Verfassungsgerichtshof

Entscheid Nr. 97/2024
vom 26. September 2024
Geschäftsverzeichnisnrn. 7907, 7929, 7930, 7931 und 7932

In Sachen: Klagen auf völlige oder teilweise Nichtigerklärung des Gesetzes vom 20. Juli 2022 « über die Sammlung und Speicherung von Identifizierungsdaten und Metadaten im Bereich der elektronischen Kommunikation und die Übermittlung dieser Daten an die Behörden », erhoben von der Kammer der französischsprachigen und deutschsprachigen Rechtsanwaltschaften, von der VoG « Académie Fiscale » und Jean Pierre Riquet, von der VoG « Liga voor Mensenrechten », von der VoG « Ligue des droits humains » und von Jens Hermans und anderen.

Der Verfassungsgerichtshof,

zusammengesetzt aus den Präsidenten Pierre Nihoul und Luc Lavrysen, und den Richtern Thierry Giet, Joséphine Moerman, Michel Pâques, Yasmine Kherbache, Danny Pieters, Sabine de Bethune, Emmanuelle Bribosia, Willem Verrijdt, Kattrin Jadin und Magalie Plovie, unter Assistenz des Kanzlers Nicolas Dupont, unter dem Vorsitz des Präsidenten Pierre Nihoul,

erlässt nach Beratung folgenden Entscheid:

I. *Gegenstand der Klagen und Verfahren*

a. Mit einer Klageschrift, die dem Gerichtshof mit am 2. Januar 2023 bei der Post aufgegebenem Einschreibebrief zugesandt wurde und am 4. Januar 2023 in der Kanzlei eingegangen ist, erhob die Kammer der französischsprachigen und deutschsprachigen Rechtsanwaltschaften, unterstützt und vertreten durch RA Alexandre Cassart, in Charleroi zugelassen, und durch RA Jean-François Henrotte, RÄin Elisabeth Kiehl und RA Eric Lemmens, in Lüttich-Huy zugelassen, Klage auf Nichtigerklärung des Gesetzes vom 20. Juli 2022 « über die Sammlung und Speicherung von Identifizierungsdaten und Metadaten im Bereich der elektronischen Kommunikation und die Übermittlung dieser Daten an die Behörden » (veröffentlicht im *Belgischen Staatsblatt* vom 8. August 2022).

b. Mit Klageschriften, die dem Gerichtshof mit am 3., 6. und 8. Februar 2023 bei der Post aufgegebenen Einschreibebriefen zugesandt wurden und am 6., 7., 8. und 9. Februar 2023 in der Kanzlei eingegangen sind, erhoben Klage auf völlige oder teilweise (Artikel 2 bis 17) Nichtigerklärung desselben Gesetzes: die VoG « Académie Fiscale » und Jean Pierre Riquet, die VoG « Liga voor Mensenrechten », unterstützt und vertreten durch RA Raf Jespers, in

Antwerpen zugelassen, die VoG « Ligue des droits humains », unterstützt und vertreten durch RÄin Catherine Forget, in Brüssel zugelassen, und Jens Hermans, die Privatstiftung « Ministry of Privacy » und Matthias Dobbelaere-Welvaert, unterstützt und vertreten durch RA Jan De Groote, in Dendermonde zugelassen.

Diese unter den Nummern 7907, 7929, 7930, 7931 und 7932 ins Geschäftsverzeichnis des Gerichtshofes eingetragenen Rechtssachen wurden verbunden.

Der Ministerrat, unterstützt und vertreten durch RA Evrard de Lophem, RA Sébastien Depré und RA Germain Haumont, in Brüssel zugelassen, hat Schriftsätze eingereicht (in allen Rechtssachen), die klagenden Parteien in den Rehtssachen Nrn. 7907, 7930 und 7931 haben Erwiderungsschriftsätze eingereicht, und der Ministerrat hat auch Gegenerwiderungsschriftsätze eingereicht (in den Rechtssachen Nrn. 7907, 7930 und 7931).

