoegdheid valt, maar precies op grond van hun eigen bevoegdheden inzake hun aangelegenheden.[33-34]

Een samenwerkingsregeling die inhoudt dat de gemeenschappen en de gewesten, of organen die daaronder ressorteren, op grond van hun eigen bevoegdheden optreden, moet het voorwerp uitmaken van een samenwerking in de zin van artikel 92*bis* van de bijzondere wet van 8 augustus 1980 'tot hervorming der instellingen'. Een andere werkwijze zou erin kunnen bestaan dat een beslissings- of raadgevend orgaan wordt opgericht waarin de gemeenschappen en de gewesten vertegenwoordigd zouden zijn, overeenkomstig artikel 92*ter* van dezelfde bijzondere wet.

[32] Dat geldt bijvoorbeeld, zij het gedeeltelijk, voor de havens, luchthavens, metro- en pre-metrostations, gemeenten, provincieraden en ziekenhuizen.

[33] Zo kan de regeling waarin de ontworpen bepaling voorziet, niet worden vergeleken met bijvoorbeeld de situatie waarin de administratie van een gemeenschap of een gewest zich bevindt, die als werkgever de federale wetgeving inzake welzijn op het werk dient na te leven.

[34] *Mutatis mutandis* heeft de afdeling Wetgeving het volgende opgemerkt in advies 37.295/4, op 28 juni 2004 gegeven over een voorontwerp dat heeft geleid tot de wet van 13 juni 2005 'betreffende de elektronische communicatie', http://www.raadvst-consetat.be/dbx/adviezen/37295.pdf:
"De autonomie van respectievelijk de gemeenschappen en de gewesten staat er immers aan in de weg dat de federale Staat of een deelentiteit eenzijdig zouden beslissen de instanties van andere deelentiteiten of van de federale Staat te betrekken bij de uitoefening van zijn of haar bevoegdheden. Alleen een wet aangenomen met een bijzondere meerderheid of een samenwerkingsakkoord zou zulk een overleg kunnen opleggen."

‡LW-BEHVMBJEH-GJDIBQW‡

Weliswaar hebben het Grondwettelijk Hof en de afdeling Wetgeving inzake elektronische communicatie reeds andere vormen van samenwerking toelaatbaar geacht, zoals een overeenkomst van het overlegcomité betreffende de wetgeving in kwestie. Maar gelet op de residuaire bevoegdheden van de federale overheid inzake elektronische communicatie en gelet op de toegewezen bevoegdheden van de gemeenschappen inzake inhoudelijke en technische aspecten van de audiovisuele en auditieve mediadiensten, geldt dit enkel in zoverre de betrokken infrastructuren "in samenwerking tussen de federale Staat en de gemeenschappen moe[s]ten worden geregeld, teneinde te bewerkstelligen dat die overheden hun respectieve normen op elkaar afstemmen en om te vermijden dat die infrastructuur en die diensten aan tegenstrijdige bepalingen worden onderworpen".[35-36]

Dat is niet het geval met het voorliggende voorontwerp: het gaat niet om het voorkomen van tegenstrijdigheden tussen twee wetgevingen die elk tot een ander bevoegdheidsniveau behoren, maar, in voorkomend geval, om het feit dat de federale overheid, op basis van haar eigen bevoegdheden, verplichtingen voorschrijft aan andere bevoegdheidsniveaus op grond van hun eigen bevoegdheden.

Bijgevolg kan niet worden gegarandeerd dat de instemming van het overlegcomité met de ontworpen tekst *in casu* toereikend is als samenwerkingsregeling.

Hoe dan ook volgt uit het dossier dat aan de afdeling Wetgeving is bezorgd, dat het georganiseerde overleg in verband met het voorliggende voorontwerp heeft plaatsgehad op basis van het samenwerkingsakkoord van 17 november 2006 tussen de Federale Staat, de Vlaamse Gemeenschap, de Franstalige Gemeenschap en de Duitstalige Gemeenschap 'betreffende het wederzijds consulteren bij het opstellen van regelgeving inzake elektronische communicatienetwerken, het uitwisselen van informatie en de uitoefening van de bevoegdheden met betrekking tot elektronische communicatienetwerken door de regulerende instanties bevoegd voor telecommunicatie of radio-omroep en televisie'. De gewesten waren bijgevolg geen partij bij dat samenwerkingsakkoord.

5. Wat betreft de duur van de bewaring bepaalt het ontworpen artikel 126/1, § 1, dat de in paragraaf 2 bedoelde gegevens gedurende twaalf maanden moeten worden bewaard, te rekenen vanaf de datum van de communicatie, tenzij een andere termijn bepaald is in hetzelfde artikel.

[35] GwH 8 november 2006, nr. 163/2006, B.4; zie ook GwH 14 juli 2004, nr. 132/2004,B.6.1., dat als volgt luidt:
"Op grond van artikel 92*bis* van de bijzondere wet van 8 augustus 1980 tot hervorming der instellingen kunnen de Staat, de gemeenschappen en de gewesten samenwerkingsakkoorden sluiten die onder meer betrekking hebben op de gezamenlijke oprichting en het gezamenlijk beheer van gemeenschappelijke diensten en instellingen, op de gezamenlijke uitoefening van eigen bevoegdheden of op de gemeenschappelijke ontwikkeling van initiatieven. Daarnaast beschikken ze over andere instrumenten om hun samenwerking gestalte te geven."

[36] Zie in het bijzonder advies 42.495/4, op 19 maart 2007 gegeven over een voorontwerp dat heeft geleid tot het decreet van de Franse Gemeenschap van 2 juli 2007 'tot vervanging van de artikelen 81 tot 83 en 90 tot 98 van het decreet van 27 februari 2003 betreffende de radio-omroep, vernietigd door het Arbitragehof op 8 november 2006', http://www.raadvst-consetat.be/dbx/adviezen/42495.pdf.

‡LW-BEHVMBJEH-GJDIBQW‡

De andere bewaringstermijnen waarin het ontworpen artikel 126/1 voorziet, zijn allemaal korter dan twaalf maanden, met uitzondering van de termijnen bepaald in paragraaf 3, 1°, tweede lid, c), en derde lid, c). Het gaat om termijnen van zes en negen maanden, bepaald in paragraaf 3, 1°, tweede lid, a) en b), en derde lid, a) en b), afhankelijk van het aantal strafbare feiten in de betreffende zone.

A priori lijken die bewaringstermijnen geen bijzondere moeilijkheden op te leveren, nog des te minder daar de termijnen bepaald in de voornoemde paragraaf 3, 1°, tweede en derde lid, de evenredigheid van de bewaring willen garanderen ten aanzien van de omvang van de criminaliteit in het gerechtelijk arrondissement of de politiezone in kwestie.

6.1. De laatste voorwaarde die volgens de lering van het arrest *La Quadrature du Net* voor de hier beoogde bewaringsverrichting wordt opgelegd, is dat die verrichting in de tijd wordt beperkt tot wat strikt noodzakelijk is.

Punt 151 van het arrest verwoordt dat vereiste duidelijker aldus:

> "Om ervoor te zorgen dat de inmenging die in de punten 147 tot en met 150 van het onderhavige arrest beschreven maatregelen inzake gerichte gegevensbewaring met zich brengen, in overeenstemming is met het evenredigheidsbeginsel, mogen die maatregelen niet langer gelden dan strikt noodzakelijk is in het licht van het ermee beoogde doel en van de omstandigheden waardoor zij worden gerechtvaardigd, met dien verstande dat zij eventueel kunnen worden verlengd mocht de noodzaak van een dergelijke bewaring blijven bestaan."

Hier lijkt niet zozeer de termijn van de gegevensbewaring te worden bedoeld, als wel de duur van de periode waarin de gegevens met het oog op hun bewaring moeten worden opgeslagen.[37]

6.2. In de regeling die bij het ontworpen artikel 126/1 wordt ingevoerd, wordt niet voorzien in een beperking van de bewaringsverrichtingen in de verschillende bedoelde zones, mits een eventuele verlenging van de maatregelen.

De reden daarvoor is dat de meeste zones in kwestie gebaseerd zijn op de aanwezigheid van gebouwen of installaties bestemd voor bepaalde functies, die volgens de stellers van het voorontwerp, vanwege de aard zelf van die functies, een specifiek risico inhouden ten aanzien van de nagestreefde doelstellingen. Met andere woorden: de stellers van het voorontwerp beogen te bepalen dat de noodzaak om de gegevens te bewaren gerechtvaardigd is zolang de gebouwen en installaties bestemd zijn voor die functies. Dezelfde redenering geldt voor de zones die zijn gedefinieerd op basis van het dreigingsniveau: daar beschouwen de stellers van het voorontwerp de bewaring als noodzakelijk zolang de dreiging ten minste op niveau 3 ligt. Hetzelfde geldt voor de zones die zijn gedefinieerd op basis van het aantal strafbare feiten, zolang dat aantal bereikt is.

[37] Vergelijk met het ontworpen artikel 39*quinquies* van het Wetboek van Strafvordering (artikel 17 van het voorontwerp).

‡LW-BEHVMBJEH-GJDIBQW‡

Om de bewaringsverrichtingen tot het strikt noodzakelijke te beperken, is elke overheid die voor de betreffende aangelegenheid bevoegd is, voorts verplicht de door de Koning aangewezen dienst er onverwijld van in kennis te stellen dat de zone in kwestie niet meer beantwoordt aan het criterium dat haar tot een zone maakt waar gegevens worden bewaard. Die dienst is bovendien belast met het bijwerken van de lijst van de zones, wat ze jaarlijks, alsook telkens wanneer een bevoegde overheid haar in kennis stelt van een wijziging, moet doen. Ten slotte moet een jaarverslag aan de Kamer van volksvertegenwoordigers worden voorgelegd, waarin met name wordt onderzocht of de categorieën van geografische zones die worden opgesomd in de wet of in het besluit waarvan in paragraaf 5 van de ontworpen bepaling sprake is, nog altijd beantwoorden aan de criteria in verband met de nagestreefde doelstellingen, en of die categorieën moeten worden gehandhaafd dan wel of er andere zones in moeten worden opgenomen.

Met die regelingen wil men garanderen dat geen enkele perimeter die aanvankelijk onder het bepaalde van het ontworpen artikel 126/1 viel, als dusdanig wordt gehandhaafd indien dat niet strikt noodzakelijk is voor de betreffende doelstellingen.

De afdeling Wetgeving begrijpt weliswaar de logica van de ingevoerde regeling, maar toch kan niet worden gegarandeerd dat die regeling volledig in overeenstemming is met de voorwaarde die in punt 151 van het arrest *La Quadrature du Net* wordt gesteld.

Zo wekt dat punt 151 de indruk dat de regeling berust op een beperking in de tijd *a priori*, met eventueel een verlenging, terwijl de ontworpen regeling van haar kant op een duurzame verrichting zonder tijdsbeperking steunt, waaraan in principe een einde wordt gemaakt zodra die regeling niet meer door enige noodzaak wordt gerechtvaardigd.

7.1. Ten slotte dienen over de voorliggende bepaling de volgende specifieke opmerkingen te worden gemaakt.

7.2. Sommige vermelde zones zijn moeilijk verenigbaar met het begrip "zone", dat de vaststelling van een geografische perimeter inhoudt. Dat geldt bijvoorbeeld voor het netwerk waarvan ASTRID gebruikmaakt en voor de informatienetwerken en -systemen die de verlening van essentiële diensten van operatoren van essentiële diensten ondersteunen, bedoeld in het ontworpen artikel 126/1, § 3, 3°, o) en p).

De ontworpen tekst zou beter worden aangevuld zodat die netwerken geografisch duidelijker worden afgebakend.