Durch Anordnung vom 28. Februar 2024 hat der Gerichtshof nach Anhörung der referierenden Richter Thierry Giet und Sabine de Bethune beschlossen, dass die Rechtssachen verhandlungsreif sind, dass keine Sitzung abgehalten wird, außer wenn eine Partei innerhalb von sieben Tagen nach Erhalt der Notifizierung dieser Anordnung einen Antrag auf Anhörung eingereicht hat, und dass vorbehaltlich eines solchen Antrags die Verhandlung nach Ablauf dieser Frist geschlossen und die Rechtssachen zur Beratung gestellt werden.

Infolge des Antrags der klagenden Partei in der Rechtssache Nr. 7907 auf Anhörung hat der Gerichtshof durch Anordnung vom 13. März 2024

- den Sitzungstermin auf den 10. April 2024 anberaumt,

- die Parteien aufgefordert, in einem spätestens am 5. April 2024 einzureichenden Ergänzungsschriftsatz, den sie in Kopie den jeweils anderen Parteien innerhalb derselben Frist zukommen lassen, ihre etwaigen Bemerkungen zu den Auswirkungen des Urteils des Europäischen Gerichtshofes für Menschenrechte *Podcasov gegen Russland* vom 13. Februar 2024 zu äußern.

Ergänzungsschriftsätze wurden eingereicht von

- der klagenden Partei in der Rechtssache Nr. 7907,

- der klagenden Partei in der Rechtssache Nr. 7930,

- den klagenden Parteien in der Rechtssache Nr. 7932,

- dem Ministerrat.

Auf der öffentlichen Sitzung vom 10. April 2024

- erschienen

. RA Jean-François Henrotte und RÄin Elisabeth Kiehl, ebenfalls *loco* RA Eric Lemmens, für die klagende Partei in der Rechtssache Nr. 7907,

. Jean Pierre Riquet, persönlich und für die VoG « Académie Fiscale » (klagende Parteien in der Rechtssache Nr. 7929),

. RA Raf Jespers, für die klagende Partei in der Rechtssache Nr. 7930,

. RÄin Catherine Forget, für die klagende Partei in der Rechtssache Nr. 7931,

. RA Jan De Groote, für die klagenden Parteien in der Rechtssache Nr. 7932,

. RA Evrard de Lophem, ebenfalls *loco* RA Sébastien Depré, und RA Germain Haumont, für den Ministerrat,

- haben die referierenden Richter Thierry Giet und Sabine de Bethune Bericht erstattet,

- wurden die vorgenannten Parteien angehört,

- wurden die Rechtssachen zur Beratung gestellt.

Durch Anordnung vom 15. Mai 2024 hat der Gerichtshof nach Anhörung der referierenden Richter Thierry Giet und Sabine de Bethune beschlossen,

- die Verhandlung wiederzueröffnen,

- die Parteien aufzufordern, in einem spätestens am 30. Mai 2024 einzureichenden Ergänzungsschriftsatz ihre Bemerkungen zu den Auswirkungen der Urteile des Gerichtshofes der Europäischen Union *La Quadrature du Net u.a.* (Personenbezogene Daten und Bekämpfung von Nachahmungen) (C-470/21) und *Procura della Repubblica presso il Tribunale di Bolzano* (C-178/22) vom 30. April 2024 auf die Behandlung der vorliegenden Klagen mitzuteilen und ihn innerhalb derselben Frist den anderen Parteien sowie der Kanzlei des Gerichtshofes per E-Mail an die Adresse « greffe@const-court.be » zu übermitteln,

- den neuen Sitzungstermin auf den 5. Juni 2024 anzuberaumen.

Ergänzungsschriftsätze wurden eingereicht von

- der klagenden Partei in der Rechtssache Nr. 7907,

- dem Ministerrat.

Auf der öffentlichen Sitzung vom 5. Juni 2024

- erschienen

. RA Alexandre Cassart ebenfalls *loco* RA Jean-François Henrotte, und RÄin Elisabeth Kiehl, ebenfalls *loco* RA Eric Lemmens, für die klagende Partei in der Rechtssache Nr. 7907,

. RA Raf Jespers, ebenfalls *loco* RÄin Catherine Forget, für die klagenden Parteien in den Rechtssachen Nrn. 7930 und 7931,

. RA Jan De Groote, für die klagenden Parteien in der Rechtssache Nr. 7932,

. RA Evrard de Lophem, ebenfalls *loco* RA Sébastien Depré, für den Ministerrat,

- haben die referierenden Richter Thierry Giet und Sabine de Bethune Bericht erstattet,

- wurden die vorgenannten Rechtsanwälte angehört,

- wurden die Rechtssachen zur Beratung gestellt.

Die Vorschriften des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof, die sich auf das Verfahren und den Sprachengebrauch beziehen, wurden zur Anwendung gebracht.

II. *Rechtliche Würdigung*

(…)

In Bezug auf das angefochtene Gesetz und dessen Kontext

B.1. Die Nichtigkeitsklagen beziehen sich auf das Gesetz vom 20. Juli 2022 « über die Sammlung und Speicherung von Identifizierungsdaten und Metadaten im Bereich der elektronischen Kommunikation und die Übermittlung dieser Daten an die Behörden » (nachstehend: Gesetz vom 20. Juli 2022).

Dieses Gesetz enthält Abänderungen des Gesetzes vom 13. Juni 2005 « über die elektronische Kommunikation » (nachstehend: Gesetz vom 13. Juni 2005) (Artikel 2 bis 17 des Gesetzes vom 20. Juli 2022), des Gesetzes vom 1. Juli 2011 « über die Sicherheit und den Schutz der kritischen Infrastrukturen » (nachstehend: Gesetz vom 1. Juli 2011) (Artikel 18 des Gesetzes vom 20. Juli 2022), des Gesetzes vom 17. Januar 2003 « über das Statut der Regulierungsinstanz des belgischen Post- und Telekommunikationssektors » (nachstehend: Gesetz vom 17. Januar 2003) (Artikel 19 bis 24 des Gesetzes vom 20. Juli 2022), des Strafprozessgesetzbuches (Artikel 25 bis 27 des Gesetzes vom 20. Juli 2022), des Gesetzes vom 5. August 1992 « über das Polizeiamt » (nachstehend: Gesetz vom 5. August 1992) (Artikel 28 des Gesetzes vom 20. Juli 2022), des Grundlagengesetzes vom 30. November 1998 « über die Nachrichten- und Sicherheitsdienste » (nachstehend: Gesetz vom 30. November 1998) (Artikel 29 bis 39 des Gesetzes vom 20. Juli 2022), des Gesetzes vom 2. August 2002 « über

die Aufsicht über den Finanzsektor und die Finanzdienstleistungen » (nachstehend: Gesetz vom 2. August 2002) (Artikel 40 und 41 des Gesetzes vom 20. Juli 2022), des Gesetzes vom 7. April 2019 « zur Festlegung eines Rahmens für die Sicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit » (nachstehend: Gesetz vom 7. April 2019) (Artikel 42 bis 43 des Gesetzes vom 20. Juli 2022) und des Gesetzes vom 24. Januar 1977 « über den Schutz der Gesundheit der Verbraucher im Bereich der Lebensmittel und anderer Waren » (Artikel 44 des Gesetzes vom 20. Juli 2022). Das Gesetz vom 20. Juli 2022 enthält ebenfalls mehrere « Übergangsbestimmungen » (Artikel 45 bis 48 des Gesetzes vom 20. Juli 2022).