Evenzo valt moeilijk te bepalen welke de zones zijn "waar het algemene dreigingsniveau, vastgesteld [krachtens] de wet van 10 juli 2006 betreffende de dreigingsanalyse, ten minste niveau 3 bedraagt, (…) en zolang niveau 3 blijft bestaan". Volgens artikel 11, § 6, van het koninklijk besluit van 28 november 2006 wordt het dreigingsniveau immers vastgesteld ten aanzien van een persoon, groepering of gebeurtenis: in zoverre de vaststelling van het dreigingsniveau betrekking heeft op een persoon of een beperkte groepering, kan ze niet altijd geografisch worden gelokaliseerd. De afdeling Wetgeving veronderstelt dan ook dat de ontworpen regeling alleen gaat over de gevallen waarin de dreiging lokaliseerbaar is in een geografisch gebied; dat zou expliciet moeten worden bepaald in de ontworpen tekst.

‡LW-BEHVMBJEH-GJDIBQW‡

7.3. De gebouwen bestemd voor de instellingen bedoeld in de hoofdstukken 5 tot 7 van titel III van de Grondwet, de gemeenten waarin zich militaire domeinen bevinden en de gebouwen bestemd voor de federale of de lokale politie, worden opgenomen in de lijst van zones waarbinnen gegevens worden bewaard, enerzijds in de ontworpen paragraaf 3, 3°, respectievelijk e), h) en f), als zones "die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit", en anderzijds in het ontworpen punt 4°, d), respectievelijk vi), vii) en viii, "voor de nationale soevereiniteit en de instellingen opgericht door de Grondwet en de wetten, decreten of ordonnanties".

De afdeling Wetgeving begrijpt de logica noch het nut van het feit dat die types van zones in die twee verschillende categorieën worden ondergebracht; dat leidt trouwens tot onduidelijkheid. De vraag rijst of die overlapping niet aan een vergissing te wijten is.

7.4. Het valt niet uit te sluiten dat zich een situatie voordoet waarin verschillende overheden in de zin van de paragrafen 3 en 5 van de ontworpen bepaling, op grond van de aangelegenheden waarvoor ze bevoegd zijn, voor eenzelfde soort zone bevoegd zouden zijn. Die situatie komt in het ontwerp niet ter sprake en wordt er niet in geregeld.

7.5. In de categorie van zones waar een mogelijke ernstige bedreiging bestaat voor de vitale belangen van de natie of voor de essentiële behoeften van de bevolking, bevinden zich "de gebouwen bestemd voor rechtspersonen waarvan het economisch en wetenschappelijk potentieel beschermd moet worden die zijn opgenomen in een lijst die jaarlijks door de staatsveiligheid en de algemene inlichtingen- en veiligheidsdienst wordt opgesteld op voorstel van de minister van Justitie en Defensie en wordt goedgekeurd door de Nationale Veiligheidsraad".

Volgens de commentaar op dat artikel verwijst dat soort zone in werkelijkheid enerzijds naar de opdrachten van de Veiligheid van de Staat, die volgens artikel 7, 1°, van de wet van 30 november 1998 onder meer de volgende opdracht heeft:

> "het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op elke activiteit die (…) het wetenschappelijk of economisch potentieel, zoals gedefinieerd door de Nationale Veiligheidsraad, of elk ander fundamenteel belang van het land, zoals gedefinieerd door de Koning op voorstel van de Nationale Veiligheidsraad, bedreigt of zou kunnen bedreigen."

Anderzijds wordt verwezen naar artikel 11, § 1, 1°, c), van dezelfde wet, dat de Algemene Dienst Inlichting en Veiligheid met name opdraagt inlichtingen in te winnen, te analyseren en te verwerken die betrekking hebben op elke activiteit die een bedreiging vormt of zou kunnen vormen voor

> "het wetenschappelijk en economisch potentieel met betrekking tot de actoren, zowel de natuurlijke als de rechtspersonen, die actief zijn in de economische en industriële sectoren die verbonden zijn met defensie en die opgenomen zijn in een op voorstel van de minister van Justitie en de minister van Landsverdediging door de Nationale Veiligheidsraad goedgekeurde lijst."

‡LW-BEHVMBJEH-GJDIBQW‡

In het licht van die precisering stelt de afdeling Wetgeving vast dat de voorliggende bepaling melding maakt van een lijst "die jaarlijks door de staatsveiligheid en de algemene inlichtingen- en veiligheidsdienst wordt opgesteld op voorstel van de minister van Justitie en Defensie en wordt goedgekeurd door de Nationale Veiligheidsraad". In verband met de aantasting van het economische en wetenschappelijke potentieel bepaalt artikel 7, 1°, van de wet van 30 november 1998, dat over de Veiligheid van de Staat gaat, niet dat die dienst een dergelijke lijst moet opstellen, terwijl artikel 11, § 1, 1°, c), van dezelfde wet bepaalt dat de Algemene Dienst Inlichting en Veiligheid van zijn kant een lijst opstelt, in soortgelijke omstandigheden als die waarin de voorliggende bepaling voorziet, maar die alleen betrekking hebben op de economische en industriële sectoren die met Defensie verband houden.

De stellers van het voorontwerp dienen alle voornoemde bepalingen te herzien om te voorkomen dat verschillende lijsten worden gemaakt, die in voorkomend geval elkaar zouden kunnen overlappen of tegenspreken, en om die bepalingen samenhangend te maken in zoverre ze betrekking hebben op de bescherming van het economische en wetenschappelijke potentieel op het nationale grondgebied en over de uitwerking van de daarmee verband houdende lijst(en).

7.6. In het ontworpen artikel 126/1, § 3, wordt meermalen melding gemaakt van "inbreuken (…) zoals bedoeld in artikel 90*ter* van het Wetboek van Strafvordering". Omwille van de transparantie en de rechtszekerheid zou nauwkeuriger moeten worden verwezen naar de onderverdelingen van het betreffende artikel waarin van de "inbreuken" in kwestie sprake is.

8. Als besluit kan worden gesteld dat het ontworpen artikel 126/1 in het licht van de voorgaande opmerkingen opnieuw moet worden onderzocht en moet worden herzien.

Algemene en ongedifferentieerde bewaring van IP-adressen die zijn toegewezen aan de bron, ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid

1. Artikel 7 van het voorontwerp beoogt heel artikel 126 van de wet van 13 juni 2005 te vervangen, zodat dat als volgt zou luiden:

> "§ 1. Onverminderd de AVG en de wet van 30 juli 2018, bewaren de operatoren die aan de eindgebruikers elektronische-communicatiediensten aanbieden, alsook de operatoren die de onderliggende elektronische-communicatienetwerken leveren, de abonnementsgegevens van de abonnee alsook de technische gegevens die noodzakelijk zijn om de eindgebruiker, de eindapparatuur of de gebruikte elektronische-communicatiedienst te identificeren, met uitzondering van de gegevens die verband houden met één enkele elektronische communicatie, op voorwaarde dat ze deze gegevens in het kader van de verstrekking van de communicatienetwerken of -diensten in kwestie verwerken of genereren.
>
> Dit artikel heeft geen betrekking op de inhoud van de communicatie.
>
> Deze gegevens worden bewaard voor de autoriteiten en doeleinden bedoeld in artikel 127/1.
>
> De in dit artikel beoogde gegevens worden bewaard vanaf de datum waarop de dienst wordt geactiveerd tot twaalf maanden na de datum vanaf wanneer een communicatie aan de hand van de gebruikte dienst voor het laatst mogelijk is.

‡LW-BEHVMBJEH-GJDIBQW‡

In afwijking van het derde lid worden de andere dynamische IP-adressen dan diegene die is gebruikt om in te tekenen op de dienst, tot twaalf maanden na het einde van de sessie bewaard.

§ 2. De Koning bepaalt, na advies van de bevoegde Gegevensbeschermingsautoriteiten en van het Instituut, de te bewaren gegevens alsook de vereisten waaraan deze gegevens moeten beantwoorden."

Die bepaling wort in de commentaar op het artikel als volgt verantwoord:

"Voor de tenuitvoerlegging van het arrest van het Grondwettelijk Hof van 22 april 2021 en het arrest-Quadrature du Net van het Europees Hof van Justitie worden voor de bewaringsplicht enkel nog de abonnementsgegevens en technische gegevens die noodzakelijk zijn voor de identificatie van de eindgebruiker, de eindapparatuur of de gebruikte elektronische-communicatiedienst beoogd, met uitzondering van de gegevens die verband houden met één enkele elektronische communicatie (zoals de identificatiecode die wordt gecreëerd voor elke communicatie). Dit artikel is van toepassing wanneer elektronische-communicatiedienst in België wordt verstrekt.

De bewaringstermijn van 12 maanden werd behouden, aangezien deze termijn overeenstemt met de strikt noodzakelijke bewaringstermijn om de autoriteiten in staat te stellen om hun onderzoeken tot een goed einde te brengen, in het bijzonder op het stuk van de strijd tegen de zware criminaliteit.

Er wordt een onderscheid gemaakt tussen het IP-adres dat gebruikt is om op de dienst in te tekenen en de overige IP-adressen. Het IP-adres dat gebruikt is om in te tekenen op de dienst is immers een gegeven dat door de operatoren moet worden bewaard in het kader van artikel 127, om de identiteit van de abonnee te kunnen vaststellen of nagaan.

De abonnementsgegevens omvatten onder andere het telefoonnummer, het e-mailadres, het nummer van de abonnee, de start- en einddatum van het abonnement. De Franse Conseil d'Etat, die de Franse wetgeving betreffende bewaring van verkeersgegevens voor de autoriteiten moest onderzoeken (arrest van 21/04/2021 nrs. 393099, 394922, 397844, 397851, 424717, 424718, FRENCH DATA NETWORK et autres), heeft daarover het volgende gesteld: 'uit de richtlijn van 12 juli 2002 en van de AVG blijkt duidelijk dat zij niet gekant zijn tegen een verplichting tot algemene en ongedifferentieerde bewaring, voor de duur van een jaar, van andere inlichtingen dan die in verband met de burgerlijke identiteit die verstrekt zijn bij het sluiten van een contract door een gebruiker of bij het aanmaken van een account enerzijds, en van de gegevens met betrekking tot de betalingen anderzijds, respectievelijk vermeld in de bepalingen onder 3° en 4° van artikel 1 van het decreet van 25 februari 2011' (punt 36) (vrij vertaald).

De technische identificatiecodes die niet gelinkt zijn aan een specifieke communicatie maar die hoofdzakelijk dienen om de eindgebruiker, de eindapparatuur of de gebruikte elektronische-communicatiedienst te identificeren, omvatten onder andere het IP-bronadres, de IMEI (International Mobile Equipment Identity), IMSI (International Mobile Subscriber Identity), ICCID (Integrated Circuit Card Identifier), het MAC-adres, het MSISDN (Mobile Station Integrated Services Digital Network), of andere identificatiecodes die zullen worden ontwikkeld in het kader van 5G of afhankelijk van de evolutie van de gebruikte technologieën. Tot op heden heeft het Hof van Justitie van de Europese Unie zich enkel uitgesproken over het IP-adres aan de bron, maar niet over de voormelde andere technische gegevens, waarvan de bewaring eveneens noodzakelijk is voor identificatiedoeleinden.

‡LW-BEHVMBJEH-GJDIBQW‡

De gegevens die noodzakelijk zijn om de eindgebruiker, de apparatuur of de elektronische-communicatiedienst te identificeren, kunnen verkeersgegevens omvatten. Zo zullen bijvoorbeeld bepaalde verkeersgegevens moeten bewaard worden om het IP-adres aan een specifieke persoon te linken of om het gebruikte telefoonnummer of MSISDN-nummer ('Mobile Subscriber Integrated Services Digital Network', met name het telefoonnummer met het internationale prefix) terug te vinden.