B.2.1. Durch das Gesetz vom 20. Juli 2022 wollte der Gesetzgeber der Nichtigerklärung des Gesetzes vom 29. Mai 2016 « über die Sammlung und Aufbewahrung der Daten im Bereich der elektronischen Kommunikation » (nachstehend: Gesetz vom 29. Mai 2016) durch den Entscheid des Gerichtshofes Nr. 57/2021 vom 22. April 2021 (ECLI:BE:GHCC:2021:ARR.057) Rechnung tragen (*Parl. Dok.*, Kammer, 2021-2022, DOC 55-2572/001, S. 4). Dieser Entscheid ist nach mehreren Vorabentscheidungsfragen ergangen, die der Verfassungsgerichtshof dem Gerichtshof der Europäischen Union (nachstehend: Gerichtshof der Europäischen Union) gestellt hat (siehe Entscheid Nr. 96/2018 vom 19. Juli 2018, ECLI:BE:GHCC:2018:ARR.096), der mit einem Entscheid der Großen Kammer vom 6. Oktober 2020 in der Sache *La Quadrature du net u.a.* (C-511/18, C-512/18 und C-520/18, ECLI:EU:C:2020:791) geantwortet hat.

B.2.2. In den Vorarbeiten zum Gesetz vom 20. Juli 2022 heißt es diesbezüglich:

« À la suite de l'arrêt *La Quadrature du Net* rendu par la Cour de Justice [CJUE] le 6 octobre 2020 (affaires jointes C-511/18, C-512/18 et C-520/18), la Cour constitutionnelle belge a, par arrêt du 22 avril 2021, annulé les articles 2, *b)*, 3 à 11 et 14 de la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques. Cette loi est connue sous le nom de ' loi *data retention* '. Le présent projet vise essentiellement à réparer cette loi et à rétablir un cadre juridique conforme à la jurisprudence en matière de conservation des ' données de trafic et de localisation ' au sens de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive ' vie privée et communications électroniques ', aussi appelée ' directive *e-privacy* '). Cette directive sera remplacée par un règlement, qui utilise une nouvelle terminologie, à savoir ' métadonnées ' au lieu de ' données de trafic et de localisation '.

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

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

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

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

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

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

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

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

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

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

Par ailleurs, la vice-première ministre souligne que des garanties complémentaires ont également été ajoutées au niveau du traitement de ces données par les opérateurs (les mesures de sécurité imposées aux opérateurs sont plus détaillées), ainsi qu'au niveau de la fourniture de ces données aux autorités (encadrement plus strict des conditions entourant cette fourniture et

contrôle préalable de la demande de l'autorité envers l'opérateur). Les exigences de la jurisprudence ont ainsi été mises en œuvre.

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

L'arrêt d'annulation de la Cour constitutionnelle du 22 avril 2021 a également rendu nécessaire une modification de l'arrêté royal 19 septembre 2013 portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques (ci-après ' arrêté royal data '). En outre, l'arrêt d'annulation a également rendu nécessaire la modification de certaines lois organiques, notamment le Code d'instruction criminelle, ou la loi sur la fonction de police. Ce sont ces lois organiques qui fixent les conditions de fourniture des données conservées par les opérateurs aux différentes autorités concernées » (*Doc. parl.*, Chambre, 2021-2022, DOC 55-2572/003, SS. 3 bis 6).

B.2.3. Im vorerwähnten Entscheid Nr. 57/2021 hat der Gerichtshof geurteilt:

« B.18. Das Urteil des Gerichtshofes vom 6. Oktober 2020 verpflichtet zu einer Änderung der Perspektive hinsichtlich der Entscheidung des Gesetzgebers: Die Pflicht zur Speicherung von Daten über die elektronische Kommunikation muss die Ausnahme sein und nicht die Regel. Eine Regelung, die eine solche Pflicht vorsieht, muss zudem klaren und präzisen Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme unterliegen und Mindesterfordernisse aufstellen (Randnr. 133). Diese Regelung muss gewährleisten, dass sich der Eingriff auf das absolut Notwendige beschränkt und muss stets ' objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen ' (Randnrn. 132 und 133).