Zoals aangegeven in het arrest La Quadrature du Net van het HvJ-EU van 6/10/2020, is het IP-bronadres het enige middel aan de hand waarvan de dader van een online-inbreuk kan worden geïdentificeerd (punt 154 van het arrest).

In het arrest van het HvJ-EU van 2 oktober 2018, Ministerio Fiscal (C207/16, punt 20), werd beschouwd dat het volgende geen ernstige inmenging vormt in de grondrechten (persoonlijke levenssfeer en bescherming van de persoonsgebonden gegevens): het verzoek van de gerechtelijke politie, ten behoeve van een strafrechtelijk onderzoek, om de telefoonnummers te krijgen die gedurende een periode van twaalf dagen werden geactiveerd aan de hand van de code voor de internationale identiteit van het mobiele toestel (hierna de 'IMEI-code') van de gestolen mobiele telefoon alsook de persoonsgebonden gegevens met betrekking tot de burgerlijke identiteit van de houders of van de gebruikers van de telefoonnummers die overeenstemmen met de via deze code geactiveerde simkaarten.

In het licht van het nut dat deze technische gegevens vertegenwoordigen voor de identificatie van daders van overtredingen online en offline, is de geplande bewaringsmaatregel evenredig."[38]

2. Het ontworpen artikel 126 moet in verband worden gebracht met het arrest *La Quadrature du Net* en met arrest nr. 57/2021 van het Grondwettelijk Hof.

Pro memorie zij gesteld dat het Hof van Justitie in het dictum van zijn arrest *La Quadrature du Net* inderdaad voor recht heeft verklaard dat artikel 15, lid 1, van richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8 en 11 en van artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, geen wetgevende maatregelen verhindert

"(…)

– die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de IP-adressen die zijn toegewezen aan de bron van een verbinding, voor een periode die niet langer is dan strikt noodzakelijk;

– die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van criminaliteit en de bescherming van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronischecommunicatiemiddelen,

(…)."

[38] Memorie van toelichting, 30-32.

‡LW-BEHVMBJEH-GJDIBQW‡

Het Hof van Justitie maakt aldus een onderscheid tussen:

– enerzijds de algemene en ongedifferentieerde bewaring van de IP-adressen die zijn toegewezen aan de bron van een verbinding, die de wetgeving aan de operatoren enkel kan opleggen ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid, en dit voor een periode die niet langer is dan strikt noodzakelijk,

– en anderzijds algemene en ongedifferentieerde bewaring van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronische communicatiemiddelen, die de wetgeving aan de operatoren kan opleggen met het oog op ruimere doelstellingen, namelijk de bescherming van de nationale veiligheid, de bestrijding van criminaliteit, ongeacht of het al dan niet om zware criminaliteit gaat, en de bescherming van de openbare veiligheid, zelfs wanneer die niet ernstig wordt bedreigd, en dit zonder dat de bewaring van die gegevens beperkt is tot "periode die niet langer is dan strikt noodzakelijk".

3. Harerzijds heeft de voorliggende bepaling betrekking op het volgende:

– de abonnementsgegevens van de abonnee, die niet worden gedefinieerd maar waarover in de commentaar op het artikel wordt gezegd dat ze "onder andere het telefoonnummer, het e-mailadres, het nummer van de abonnee, de start- en einddatum van het abonnement [omvatten]", en

– de gegevens die noodzakelijk zijn voor de identificatie van de eindgebruiker, de eindapparatuur of de gebruikte elektronische-communicatiedienst, die al evenmin worden gedefinieerd maar waarover de commentaar op het artikel stelt dat ze "onder andere het IP-bronadres, de IMEI (*International Mobile Equipment Identity),* IMSI *(International Mobile Subscriber Identity*), ICCID (*Integrated Circuit Card Identifier*), het MAC-adres, het MSISDN (*Mobile Station Integrated Services Digital Network*), of andere identificatiecodes die zullen worden ontwikkeld in het kader van 5G of afhankelijk van de evolutie van de gebruikte technologieën [omvatten]".

In verband met de in de ontworpen bepaling vermelde gegevens die niet uitsluitend betrekking zouden hebben op de "burgerlijke identiteit van de gebruikers van elektronische communicatiemiddelen", maar IP-bronadressen zijn, of in verband met de gegevens waarvan de bewaring soortgelijke risico's kan meebrengen als die waartoe de bewaring van en de toegang tot IP-brongegevens aanleiding geven,[39] dient te worden opgemerkt dat de bewaring van

[39] Het Hof van Justitie heeft in zijn arrest *La Quadrature du Net* het volgende opgemerkt over de IP-bronadressen:
"152. Opgemerkt dient te worden dat IP-adressen weliswaar behoren tot de verkeersgegevens, maar los van een bepaalde communicatie worden gegenereerd en primair dienen om via de aanbieders van elektronische communicatiediensten de natuurlijke persoon te identificeren die eigenaar is van een eindapparaat waarvandaan via het internet wordt gecommuniceerd. Voor zover bij e-mailverkeer en internettelefonie uitsluitend de IP-adressen van de bron van de communicatie en niet die van de ontvanger ervan worden bewaard, geven die adressen als zodanig geen enkele informatie prijs over de derden die in contact zijn geweest met de persoon die aan de basis ligt van de communicatie. Deze categorie gegevens is dan ook van mindere gevoelige aard dan de andere verkeersgegevens.
153. Aangezien IP-adressen echter onder meer kunnen worden gebruikt om de volledige zoekgeschiedenis van een internetgebruiker te traceren en dus om een volledig beeld te krijgen van diens online activiteit, kan aan de hand van die gegevens een gedetailleerd profiel van de betrokkene worden opgesteld. De voor een dergelijke tracking noodzakelijke bewaring en analyse van IP-adressen vormen dan ook ernstige inmengingen in de door de artikelen 7

‡LW-BEHVMBJEH-GJDIBQW‡

die gegevens in de ontworpen bepaling geenszins wordt beperkt tot doeleinden van bescherming van de nationale veiligheid, bestrijding van zware criminaliteit en voorkoming van ernstige bedreigingen van de openbare veiligheid.

Het ontworpen artikel 126, § 1, derde lid, bepaalt weliswaar dat "[d]eze gegevens worden bewaard voor de autoriteiten en doeleinden bedoeld in artikel 127/1", maar in het ontworpen artikel 127/1, meer bepaald in § 1, 1° en 2°, worden die doeleinden op algemene wijze geformuleerd en worden ze niet beperkt tot "de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid".

4. Daaruit vloeit voort dat de in het ontworpen artikel 126 ingevoerde regeling in combinatie met het ontworpen artikel 127/1 niet de inachtneming kan garanderen van artikel 15, lid 1, van richtlijn 2002/58/EG, gelezen in het licht van de lering van het arrest *La Quadrature du Net*, wat betreft de algemene en ongedifferentieerde bewaring van IP-bronadressen, en bij analogie van alle vergelijkbare gegevens, waarvan de bewaring soortgelijke risico's inhoudt als die welke verbonden zijn aan de bewaring van de IP-bronadressen, zoals naar voren gebracht door het Hof van Justitie.

Het ontworpen dispositief moet in het licht van deze opmerking worden herzien en aangevuld.

5. Ten slotte stelt de voorliggende bepaling dat de gegevens die ze vermeldt, bewaard worden "vanaf de datum van activering van de dienst tot twaalf maanden na de datum vanaf wanneer communicatie voor het laatst mogelijk is aan de hand van de gebruikte dienst". Voor andere dynamische IP-adressen dan die welke worden gebruikt om in te tekenen op de dienst, wordt bepaald dat ze tot twaalf maanden na het einde van de sessie worden bewaard.

Dergelijke termijnen kunnen relatief lang lijken ten aanzien van de vereisten die voortvloeien uit de lering van het arrest *La Quadrature du Net*.

In de commentaar op het artikel wordt dienaangaande het volgende gepreciseerd:

> "De bewaringstermijn van 12 maanden werd behouden, aangezien deze termijn overeenstemt met de strikt noodzakelijke bewaringstermijn om de autoriteiten in staat te stellen om hun onderzoeken tot een goed einde te brengen, in het bijzonder op het stuk van de strijd tegen de zware criminaliteit."

Dat is een heel algemene verantwoording die meer weg heeft van een beginselverklaring.

De stellers van het voorontwerp moeten de vastgestelde termijnen beter kunnen verantwoorden met concrete en afdoende gegevens.

---

en 8 van het Handvest gewaarborgde grondrechten van de internetgebruiker, die een ontmoedigend effect als bedoeld in punt 118 van het onderhavige arrest kunnen hebben".
De ernst van de aldus beschouwde inmenging heeft het Hof van Justitie ertoe gebracht die categorie van gegevens strenger te behandelen dan de gegevens betreffende de burgerlijke identiteit van de gebruikers.

‡LW-BEHVMBJEH-GJDIBQW‡

De voorliggende bepaling moet in het licht van deze opmerking opnieuw worden onderzocht.

Algemene en ongedifferentieerde bewaring van gegevens betreffende de burgerlijke identiteit van de gebruikers van elektronische communicatiemiddelen, ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de bescherming van de openbare veiligheid

1. Volgens de lering van het arrest *La Quadrature du Net* kan worden aanvaard dat een wetgeving een algemene en ongedifferentieerde bewaring van gegevens betreffende de burgerlijke identiteit van de gebruikers van elektronische communicatiemiddelen mogelijk maakt ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de bescherming van de openbare veiligheid.

Artikel 9 van het voorontwerp, dat strekt tot vervanging van artikel 127 van de wet van 13 juni 2005, wil een dergelijke bewaring regelen.

Ten aanzien van de vereisten van het internationaal en het Europees recht die hierboven zijn vermeld, lijkt deze bepaling in principe geen moeilijkheden op te leveren.

Dat neemt niet weg dat de algemene machtiging die het ontworpen artikel 127, § 2, tweede lid, aan de operatoren verleent om "automatisch een vergelijking uit [te] voeren tussen de biometrische gegevens op de foto van het identiteitsstuk van de abonnee en deze van zijn gezicht" buitensporig kan lijken ten aanzien van het nagestreefde doel, in het bijzonder gelet op het feit dat die gegevens zouden kunnen worden verzameld bij alle abonnees, zijnde om het even welke natuurlijke persoon van alle operatoren, zonder dat de wetgever die mogelijkheid ook maar afbakent en beperkt tot specifieke gevallen waarin de maatregel noodzakelijk is.

Naar aanleiding van een vraag daarover hebben de gemachtigden van de minister evenwel uitgelegd dat de beoogde biometrische vergelijking enkel zou worden verricht in de tijdspanne die nodig is om een persoon te identificeren, en geen enkele opslag noch vervolgens enige bewaring van de gegevens zou inhouden. In die context lijkt de beoogde maatregel niet buitensporig te zijn.

In een andere gedachtegang, en in zeer bijkomende orde, ziet de afdeling Wetgeving niet in hoe het ontworpen artikel 127, § 2, tweede lid, zich zou moeten verhouden tot de machtiging die bij het ontworpen artikel 127, § 3, eerste lid, 1° en 2°, aan de Koning wordt verleend. Die machtiging houdt in dat de Koning kan "bepalen of de operator zelf zijn abonnees moet identificeren of louter deze identificatie mogelijk moet kunnen maken" en dat hij "de methodes voor identificatie [kan] bepalen die de operatoren kunnen gebruiken, inclusief een door een operator voorgestelde identificatiemethode onderwerpen aan een voorafgaande machtiging van de minister [bevoegd voor de elektronische communicatie] en van de minister van Justitie".

Artikel 9 van het voorontwerp moet in het licht van deze opmerkingen worden herzien.

‡LW-BEHVMBJEH-GJDIBQW‡

Gebruikmaken van een bevel aan de aanbieders van elektronischecommunicatiediensten tot spoedbewaring gedurende een bepaalde periode van de in hun handen zijnde verkeers- en locatiegegevens ten behoeve van de bestrijding van zware criminaliteit en, a fortiori, de bescherming van de nationale veiligheid

1. Er wordt aan herinnerd dat uit het arrest *La Quadrature du Net* volgt dat ten behoeve van de bestrijding van zware criminaliteit en, *a fortiori*, de bescherming van de nationale veiligheid een wetgeving toelaatbaar is die het mogelijk maakt om via een aan effectieve rechterlijke toetsing onderworpen beslissing van de bevoegde autoriteit aan aanbieders van elektronische communicatiediensten een bevel op te leggen tot spoedbewaring van de in hun handen zijnde verkeers- en locatiegegevens gedurende een bepaalde periode.

2.1. Artikel 32 van het voorontwerp strekt ertoe een paragraaf 1*bis*/1 in te voegen in artikel 84 van de wet van 2 augustus 2002 'betreffende het toezicht op de financiële sector en de financiële diensten'. Die paragraaf luidt als volgt:

> "Voor inbreuken op de artikelen 14 of 15 van de Verordening 596/2014, of de bepalingen genomen op basis of in uitvoering ervan, kan de auditeur, of, in zijn afwezigheid, de adjunct-auditeur, de in paragraaf 1, tweede lid, bedoelde actoren bevelen om de gegevens bedoeld in paragraaf 1, eerste lid, die riskeren te worden verwijderd of anoniem gemaakt, te bewaren totdat hij de toestemming van een onderzoeksrechter heeft bekomen.
>
> Paragrafen 1, vierde en vijfde lid, en 3 zijn van overeenkomstige toepassing op het in het eerste lid bedoelde bevel.
>
> De in paragraaf 1, tweede lid, bedoelde actoren zorgen ervoor dat de integriteit, de kwaliteit en de beschikbaarheid van de gegevens gewaarborgd is en dat de gegevens op een veilige manier bewaard worden.
>
> De auditeur, of, in zijn afwezigheid, de adjunct-auditeur, bezorgt het in het eerste lid bedoelde bevel aan de onderzoeksrechter gelijktijdig met zijn verzoek tot voorafgaande toestemming om de mededeling te vorderen van de in paragraaf 1, eerste lid, bedoelde gegevens. Wanneer de onderzoeksrechter de toestemming weigert om de mededeling te vorderen van de gegevens waarop het bevel betrekking heeft of oordeelt dat het bevel niet wettig of niet gerechtvaardigd was, vervalt het bevel."

2.2.1. Gelet op de lering van het arrest *La Quadrature du Net*, geeft die bepaling aanleiding tot twee opmerkingen.

2.2.2. Allereerst rijst de vraag of de "*quick freeze*", de snelle gegevensbewaring die op die manier toegestaan wordt, zich wel beperkt tot feiten die verband houden met "de bestrijding van zware criminaliteit en, *a fortiori*, de bescherming van de nationale veiligheid".

De bespreking van het artikel vermeldt in dat verband het volgende:

> "Bovendien wordt deze mogelijkheid tot quick freeze enkel voorzien voor inbreuken op het verbod op marktmisbruik (artikelen 14 of 15 van Verordening (EU) nr. 596/2014 van het Europees Parlement en de Raad van 16 april 2014 betreffende marktmisbruik (Verordening marktmisbruik)), wat een ernstig misdrijf uitmaakt. De impact daarvan op de integriteit van de financiële markten en het vertrouwen van de beleggers is immers groot. Binnen de financiële sector gaat het om één van de

‡LW-BEHVMBJEH-GJDIBQW‡

meest ernstige inbreuken, wat o.m. blijkt uit het feit dat de Verordening marktmisbruik voor deze inbreuken aanzienlijk hogere minimale maximumboetes vereist dan voor de inbreuken op andere bepalingen van de verordening en op de meeste andere Europese financiële wetgeving, alsook uit het feit dat Richtlijn 2014/57/EU van het Europees Parlement en de Raad van 16 april 2014 betreffende strafrechtelijke sancties voor marktmisbruik de lidstaten oplegt om voor marktmisbruik ook strafrechtelijke sancties te voorzien (uitgewerkt in de artikelen 39 en 40 van de wet van 2 augustus 2002). In het kader van de doorgaans complexe en tijdsintensieve onderzoeken inzake marktmisbruik spelen elektronische communicatiegegevens dikwijls een belangrijke rol in de bewijsvoering, bijvoorbeeld om vast te stellen dat personen op een bepaald moment met elkaar in contact zijn geweest en er tussen twee of meer personen een relatie bestaat."

Verordening 596/2014 voorziet in haar artikel 30 met betrekking tot de inbreuken op haar artikelen 14 en 15 weliswaar in sancties die in theorie zwaar lijken en die in elk geval zwaarder zijn dan de straffen bepaald voor andere strafbare feiten.

Zo schrijft artikel 30, lid 2, van die verordening met betrekking tot natuurlijke personen voor dat de lidstaten ervoor moeten zorgen dat de bevoegde autoriteiten een maximale administratieve financiële sanctie kunnen opleggen van ten minste 5 000 000 EUR.

Met betrekking tot rechtspersonen bedraagt dat maximumbedrag ten minste 15 000 000 EUR of 15 % van de totale jaaromzet van de rechtspersoon overeenkomstig de meest recente beschikbare en door het management goedgekeurde jaarrekeningen.

Dat neemt evenwel niet weg dat die sancties volgens de verordening zelf administratieve financiële sancties zijn en geen strafsancties.

Bovendien stelt de verordening geen minimumbedrag vast voor die sancties, maar enkel de onderste drempel van het maximumbedrag van de sanctie.

Wat de artikelen 39 en 40 van de wet van 2 augustus 2002 betreft waarnaar in de bespreking van het artikel verwezen wordt, wordt respectievelijk voorzien in de volgende minimale strafsancties:

– wat artikel 39, § 1, betreft: een gevangenisstraf van één maand en een geldboete van 300 euro;

– wat artikel 40, § 6, betreft: een gevangenisstraf van drie maanden en een geldboete van 50 euro.

In die omstandigheden lijkt het moeilijk aanneembaar dat in theorie alle strafbare feiten waarop die verschillende bepalingen van toepassing zijn per definitie onder de noemer "zware criminaliteit" vallen.[40]

[40] Vergelijk op dat punt met het ontworpen artikel 39*quinquies* van het Wetboek van Strafvordering (artikel 17 van het voorontwerp) dat betrekking heeft op misdrijven "die een correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben".

‡LW-BEHVMBJEH-GJDIBQW‡

Hoewel de afdeling Wetgeving de logica begrijpt van de rechtvaardigingen die in de bespreking van de artikelen aangevoerd worden, dient, teneinde ervoor te zorgen dat het ontworpen dispositief in overeenstemming is met de beginselen voortvloeiend uit het arrest *La Quadrature du Net*, de injunctiebevoegdheid waarvan sprake is beperkt te worden tot de feiten waarvan de ernst aangetoond is of verondersteld kan worden op basis van de gegevens waarover de auditeur of de adjunct-auditeur beschikt.

2.2.3. Bovendien zou de ontworpen regeling beter aldus aangevuld worden dat daarin bepaald wordt dat de aan de onderzoeksrechter gerichte aanvraag tot toegang tot de gegevens met het aan de betrokken operator(en) gegeven bevel tot "*quick freeze*" moet samenvallen of daar op zijn minst onverwijld moet op volgen.

Dat samenvallen of het bijna samenvallen ervan biedt immers een grotere garantie op een effectieve rechterlijke toetsing, zoals wordt voorgeschreven door het Europees recht.

2.2.4. Artikel 32 van het voorontwerp moet in het licht van die opmerkingen herzien worden.

3. Artikel 24 van het voorontwerp strekt ertoe een artikel 16/2/1 in te voegen in de wet van 30 november 1998.

Afgezien van de bijzondere opmerkingen waartoe die bepaling aanleiding geeft, gelet op de dubbelzinnigheden, de onnauwkeurigheden en de andere moeilijkheden waarmee ze behept is en die in de bijzondere opmerkingen hierna aan bod komen, vraagt de afdeling Wetgeving zich af op welke wijze voldaan zal worden aan het vereiste van een effectieve rechterlijke toetsing dat voortvloeit uit de lering van het arrest *La Quadrature du Net*.

Artikel 24 moet in het licht van die opmerking opnieuw onderzocht worden.

BIJZONDERE OPMERKINGEN

INDIENINGSBESLUIT

Het indieningsbesluit moet als volgt gesteld worden:

"Filip I, Koning der Belgen,

Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

Op de voordracht van de Minister van Telecommunicatie, de Minister van Justitie en de Minister van Defensie,

HEBBEN WIJ BESLOTEN EN BESLUITEN WIJ:

‡LW-BEHVMBJEH-GJDIBQW‡

De Minister van Telecommunicatie, de Minister van Justitie en de Minister van Defensie zijn ermee belast in onze naam bij de Kamer van volksvertegenwoordigers het ontwerp van wet in te dienen waarvan de tekst hierna volgt:"[41]

DISPOSITIEF

Artikel 4

1. De ontworpen paragraaf 4, derde lid, van artikel 122 van de wet van 13 juni 2005 bepaalt dat de locatiegegevens en andere verkeersgegevens die nodig zijn om een vermoed geval van fraude of van moedwillig gebruik van een elektronische-communicatienetwerk op te sporen en te analyseren minstens vier maanden door de operatoren bewaard moeten worden.

De bespreking van het artikel vermeldt in dat verband het volgende:

"De termijn van vier maanden is in aanmerking genomen voor de toepassing van het derde lid, aangezien de fraude een impact kan hebben op de facturering van de operator tegenover de abonnee (of van een onderneming tegenover de abonnee).

De minimale termijn van vier maanden bewaring houdt rekening met een volledige factureringscyclus (eerste maand volgend op het verbruik van de dienst), met een minimale duur voor betwisting (van 15 dagen tot 1 maand, de tweede maand volgend op het verbruik van de dienst), met een periode voor de behandeling van de betwisting die een uitwisseling tussen de abonnee en de operator mogelijk maakt (de derde maand volgend op de betwisting van de dienst) en met een periode van mogelijke vertraging in die behandeling (de vierde maand volgend op het verbruik).

De termijn van 4 maanden zal het ook mogelijk maken om rekening te houden met de ontwikkelingen op het stuk van fraude."

Hoewel die toelichting *prima facie* blijkbaar een bewaartermijn van vier maanden kan rechtvaardigen, zou de bewaring van de betrokken gegevens buiten die termijn echter beter door de ontworpen bepaling afgebakend moeten worden, teneinde te voorzien in een maximumtermijn die zich tevens hoe dan ook tot het strikt noodzakelijke beperkt, gelet op de doeleinden van de bewaring, namelijk enerzijds de fraudebestrijding en anderzijds de bestrijding van kwaadwillige oproepen, die per definitie twee verschillende doeleinden zijn.

2. De ontworpen paragraaf 4, vierde lid, van artikel 122 van de wet van 13 juni 2005 luidt als volgt:

"Wanneer een operator een mogelijk of bewezen geval van fraude of een mogelijk of bewezen geval van kwaadwillig gebruik van het netwerk heeft opgespoord, neemt hij de gepaste maatregelen, rekening houdend met de meest recente technische mogelijkheden, om te vermijden dat de eindgebruiker schade ondervindt of wordt ontriefd."

[41] *Beginselen van de wetgevingstechniek - Handleiding voor het opstellen van wetgevende en reglementaire teksten*, www.raadvst-consetat.be, tab "Wetgevingstechniek", aanbevelingen 226 en 227, formule F 5.