B.19. Es obliegt dem Gesetzgeber, eine Regelung auszuarbeiten, mit der die auf dem Gebiet des Schutzes personenbezogener Daten geltenden Grundsätze im Lichte der Rechtsprechung des Gerichtshofes der Europäischen Union eingehalten werden, und gegebenenfalls die von diesem angegebenen Präzisierungen in Bezug auf die verschiedenen Arten von Rechtsvorschriften, die als vereinbar mit Artikel 15 Absatz 1 der Richtlinie 2002/58/EG im Lichte der Artikel 7, 8, 11 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union betrachtet werden, zu berücksichtigen. Insbesondere obliegt es ebenfalls dem Gesetzgeber, in diesem Kontext die Unterscheidungen vorzunehmen, die zwischen den verschiedenen der Vorratsspeicherung unterliegenden Datenarten notwendig

sind, sodass gewährleistet ist, dass sich der Eingriff für jede Datenart auf das absolut Notwendige beschränkt ».

B.2.4. Mit diesem Entscheid hat der Gerichtshof entschieden, dass es dem Gesetzgeber obliegt, eine neue Regelung bezüglich der Pflicht zur Vorratsspeicherung von Daten über die elektronische Kommunikation unter Einhaltung der auf dem Gebiet geltenden Grundsätze auszuarbeiten, im Lichte der Rechtsprechung des Gerichtshofes der Europäischen Union in Bezug auf Artikel 15 Absatz 1 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 « über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) » (nachstehend: Richtlinie 2002/58/EG), gelesen wiederum im Lichte der Artikel 7, 8, 11 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union (nachstehend: Charta).

B.2.5. Artikel 15 Absatz 1 der Richtlinie 2002/58/EG lautet:

« Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 dieser Richtlinie beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG für die nationale Sicherheit, (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zweck können die Mitgliedstaaten unter anderem durch Rechtsvorschriften vorsehen, dass Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden. Alle in diesem Absatz genannten Maßnahmen müssen den allgemeinen Grundsätzen des Gemeinschaftsrechts einschließlich den in Artikel 6 Absätze 1 und 2 des Vertrags über die Europäische Union niedergelegten Grundsätzen entsprechen ».

B.2.6. Im Tenor des vorerwähnten Urteils vom 6. Oktober 2020 hat der Gerichtshof der Europäischen Union für Recht erkannt:

« 1. Art. 15 Abs. 1 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 geänderten Fassung ist im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union dahin auszulegen, dass er Rechtsvorschriften entgegensteht, die zu den in Art. 15 Abs. 1 genannten Zwecken präventiv eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten

vorsehen. Dagegen steht Art. 15 Abs. 1 der Richtlinie 2002/58 in der durch die Richtlinie 2009/136 geänderten Fassung im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta der Grundrechte Rechtsvorschriften nicht entgegen, die

- es zum Schutz der nationalen Sicherheit gestatten, den Betreibern elektronischer Kommunikationsdienste aufzugeben, Verkehrs- und Standortdaten allgemein und unterschiedslos auf Vorrat zu speichern, wenn sich der betreffende Mitgliedstaat einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit gegenübersieht, sofern diese Anordnung Gegenstand einer wirksamen, zur Prüfung des Vorliegens einer solchen Situation sowie der Beachtung der vorzusehenden Bedingungen und Garantien dienenden Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle sein kann, deren Entscheidung bindend ist, und sofern die Anordnung nur für einen auf das absolut Notwendige begrenzten, aber im Fall des Fortbestands der Bedrohung verlängerbaren Zeitraum ergeht;

- zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit auf der Grundlage objektiver und nicht diskriminierender Kriterien anhand von Kategorien betroffener Personen oder mittels eines geografischen Kriteriums für einen auf das absolut Notwendige begrenzten, aber verlängerbaren Zeitraum eine gezielte Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen;

- zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit für einen auf das absolut Notwendige begrenzten Zeitraum eine allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, vorsehen;

- zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zum Schutz der öffentlichen Sicherheit eine allgemeine und unterschiedslose Vorratsspeicherung der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten vorsehen;

- es zur Bekämpfung schwerer Kriminalität und, *a fortiori*, zum Schutz der nationalen Sicherheit gestatten, den Betreibern elektronischer Kommunikationsdienste mittels einer Entscheidung der zuständigen Behörde, die einer wirksamen gerichtlichen Kontrolle unterliegt, aufzugeben, während eines festgelegten Zeitraums die ihnen zur Verfügung stehenden Verkehrs- und Standortdaten umgehend zu sichern.