‡LW-BEHVMBJEH-GJDIBQW‡

Zoals die bepaling geredigeerd is, kan ze uitgelegd worden in die zin dat ze aan de operatoren uitzonderlijk grote verplichtingen oplegt welke zouden kunnen impliceren dat door hen maatregelen genomen moeten worden die er weliswaar op gericht zijn de belangen van een gebruiker te beschermen, maar die ten nadele van een andere gebruiker tot stand zouden komen op basis van elementen die na een adequaat onderzoek niet anderszins aangetoond worden door een administratieve overheid of een jurisdictioneel orgaan. Dergelijke verplichtingen zijn vatbaar voor kritiek in het licht van het recht op eerbiediging van het privéleven, de vrijheid van meningsuiting en het gelijkheids- en non-discriminatiebeginsel.

De bespreking van het artikel geeft in dat verband echter de volgende toelichting:

"Wanneer de operator een mogelijk of bewezen geval van fraude heeft opgespoord jegens zijn abonnee, dient hij de meest gepaste maatregelen te nemen om zijn abonnee te beschermen. Een van die maatregelen kan bestaan in het informeren van deze laatste, bijvoorbeeld hem melden dat de oproep frauduleus kan zijn.

Verder moeten de operatoren kunnen bijdragen tot het vaststellen van kwaadwillig gebruik van het netwerk (bijvoorbeeld door te bevestigen dat er wel degelijk een zekere communicatie is binnengekomen in het kader van een klacht in verband met telefonische pesterijen).

In geval van telefonische pesterijen moet het slachtoffer zich in de praktijk richten tot de Ombudsdienst voor telecommunicatie.

Deze laatste, die als opdracht heeft hulp te verlenen aan de slachtoffers en die niet onder een politiedienst valt, zal dan via de betrokken operatoren de naam, voornaam en het adres van de dader van de telefonische pesterijen kunnen krijgen en zal deze gegevens kunnen verstrekken aan het slachtoffer van die pesterijen (zie artikel 43*bis*, § 3, 7°, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven). In de praktijk zou een termijn van gegevensbewaring van minder dan 12 maanden problematisch zijn gezien de verschillende voormelde stappen die moeten worden gevolgd. Er dient ook te worden benadrukt dat de telefonische pesterijen geen impact zullen hebben op de facturering van de operator aan de abonnee, aangezien het om binnenkomende communicatie gaat."

Op de vraag wat de draagwijdte is van de voorliggende bepaling hebben de gemachtigden van de minister voorts in hoofdzaak het volgende geantwoord:

– wat betreft fraude en kwaadwillig gebruik, beperken de aldus verwachte tussenkomsten van de operatoren zich tot de kennelijke en algemeen verbreide vormen van fraude en kwaadwillig gebruik van het net, zoals het gebruik dat op alle of op een groep van eindgebruikers gericht is met het doel winst te maken of schade te berokkenen;

– voor het overige hebben de algemene verplichtingen die aan de operatoren opgelegd worden als zodanig geen betrekking op het kwaadwillig gebruik ten aanzien van bepaalde personen, zoals pestgedrag via communicatienetwerken, aangezien de ontworpen regeling niet strekt tot wijziging van de bestaande regeling die een voorafgaande tussenkomst van de ombudsdienst impliceert.

‡LW-BEHVMBJEH-GJDIBQW‡

Uit al die elementen volgt dat de verplichtingen die bij het hierboven weergegeven lid aan de operatoren opgelegd worden volgens de bedoeling van de stellers van het voorontwerp in feite een beperktere draagwijdte blijken te hebben dan die welke men uit de huidige redactie van die bepaling meent te kunnen afleiden.

Er moet evenwel rekening gehouden worden met het zesde lid van het ontworpen artikel 122, § 4, waarbij de Koning onder meer gemachtigd wordt om bij een besluit vastgesteld na overleg in de Ministerraad en na advies van het Instituut en de bevoegde gegevensbeschermingsautoriteiten "de acties [te bepalen] die de operator moet of mag ondernemen wanneer hij een vermoed of bewezen geval van fraude of van kwaadwillig gebruik van het netwerk heeft opgespoord".

Ter rechtvaardiging van het feit dat de Koning die acties – zonder daartoe gehouden te zijn – zou kunnen bepalen, wordt in de bespreking van het artikel het volgende gesteld:

> "De aanneming van dit koninklijk besluit is niet verplicht in het licht van de volgende uitdagingen. Ten eerste evolueert fraude aanzienlijk mettertijd. Bepaalde vormen van fraude kunnen verdwijnen of minder belangrijk worden terwijl nieuwe soorten van fraude kunnen opduiken.
>
> (…)
>
> Bovendien kunnen de acties die de operator onderneemt wanneer hij een mogelijk of bewezen geval van fraude heeft opgespoord, variëren naargelang van het type van fraude en van de graad van zekerheid die de operator heeft ten opzichte van het feit dat het wel degelijk om fraude gaat (enkel aanwijzingen of een zekerheid wat dat betreft)."

Gelet op die rechtvaardigingen rijst de vraag of het wel degelijk de bedoeling is om de verplichtingen die aan de operator opgelegd worden te beperken tot de kennelijke hinder (fraude of kwaadwillig gebruik), wat een grotere garantie zou bieden voor de proportionaliteit van de ontworpen bepaling in het licht van de hierboven besproken rechten en vrijheden, dan wel of dat niet de bedoeling is.

Hoewel de afdeling Wetgeving kan begrijpen dat de snelle evolutie en diversificatie van die hinder enige flexibiliteit en een vorm van reactiviteit vereisen, zouden de voornoemde rechten en vrijheden bovendien beter gewaarborgd worden indien de Koning gehouden – en niet gewoon gemachtigd – zou zijn een definitie te geven van de acties of de categorieën van acties die door de operator ondernomen moeten worden en hij daarbij het geval van kennelijke of "bewezen" hinder zou onderscheiden van de andere gevallen.

Ten slotte moeten de criteria ter afbakening van de aldus aan de Koning verleende machtiging door de wetgever gepreciseerd worden om te voldoen aan het legaliteitsbeginsel dat in artikel 22 van de Grondwet vervat is.

3. Uit de toelichtingen die de gemachtigden van de minister verstrekt hebben, blijkt dat het bestaan van een kwaadwillig gebruik van het netwerk, zoals bedoeld in het ontworpen artikel 122, § 4, zesde lid, niet door de operator aangetoond zal moeten worden maar door de ter zake bevoegde autoriteiten, zoals de ombudsdienst.

‡LW-BEHVMBJEH-GJDIBQW‡

De ontworpen tekst moet herzien en aangevuld worden zodat dat nader bepaald wordt.

4. De voorliggende bepaling moet in het licht van die opmerkingen herzien worden.

Artikel 5

1. Artikel 5, 1°, strekt tot vervanging van artikel 123, § 1, van de wet van 13 juni 2005, om daarin specifiek te voorzien in een regeling met betrekking tot de bewaring van de andere locatiegegevens dan de verkeersgegevens.

Die bepaling zet artikel 9 van richtlijn 2002/58/EG om, dat luidt als volgt:

"1. Wanneer andere locatiegegevens dan verkeersgegevens die betrekking hebben op gebruikers of abonnees van elektronische-communicatienetwerken of -diensten verwerkt kunnen worden, mogen deze gegevens slechts worden verwerkt wanneer zij anoniem zijn gemaakt of wanneer de gebruikers of abonnees daarvoor hun toestemming hebben gegeven, [voor zover] en voor zolang zulks nodig is voor de levering van een dienst met toegevoegde waarde. De dienstenaanbieder moet de gebruikers of abonnees, voorafgaand aan het verkrijgen van hun toestemming, in kennis stellen van de soort locatiegegevens anders dan verkeersgegevens, die zullen worden verwerkt, en van de doeleinden en de duur van die verwerking, en hun meedelen of deze gegevens aan een derde zullen worden doorgegeven ten behoeve van de levering van de dienst met toegevoegde waarde. Gebruikers of abonnees kunnen hun toestemming voor de verwerking van andere locatiegegevens dan verkeersgegevens te allen tijde intrekken.

2. Wanneer de gebruikers of abonnees toestemming hebben gegeven voor de verwerking van andere locatiegegevens dan verkeersgegevens, moet de gebruiker of abonnee de mogelijkheid behouden om op eenvoudige en kosteloze wijze tijdelijk de verwerking van dergelijke gegevens te weigeren voor elke verbinding met het netwerk of voor elke transmissie van communicatie.

3. De verwerking van locatiegegevens anders dan verkeersgegevens in overeenstemming met de leden 1 en 2, moet worden beperkt tot personen die werkzaam zijn onder het gezag van de aanbieder van het openbare elektronische-communicatienetwerk of de openbare elektronische-communicatiedienst of de derde die de dienst met toegevoegde waarde levert, en moet beperkt blijven tot hetgeen noodzakelijk is om de dienst met toegevoegde waarde te kunnen aanbieden."

2. Uit die bepaling volgt dat, wanneer de betrokken gegevens mogen worden verwerkt, die verwerking slechts plaatsvindt nadat die gegevens anoniem zijn gemaakt of de gebruikers of abonnees daarvoor hun toestemming hebben gegeven, voor zover en voor zolang zulks nodig is voor de levering van een dienst met toegevoegde waarde.

‡LW-BEHVMBJEH-GJDIBQW‡

Er is dus voorzien in twee gevallen, op voorwaarde dat die gegevens "mogen worden verwerkt":

– ofwel werden de gegevens anoniem gemaakt;

– ofwel heeft de gebruiker of abonnee zijn toestemming gegeven; in dit geval mogen ze slechts worden verwerkt voor zover en voor zolang zulks nodig is voor de levering van een dienst met toegevoegde waarde.

De ontworpen tekst voorziet dan weer in vijf gevallen. De gevallen die zijn opgenomen in het ontworpen artikel 123, § 1, 1°, 2° en 5° van de wet van 13 juni 2005, zijn niet opgenomen in artikel 9 van richtlijn 2002/58/EG.

Eén van die drie andere overwogen gevallen levert op zich geen moeilijkheden op. Wanneer de verwerking "noodzakelijk is om te voldoen aan een wettelijke verplichting" (ontworpen artikel 123, § 1, 5°), spreekt het immers voor zich dat die verwerking aanvaardbaar is van zodra de wetsbepaling die in die verwerking voorziet, zelf voldoet aan het voorschrift van richtlijn 2002/58/EG, en in het bijzonder artikel 15, lid 1, ervan. Met andere woorden, zo er al een probleem is, zou dat niet schuilen in het ontworpen artikel 123, § 1, 5°, van de wet van 13 juni 2005, maar, in voorkomend geval, in de bepaling(en) die voorzien in "de wettelijke verplichting", welke bepalingen zich elders in het ontwerp bevinden. Er wordt dan ook verwezen naar het onderzoek van die bepalingen.

De gevallen bedoeld in artikel 123, § 1, 1° en 2°, doen daarentegen vragen rijzen. Ze hebben betrekking op de bewaring en de verwerking:

1° "wanneer dat noodzakelijk is voor de goede werking en de veiligheid van het netwerk of van de dienst, waarbij de gegevens worden bewaard zolang dit voor dat doel noodzakelijk is", of

2° "wanneer dat noodzakelijk is om fraude of kwaadwillig gebruik van het netwerk op te sporen, waarbij de gegevens worden bewaard zolang dit voor dat doel noodzakelijk is".

Die twee gevallen doen denken aan de gevallen waarvan ook sprake is in artikel 4 van het voorontwerp dat zijnerzijds betrekking heeft op de verkeersgegevens, zoals bedoeld in artikel 6 van richtlijn 2002/58/EG.

Artikel 15, lid 1, van dezelfde richtlijn staat de lidstaten toe wettelijke maatregelen te treffen ter beperking van de reikwijdte van de in artikel 9 van deze richtlijn bedoelde rechten en plichten, maar dan wel onder de voorwaarden van dat artikel 15. De overwogen maatregel moet met name een in een democratische samenleving noodzakelijke, redelijke en proportionele maatregel zijn ter waarborging van de nationale veiligheid – d.w.z. de staatsveiligheid – de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronische-communicatiesysteem. Een dergelijke maatregel, die zou bestaan in het bewaren van gegevens, moet overigens in de tijd beperkt blijven tot hetgeen noodzakelijk is.

‡LW-BEHVMBJEH-GJDIBQW‡

Wat het ontworpen artikel 123 betreft, dient erop te worden gewezen dat

1° in de bespreking van het artikel geen melding wordt gemaakt van de gevallen waarvan sprake; *a fortiori* is het op grond van de bespreking van het artikel niet duidelijk in welk opzicht en of de overwogen maatregelen beantwoorden aan de voorwaarden van artikel 15, lid 1, van richtlijn 2002/58/EG, inzonderheid wat betreft de noodzakelijkheid, het doel en de evenredigheid;

2° de vermelding, in de ontworpen tekst, dat de gegevens "worden bewaard zolang dit voor [het beoogde] doel noodzakelijk is", niet nauwkeurig genoeg is; de wetgever zou op zijn minst een maximale bewaringstermijn moeten bepalen, die hij bovendien moet kunnen rechtvaardigen.

Het ontworpen artikel 123, § 1, 1° en 2°, moet worden herzien in het licht van die twee opmerkingen.

3. De bepaling onder 2°, eerste streepje, strekt tot opheffing van de woorden "definitief of tijdelijk", die voorkomen in artikel 123, § 2, 1°, e), van de wet van 13 juni 2005.

In de bespreking van het artikel staat daarover het volgende:

> "Paragraaf 2 beoogt niet langer de tijdelijke of definitieve intrekking van de toestemming aangezien het begrip van toestemming in de zin van de AVG niet voorziet in een dergelijk onderscheid."

Die verantwoording gaat echter voorbij aan het feit dat volgens artikel 9 van richtlijn 2002/58/EG gebruikers en abonnees die hun toestemming hebben gegeven voor de verwerking van andere locatiegegevens dan verkeersgegevens, de mogelijkheid behouden om op eenvoudige en kosteloze wijze tijdelijk de verwerking van dergelijke gegevens te weigeren voor elke verbinding met het netwerk of voor elke transmissie van communicatie.

De voorliggende bepaling moet aldus worden herzien dat artikel 123 van de wet van 13 juni 2005 uitdrukkelijk in die mogelijkheid voorziet.

Artikel 7

Zelfs indien de ontworpen paragraaf 2 de Koning machtigt om de te bewaren gegevens te definiëren en de vereisten waaraan die moeten beantwoorden, zou het beter zijn in het ontworpen dispositief op zijn minst het begrip "abonnementsgegevens", uitdrukkelijk te definiëren. Hetzelfde geldt voor het begrip "onderliggende elektronische communicatienetwerken".

‡LW-BEHVMBJEH-GJDIBQW‡

Artikel 10

1. Het ontworpen artikel 127/1 geeft een vrij algemene opsomming van de categorieën van autoriteiten die toegang hebben tot de gegevens die worden bewaard krachtens de artikelen 122, 123, 126, 126/1, en 127, en voor welke doeleinden.

In de filosofie van de ontworpen tekst en zoals in de bespreking van het artikel wordt uiteengezet,

> "is het nodig dat [de autoriteit] beantwoordt aan een van de doeleinden bedoeld in artikel 127/1 en dat haar organieke of sectorale wet haar machtigt om deze gegevens te krijgen van de operator opdat [ze] gegevens kan krijgen van de operator."

Hoewel het gemakkelijk te begrijpen valt dat het in de bedoeling van de stellers van het voorontwerp ligt om de voorwaarden voor het bewaren van de gegevens in de wet van 13 juni 2005 op te nemen, terwijl de voorwaarden voor toegang tot die gegevens thuishoren in de organieke wetgeving van de overheden waarvoor een machtiging tot toegang in overweging wordt genomen, neemt dit niet weg dat, om een nuttig gevolg te geven aan de finaliteit of finaliteiten van een bewaring, de autoriteiten die toegang hebben tot de gegevens dezelfde finaliteit dienen na te streven. Het doel dient ook voldoende nauwkeurig te worden omschreven en de regels die de doeleinden van bewaring en toegang omschrijven, moeten gemakkelijk te begrijpen zijn.

De vraag rijst of de bij het ontworpen artikel 127/1 ingevoerde regeling, in samenhang met enerzijds de algemene bepalingen inzake de bewaring van de gegevens, en anderzijds de specifieke bepalingen die de toegang tot de gegevens bepalen, aan die vereisten voldoet.

2. Volgens de bespreking van het artikel hebben de stellers van het voorontwerp, bij het aannemen van artikel 127/1, de volgende doelstellingen:

> "(...) enerzijds om, in een zekere mate, de operatoren rechtszekerheid te bieden wat betreft de autoriteiten die het recht hebben om toegang te krijgen tot de gegevens die ze bewaren en anderzijds om de eindgebruikers transparantie te geven over het gebruik van hun identificatie-, verkeers- en locatiegegevens".

De afdeling Wetgeving vraagt zich echter zich af of die bepaling, zoals ze is geformuleerd, niet een pervers effect zou kunnen hebben dat in strijd is met de rechtszekerheid.

Aldus kan het ontworpen artikel 127/1, ook al verwijst het, wat de toegang betreft, uitdrukkelijk naar de voorwaarden die zijn vastgesteld in de specifieke bepalingen op grond waarvan de categorieën van betrokken autoriteiten toegang hebben tot de bewaarde gegevens, de indruk wekken dat alle daarin genoemde categorieën van autoriteiten toegang hebben tot alle in de artikelen 122, 123, 126, en 126/1 bedoelde gegevens.

Dit kan evenwel tot verwarring leiden.

‡LW-BEHVMBJEH-GJDIBQW‡

Zo kunnen de algemene en ongedifferentieerde bewaring van de IP-bron adressen bedoeld in artikel 123 van de wet van 13 juni 2005, zoals het bij het ontwerp wordt gewijzigd, en de gegevens die het voorwerp uitmaken van een gerichte bewaring als bedoeld in het ontworpen artikel 126/1, enkel worden bewaard ten behoeve van de vrijwaring van de nationale veiligheid, de strijd tegen zware criminaliteit en de preventie van ernstige dreigingen van de openbare veiligheid.

Die beperking blijkt niet uit de lezing van artikel 127/1, waarvan paragraaf 1, 1°, heel algemeen verwijst naar de preventie, het onderzoek, de opsporing en de vervolging van strafrechtelijke inbreuken, van inbreuken waarvoor een administratieve sanctie met strafkarakter kan worden opgelegd, of inbreuken gepleegd met behulp van een elektronisch-communicatienetwerk.

Wat de doelgerichte geografische bewaring betreft, vermeldt artikel 126/1 dat de betrokken gegevens worden bewaard ten behoeve van de vrijwaring van de nationale veiligheid, de strijd tegen zware criminaliteit en de preventie van ernstige dreigingen van de openbare veiligheid en de bescherming van de vitale belangen van een natuurlijke persoon. Wat het openbaar ministerie betreft, volgt de naleving van het criterium "zware criminaliteit" tevens uit het ontworpen artikel 39*quinquies*, van het Wetboek van Strafvordering (artikel 17 van het voorontwerp).

Aangezien het ontworpen artikel 127/1, § 1, ertoe strekt de finaliteit van de toegang te omschrijven, neemt dat niet weg dat die finaliteit in verband moet kunnen worden gebracht met de finaliteit van de ingevoerde regeling voor de bewaring van de gegevens. Wat evenwel de bewaring van IP-bron adressen betreft, wordt in het ontworpen artikel 126, § 1, die enkel verwijst naar de doeleinden bedoeld in het ontworpen artikel 127/1, geen enkele specifieke finaliteit genoemd. Die verwijzing is ontoereikend in het licht van de eisen van het Hof van Justitie met betrekking tot de bescherming van de nationale veiligheid, de bestrijding van ernstige criminaliteit en het voorkomen van ernstige bedreigingen van de openbare veiligheid.

De ontworpen bepaling moet derhalve worden herzien om het verband tussen het doeleinde van de bewaring en het doeleinde van de toegang duidelijk te maken en om elke dubbelzinnigheid weg te nemen die ertoe zou kunnen leiden dat bijvoorbeeld in gevallen waarin de bewaring enkel kan plaatsvinden ter bestrijding van zware criminaliteit, de autoriteiten toegang tot die gegevens zouden kunnen krijgen om niet-zware criminaliteit te bestrijden.

2. De beoordeling van het begrip "administratieve sanctie met strafkarakter" – d.i., volgens de bespreking van het artikel, een sanctie die in het interne recht als administratieve sanctie wordt bestempeld, maar die als strafrechtelijk kan worden aangemerkt in de zin van het Verdrag inzake de bescherming van de Rechten van de Mens en de Fundamentele Vrijheden – mag niet worden overgelaten aan de operator die toegang tot de bewaarde gegevens zou verlenen, noch aan de autoriteit die toegang tot de gegevens zou vragen.

Dat bij uitstek jurisprudentiële begrip hangt dus af van een beoordeling van elk geval afzonderlijk, wat niet verenigbaar is met de voorzienbaarheid en de nauwkeurigheid die wordt verwacht van een wettelijke regeling die voorziet in een systeem van inmenging in het recht op eerbiediging van het privéleven.

‡LW-BEHVMBJEH-GJDIBQW‡

3. Gelet op de aldus benadrukte elementen, vraagt de afdeling Wetgeving zich af of de voorliggende bepaling niet eerder van aard is om de rechtszekerheid te ondermijnen, in plaats van deze te waarborgen.

Die bepaling moet in het licht van de voorgaande opmerkingen opnieuw worden onderzocht.

Artikel 11

1. Het is de afdeling Wetgeving niet duidelijk wat de strekking is van het derde lid van het ontworpen artikel 127/2, § 2, dat als volgt luidt:

> "De operatoren zijn in staat verbanden te leggen tussen de gegevens bewaard voor de autoriteiten."

In de bespreking van het artikel wordt in dat verband het volgende vermeld:

> "Het is aan de operatoren om te beslissen hoe ze zich organiseren voor de bewaring van de gegevens ten behoeve van de autoriteiten (in het bijzonder de gegevens bewaard conform de artikelen 126, 126/1, 127). Wanneer eenzelfde gegeven wordt bedoeld in verscheidene artikelen, mogen ze dat gegeven dus één keer bewaren. De operatoren moeten daarentegen in staat zijn om verbanden te leggen tussen de gegevens bewaard voor de autoriteiten. Dat is nodig aangezien een operator, om te antwoorden op een verzoek van een autoriteit, genoopt zou kunnen zijn om gegevens te raadplegen die zijn bewaard op basis van verschillende artikelen."

Aldus laat de bespreking van het artikel niet toe om beter te begrijpen wat de aard is van het "verband" dat de operator moet leggen tussen de bewaarde gegevens.

De voorliggende bepaling mag op zijn minst geen verplichting opleggen die de operator zou belasten met de beoordeling, uit opportuniteitsoverwegingen, van de inhoud van de desbetreffende gegevens en van de relevantie om tussen die gegevens een verband te leggen. Met andere woorden, het te leggen verband kan enkel technisch of technologisch van aard zijn, en het leggen van dat verband mag de operator er als het ware niet toe brengen om de gegevens waartoe alleen de autoriteiten die daartoe gemachtigd zijn, toegang hebben, te onderzoeken of te analyseren.

Op een vraag in dat verband hebben de gemachtigden van de minister geantwoord dat dit niet de bedoeling is. De voorliggende bepaling en de bespreking van het artikel moeten worden herzien om de bedoeling van de steller ervan duidelijk weer te geven.

3. Wat de in het ontworpen artikel 127/2, § 3, tweede lid, 1°, beoogde vernietiging van de gegevens betreft, zou het dispositief beter tegemoetkomen aan de vereisten inzake de onherroepelijke vernietiging van de gegevens indien een autoriteit, zoals het Instituut, specifiek zou worden belast met de regelmatige controle op die vernietiging.[42]

[42] Zie in die zin advies 58.449/4, punt 3.4.2.2.2.

‡LW-BEHVMBJEH-GJDIBQW‡

Artikel 12

Paragraaf 3 van het ontworpen artikel 127/3 luidt als volgt:

"De Koning kan na advies van de bevoegde gegevensbeschermingsautoriteiten, en van het Instituut het volgende bepalen:

1° de vereisten waaraan de Coördinatiecel moeten beantwoorden, in het bijzonder op het vlak van beschikbaarheid en bereikbaarheid;

2° de vereisten waaraan een lid van de Coördinatiecel moet beantwoorden, inclusief hem in voorkomend geval verplichten om het voorwerp uit te maken van een positief veiligheidsadvies;

3° indien een positief veiligheidsadvies wordt opgelegd, de categorieën van operatoren die vrijgesteld zijn van de verplichting om een veiligheidsofficier aan te stellen zoals bepaald in artikel 22quinquies, § 6, van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, alsook de regels die van toepassing zijn bij gebrek aan een dergelijke officier;

4° de regels die het mogelijk maken dat de Belgische autoriteiten die de contactgegevens van de Coördinatiecel en van de leden ervan moeten kennen, daarvan op de hoogte worden gebracht;

5° de overige regels die de samenwerking van de operatoren met de Belgische autoriteiten of met sommige van hen regelen, met inbegrip van, in voorkomend geval en per betrokken overheid:

a) de overdrachtsmodus, de vorm en de inhoud van de verzoeken en antwoorden;

b) het dringendheidsniveau voor de behandeling van de verzoeken;

c) de reactietermijn voor de antwoorden;

d) de vereiste beschikbaarheid van de dienst;

e) de modaliteiten voor het testen van de samenwerking;

f) de tarieven van de vergoeding van die samenwerking.

Indien nodig kan de Koning verschillende regels bepalen volgens verschillende categorieën van operatoren, met name volgens het aantal vorderingen dat zij ontvangen van de gerechtelijke autoriteiten en de inlichtingen- en veiligheidsdiensten, de plaats van vestiging en de plaats waar zij hun activiteiten uitvoeren."

Die bepaling geeft aanleiding tot verschillende opmerkingen.

2. In het ontworpen artikel 127/3, § 3, wordt bepaald dat de Koning de regels waarvan het voorwerp erin is opgenomen, "kan" bepalen en niet dat Hij die regels "bepaalt".

Bij gebrek aan uitvoering door de Koning van de mogelijkheid die Hem wordt verleend bij die ontworpen bepaling, zal bijgevolg geen enkele regel met betrekking tot de verschillende opgesomde punten worden vastgesteld.

Zo zou het bijvoorbeeld kunnen dat er geen enkele regel betreffende de vereisten waaraan de leden van de Coördinatiecel moeten voldoen, wordt bepaald.

‡LW-BEHVMBJEH-GJDIBQW‡

Die vereisten zijn evenwel van essentieel belang teneinde te verzekeren dat de Coördinatiecel doeltreffend en efficiënt zal samenwerken met de autoriteiten en dat ze over alle passende waarborgen zal beschikken voor de bewaring en de veilige overdracht van de betrokken gegevens, overeenkomstig de bepalingen van de ontworpen wet.

Bijgevolg dient de ontworpen machtiging zodanig te worden opgesteld dat de Koning niet alleen gemachtigd, maar ertoe gehouden is om de desbetreffende regels vast te leggen.

3. Het staat aan de wetgever om de criteria te bepalen die de Koning moet hanteren wanneer Hij uitvoering moet geven aan de ontworpen bepaling, in het bijzonder wat betreft de regels die vervat zijn in de ontworpen paragraaf 3, eerste lid, 2° en 3°.

Dat geldt in het bijzonder voor de principiële vraag of al dan niet een positief veiligheidsadvies wordt opgelegd, zelfs los van het feit dat de verschillende regels die, op basis van de criteria waarin het tweede lid van de ontworpen derde paragraaf voorziet, aan verschillende categorieën van operatoren zouden worden opgelegd.[43]

4. De voorliggende bepaling moet worden herzien in het licht van de voorgaande opmerkingen.

Artikel 13

Artikel 13 van het voorontwerp strekt ertoe in de wet van 13 juni 2005 een nieuw artikel 127/4 in te voegen dat als volgt luidt:

> "Bij een besluit vastgesteld na overleg in de Ministerraad, stelt de Koning op voorstel van de minister van Justitie en de minister, na advies van de bevoegde gegevensbeschermingsautoriteiten en van het Instituut, de voorwaarden vast waaronder de aanbieders van private elektronische-communicatienetwerken en elektronische-communicatiediensten die niet openbaar beschikbaar zijn de gegevens die de identificatie mogelijk maken van de betrokken personen, van de eindapparatuur of van de gebruikte elektronische-communicatiedienst, met uitzondering van de gegevens die verband houden met één enkele elektronische communicatie, registreren en bewaren, met het oog op het opsporen en de beteugeling van strafbare feiten en met het oog op de beteugeling van kwaadwillige oproepen naar de nooddiensten, voor het onderzoek bij de ombudsdienst voor telecommunicatie naar de identiteit van elke persoon die kwaadwillig gebruik heeft gemaakt van een elektronische-communicatienetwerk of -dienst, evenals met het oog op de vervulling van de inlichtingsopdrachten bepaald in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.
>
> Bij een besluit vastgesteld na overleg in de Ministerraad, stelt de Koning op voorstel van de minister van Justitie en de minister, na advies van de bevoegde gegevensbeschermingsautoriteiten en van het Instituut, de technische en administratieve maatregelen vast die aan de aanbieders beoogd in het eerste lid worden opgelegd om de betrokken personen te kunnen identificeren en het opsporen, lokaliseren, afluisteren, kennisnemen en opnemen van niet voor het publiek toegankelijke [communicatie]

[43] Zie in soortgelijke zin advies 58.449/4, opmerking bij artikel 5.

‡LW-BEHVMBJEH-GJDIBQW‡

mogelijk te maken onder de voorwaarden bepaald door de artikelen 46*bis*, 88*bis*, 90*ter* tot 90*decies*, 464/13, 464/25 en 464/26 van het Wetboek van strafvordering, evenals de voorwaarden bepaald in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

De aanbieders beoogd in het eerste lid zorgen ervoor dat de in het eerste lid van deze paragraaf vermelde gegevens onbeperkt toegankelijk zijn vanuit België."

Die machtigingen zijn kennelijk te verregaand. Met betrekking tot de aanbieders van private elektronische-communicatienetwerken en elektronische-communicatiediensten die niet voor het publiek toegankelijk zijn, hebben ze immers tot doel de Koning te machtigen om volledig de regelingen te bepalen die gelden:

– inzake de registratie en de bewaring van de gegevens die de identificatie mogelijk maken van de betrokken personen, van de eindapparatuur of van de gebruikte elektronische-communicatiedienst, ook met het oog op het opsporen en de beteugeling van strafbare feiten, met het oog op de beteugeling van kwaadwillige oproepen naar de nooddiensten, voor het onderzoek bij de ombudsdienst voor telecommunicatie naar de identiteit van elke persoon die kwaadwillig gebruik heeft gemaakt van een elektronische-communicatienetwerk of -dienst, evenals met het oog op de vervulling van de inlichtingsopdrachten bepaald in de wet van 30 november 1998;

– met betrekking tot de maatregelen om de betrokken personen te kunnen identificeren en het opsporen, lokaliseren, afluisteren, kennisnemen en opnemen van niet voor het publiek toegankelijke communicatie mogelijk te maken onder de voorwaarden bepaald in het Wetboek van Strafvordering en in de wet van 30 november 1998.

Gelet op het in artikel 22 van de Grondwet vervatte legaliteitsbeginsel, moet voor dergelijke inmengingen in het recht op eerbiediging van het privéleven, meer bepaald het bewaren van en de toegang tot persoonsgegevens, voorzien worden in een regeling die naar behoren afgebakend wordt door de wetgever.

In casu ontbreekt een dergelijke regeling totaal.

De voorliggende bepaling moet bijgevolg grondig herzien worden.

Artikel 14

1. In de ontworpen paragraaf 2, derde lid, dienen de woorden "De in het eerste lid bedoelde" vervangen te worden door de woorden "De in het tweede lid bedoelde".

2. In de ontworpen paragraaf 2, zesde lid, dient de aard omschreven te worden van de nietigheid waarvan sprake is: gaat het, zoals verondersteld kan worden, om nietigheid van rechtswege en van openbare orde?

‡LW-BEHVMBJEH-GJDIBQW‡

Artikel 16

1. Artikel 16 strekt ertoe een punt 2°/1 in te voegen in artikel 14, § 2, van de wet van 17 januari 2003 'met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector' teneinde het voor het Instituut mogelijk te maken om "van de operatoren de identificatie-, verkeers- of locatiegegevens [te] vragen in de zin van de wet van 13 juni 2005 betreffende de elektronische communicatie, op voorwaarde dat dat nodig is voor de vervulling van een van zijn opdrachten".

Het Instituut zou aldus toegang kunnen hebben tot alle gegevens die opgesomd worden, zonder dat een onderscheid gemaakt wordt tussen de categorieën van gegevens en zonder dat uitdrukkelijk aangegeven wordt welke precieze bedoeling die toegang rechtvaardigt.

Het ontworpen artikel 127, § 1, maakt geen betere afbakening mogelijk van de inmenging waartoe het Instituut aldus gemachtigd wordt, aangezien in dat ontworpen artikel 127/1, § 1, enkel bepaald wordt dat, wat het Instituut betreft, de bewaring van de gegevens bedoeld in de artikelen 122, 123, 126, 126/1 en 127, van de wet van 13 juni 2005, zoals die zullen luiden nadat ze bij de ontworpen tekst gewijzigd zullen zijn, "de uitvoering en de toetsing van de wet" van 13 juni 2005 als doel heeft.

In de bespreking van het artikel staat in dat verband het volgende:

> "De ingevoegde bepaling beoogt dat het Instituut toegang kan hebben tot de identificatie-, verkeers- of locatiegegevens in de zin van de wet van 13 juni 2005 betreffende de elektronische communicatie, wanneer dat nodig blijkt voor de vervulling van een van zijn opdrachten.
>
> Dat is met name het geval bij de controle van de inachtneming door de operatoren van hun wettelijke verplichtingen zoals de verplichting om een gedetailleerde facturering op te stellen, vastgelegd in artikel 110 van de wet van 13 juni 2005 betreffende de elektronische communicatie, of in het kader van de tenuitvoerbrenging van artikel 114 van diezelfde wet. Zo moet het BIPT, in het geval van de gedetailleerde facturering, in staat zijn om een operator een staal van zijn facturen te vragen. Deze facturen bevatten verkeersgegevens, zoals de ontvangers, data, tijdstippen en duur van de gevoerde gesprekken."

2. Vastgesteld moet worden dat een toegang die zo algemeen is als die waarin door de ontworpen tekst voorzien wordt, wat de proportionaliteit betreft, niet verantwoord lijkt ten aanzien van artikel 15, lid 1, van richtlijn 2002/58/EG, zoals begrepen in het licht van de desbetreffende rechtspraak van het Hof van Justitie.

Het in de bespreking van het artikel vermelde voorbeeld, dat uitermate gericht blijkt te zijn, ontkracht daarentegen de noodzaak om zo'n ruime toegang toe te staan.

Even fundamenteel is de vraag welke daadwerkelijke waarborgen de betrokken personen zouden genieten tegen eventuele misbruiken.

3. De voorliggende bepaling moet in het licht van de voorgaande opmerkingen herzien worden.

‡LW-BEHVMBJEH-GJDIBQW‡

Artikel 24

1. Uit de bespreking van het artikel blijkt dat het eerste lid, 1°, van het ontworpen artikel 16/2/1 van de wet van 30 november 1998 betrekking heeft op een bevel tot een klassieke "*quick freeze*" van de reeds door de operatoren bewaarde gegevens, terwijl het eerste lid, 2°, ervan betrekking heeft op een bevel tot een "*quick freeze*" voor de toekomst.

In het ontworpen dispositief komt dat onderscheid niet duidelijk tot uiting, inzonderheid niet wat de exacte draagwijdte is van het bevel waarin het ontworpen eerste lid, 2°, voorziet.

2. Bovendien dient met betrekking tot de duur van bewaring van de gegevens een onderscheid gemaakt te worden tussen de twee voormelde gevallen.

Zo wordt met betrekking tot de klassieke "*quick freeze*" in het vierde lid van de ontworpen bepaling een antwoord gegeven op de vraag hoelang de gegevens bewaard moeten worden waarvoor een bevel tot bewaring gegeven werd.

Wat daarentegen de "*quick freeze*" voor de toekomst betreft, is de ontworpen bepaling niet duidelijk genoeg: op basis van die bepaling is het niet mogelijk om een onderscheid te maken tussen de duur van de "*quick freeze*" maatregel enerzijds en de duur van bewaring van de aldus bevroren gegevens anderzijds. Om ervoor te zorgen dat de "*quick freeze*" voor de toekomst niet verder gaat dan wat strikt noodzakelijk is voor de nationale veiligheid, zou de ontworpen tekst op dat punt aangevuld moeten worden teneinde, onder voorbehoud van een eventuele verlenging, een maximumduur vast te stellen voor de bewaring.[44] Een andere mogelijkheid zou erin kunnen bestaan om de bewaring van de gegevens te beperken tot de duur van de "*quick freeze*". Elke dubbelzinnigheid ter zake dient hoe dan ook weggenomen te worden.

In de context van de aldus ingevoerde regeling , is het de afdeling Wetgeving ten slotte niet duidelijk wat de exacte draagwijdte is van het achtste lid waarin bepaald wordt dat de door de operatoren bewaarde gegevens twaalf maanden na het begin van hun bewaring vernietigd worden.

3. De ontworpen bepaling moet herzien worden teneinde elke dubbelzinnigheid over de ingevoerde regeling weg te nemen, in het bijzonder wat betreft de duur van de "*quick freeze*" voor de toekomst en wat betreft de bewaartermijn van de gegevens, en dit om te garanderen dat die termijn tot het strikt noodzakelijke beperkt wordt en dat de gegevens door de operatoren vernietigd worden zodra die noodzaak komt te vervallen.

[44] Vergelijk met het ontworpen artikel 39*quinquies*, derde lid, zesde en zevende streepje, van het Wetboek van Strafvordering (artikel 17 van het voorontwerp).

‡LW-BEHVMBJEH-GJDIBQW‡

Artikel 28

De afdeling wetgeving heeft in haar advies 42.178/2 van 19 februari 2007 over een voorontwerp dat geleid heeft tot de wet van 4 februari 2010 'betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten'[45], reeds benadrukt dat, hoewel de evenredigheids-en subsidiariteitsbeginselen bepalend zijn voor het aanwenden van de specifieke methodes en, *a fortiori*, de uitzonderlijke methodes, het bovendien van belang is na te gaan of de bij het voorontwerp ingevoerde controlemiddelen de effectieve waarborg bieden dat deze methodes zullen worden aangewend met inachtneming van de fundamentele rechten.

Om de naleving van die beginselen te garanderen, zou de ontworpen bepaling moeten worden aangevuld om te voorzien in een maximumduur – waarbij in voorkomend geval wordt voorzien in een verlenging die wordt gerechtvaardigd door de strikte noodzakelijkheid – van de opsporing of lokalisatie, welke duur in verhouding zou staan tot de ernst van de gegevens die de aanwending van de methode rechtvaardigen.

Bovendien ziet de afdeling Wetgeving, wat de procedurele waarborgen betreft, niet in hoe het gerechtvaardigd kan worden dat voor de voorgenomen specifieke methode geen schriftelijke beslissing van het diensthoofd vereist is, zoals het geval is voor andere specifieke methoden.

De voorliggende bepaling moet worden herzien in het licht van die opmerkingen.

Artikel 34

Het ontworpen artikel 62, paragraaf 2, tweede lid, van de wet van 7 april 2019 'tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid' bepaalt dat het nationaal Computer Security Incident Response Team (afgekort "CSIRT") om toegang te krijgen tot de door de operatoren bewaarde identificatie- , verkeers- en locatiegegevens, zich houdt aan "de regels en procedures bedoeld in de wet van 13 juni 2005 betreffende de elektronische communicatie".

Die bepaling laat qua duidelijkheid te wensen over. Ze moet verwijzen naar de precieze bepalingen van de wet van 13 juni 2005 die, in voorkomend geval, uitgaande van verschillende hypotheses, van toepassing zullen zijn op het Nationaal CSIRT.

Het ontworpen artikel 62 moet dienovereenkomstig worden herzien en aangevuld.

[45] http://www.raadvst-consetat.be/dbx/adviezen/42178.pdf.

‡LW-BEHVMBJEH-GJDIBQW‡

Artikel 36

1. Artikel 36 bepaalt dat de ontworpen wet "in werking treedt [lees: "uitwerking heeft"] op de dag waarop de vernietiging van de wet van 29 mei 2016 door het arrest nr. 57/2021 van het Grondwettelijk Hof gevolgen ressorteert".

De bespreking van het artikel stelt het volgende:

"De wet treedt retroactief in werking, zodat er geen juridisch vacuüm ontstaat waardoor belangrijke elektronische communicatiegegevens die cruciaal zouden zijn voor het onderzoek, niet langer zouden bewaard worden".

Zoals artikel 36 is gesteld, strekt het ertoe aan de voorliggende wet terugwerkende kracht te verlenen tot de dag waarop de vernietiging van de wet van 29 mei 2016 zelf uitwerking heeft gehad, dat wil zeggen tot de dag van de inwerkingtreding van die wet.

2.2. Het voorliggende voorontwerp strekt immers tot invoering van een gearticuleerd systeem voor de bewaring van en de toegang tot persoonsgegevens op het gebied van de elektronische communicatie.

De kern van de ontworpen regeling ligt in de artikelen 126 tot 127/4 die bij het voorontwerp worden ingevoegd in de wet van 13 juni 2005.

De schending van die nieuwe bepalingen zal strafrechtelijk worden bestraft krachtens de wijzigingen die bij artikel 15 van het voorontwerp worden aangebracht in artikel 145, § 1, van dezelfde wet.

Dat artikel 15 strekt er tevens toe aan hetzelfde artikel 145 een paragraaf 3*ter* toe te voegen die luidt als volgt:

"Met geldboete van 50 euro tot 50 000 euro en met gevangenisstraf van zes maanden tot drie jaar of met één van die straffen alleen wordt gestraft:

1° iedere persoon die, naar aanleiding van de uitoefening van zijn functie, buiten de gevallen die de wet bepaalt of zonder inachtneming van de vormen die zij voorschrijft, met bedrieglijk opzet of met het oogmerk om te schaden, de door de operator voor de autoriteiten bewaarde gegevens op enige manier overneemt, bij zich houdt of er enig gebruik van maakt.

2° hij die, terwijl hij weet dat de gegevens bekomen zijn door het plegen van het misdrijf bedoeld in 1°, deze gegevens bij zich houdt, aan een andere persoon onthult of verspreidt, of er enig gebruik van maakt."

De terugwerkende kracht die aan het voorontwerp bij artikel 36 ervan wordt verleend, schendt bijgevolg het beginsel dat strafwetten niet terugwerken, welk beginsel is vastgelegd in artikel 7 van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden en in artikel 15 van het Internationaal verdrag inzake burgerrechten en politieke rechten.

‡LW-BEHVMBJEH-GJDIBQW‡

2.3. Voorts dient eraan te worden herinnerd dat het Grondwettelijk Hof in zijn arrest nr. 57/2021 de bij artikel 8, derde lid, van de bijzondere wet op het Grondwettelijk Hof van 6 januari 1989 geboden mogelijkheid heeft geweigerd om de gevolgen van de vernietigde bepalingen van de wet van 29 mei 2016 te handhaven. Daarmee heeft het Hof uitvoering gegeven aan hetgeen het Hof van Justitie zelf in zijn arrest *La Quadrature du Net* had geoordeeld, namelijk dat:

> "aan de voorrang en de uniforme toepassing van het Unierecht zou afbreuk worden gedaan indien de nationale rechterlijke instanties bevoegd waren om, al was het maar tijdelijk, aan nationale bepalingen voorrang te geven boven het Unierecht waarmee deze bepalingen in strijd zijn."[46]

De uitgesproken nietigverklaring heeft dus zelf *ex tunc* "uitwerking gehad" op de dag waarop de wet van 29 mei 2016 in werking is getreden.

De terugwerkende kracht die aan het voorliggende dispositief wordt verleend, zal ertoe leiden dat *ex post* rechtsgrond wordt verleend aan een reeks inmengingen in het recht op eerbiediging van het privéleven waarvoor thans geen rechtsgrond voorhanden is als gevolg van het vernietigingsarrest nr. 57.2021 van het Grondwettelijk Hof dat, gelet op het arrest *La Quadrature du Net* van het Hof van Justitie, geen beperking in de tijd bevat. In zoverre ze tot gevolg heeft dat de inmengingen in de grondrechten van personen – van wie de gegevens zijn bewaard, voor het verleden worden gevalideerd – welke inmengingen geacht moeten worden strijdig te zijn met het Unierecht, is een dergelijke terugwerkende kracht niet aanvaardbaar in het licht van het Unierecht[47].

3. Uit de voorgaande overwegingen volgt dat artikel 36 moet worden weggelaten.

LE GREFFIER – DE GRIFFIER LE PRÉSIDENT – DE VOORZITTER

Anne-Catherine VAN GEERSDAELE Martine BAGUET

[46] Punt 217.

[47] Voor het overige dient eraan te worden herinnerd dat het Grondwettelijk Hof in zijn arrest nr. 57/2021 van 22 april 2021 uitdrukkelijk heeft bepaald dat de bewijzen die zouden zijn verzameld met toepassing van de vernietigde bepalingen van de wet van 29 mei 2016, per geval toelaatbaar kunnen worden verklaard:
"B.24.3 Het staat aan de bevoegde strafrechter, in voorkomend geval, uitspraak te doen over de toelaatbaarheid van de bewijzen die werden verzameld bij de tenuitvoerlegging van de vernietigde bepalingen, overeenkomstig artikel 32 van de voorafgaande titel van het Wetboek van stafvordering en in het licht van de door het Hof van Justitie in het voormelde arrest van 6 oktober 2020 aangebrachte preciseringen."

‡LW-BEHVMBJEH-GJDIBQW‡