Diese Rechtsvorschriften müssen durch klare und präzise Regeln sicherstellen, dass bei der Speicherung der fraglichen Daten die für sie geltenden materiellen und prozeduralen Voraussetzungen eingehalten werden und dass die Betroffenen über wirksame Garantien zum Schutz vor Missbrauchsrisiken verfügen ».

B.3.1. Aus den Vorarbeiten zum Gesetz vom 20. Juli 2022 geht außerdem hervor, dass der Gesetzgeber ebenfalls der Nichtigerklärung des Gesetzes vom 1. September 2016 « zur Abänderung von Artikel 127 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation und von Artikel 16/2 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste » (nachstehend: Gesetz vom 1. September 2016) durch

den Entscheid des Gerichtshofes Nr. 158/2021 vom 18. November 2021 (ECLI:BE:GHCC:2021:ARR.158) Rechnung tragen wollte (*Parl. Dok.*, Kammer, 2021-2022, DOC 55-2572/003, S. 7).

B.3.2. In den Vorarbeiten zum Gesetz vom 20. Juli 2022 heißt es diesbezüglich:

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

Dans cet arrêt, la Cour ne remet pas en cause le principe de l'identification des utilisateurs de cartes prépayées, mais elle annule la modification apportée par la loi du 1er septembre 2016 à l'article 127 de la loi du 13 juin 2005, ' uniquement en ce qu'(elle) ne détermine pas les données d'identification qui sont collectées et traitées et les documents d'identification qui entrent en considération '. La Cour considère que l'article 22 de la Constitution exige que ces données et documents soient énumérés dans la loi. Elle maintient les effets de la disposition annulée jusqu'à l'entrée en vigueur d'une norme législative qui énumère ces données d'identification et ces documents d'identification et au plus tard jusqu'au 31 décembre 2022 inclus.

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

B.4. Aus den Vorarbeiten zum Gesetz vom 20. Juli 2022 geht hervor, dass der Gesetzgeber sowohl den vorerwähnten Entscheid Nr. 57/2021 als auch das Urteil des Gerichtshofes der Europäischen Union vom 6. Oktober 2020, auf dem er beruht, aber auch den vorerwähnten Entscheid Nr. 158/2021 gründlich geprüft hat.

In Bezug auf den Umfang der Nichtigkeitsklagen

B.5.1. Der Gerichtshof muss der Umfang der Nichtigkeitsklagen auf der Grundlage des Inhaltes der Klageschriften bestimmen.

Für nichtig erklären kann der Gerichtshof nur ausdrücklich angefochtene gesetzeskräftige Bestimmungen, gegen die Klagegründe angeführt werden, und gegebenenfalls Bestimmungen,

die zwar nicht angefochten werden, aber untrennbar mit den für nichtig zu erklärenden Bestimmungen verbunden sind.

B.5.2.1. Die klagende Partei in der Rechtssache Nr. 7907 beantragt die Nichtigerklärung der Artikel 5 Nrn. 4 und 6, 8 bis 11, 13 bis 15, 19, 21, 22, 24 bis 42 und 44 des Gesetzes vom 20. Juli 2022.

B.5.2.2. Die klagenden Parteien in der Rechtssache Nr. 7929 beantragen die Nichtigerklärung der Artikel 2 bis 17 des Gesetzes vom 20. Juli 2022.

B.5.2.3. Die klagenden Parteien in den Rechtssachen Nrn. 7930, 7931 und 7932 beantragen die Nichtigerklärung des gesamten Gesetzes vom 20. Juli 2022.

Die klagende Partei in der Rechtssache Nr. 7930 legt jedoch nur Klagegründe gegen die Artikel 5, 6, 8, 9, 11, 12, 13, 27 und 45 des Gesetzes vom 20. Juli 2022 dar. Sie beanstandet außerdem das Bestehen einer Gesetzeslücke in Bezug auf die vom Berufsgeheimnis abgedeckten Daten.

Im Übrigen ist der einzige Klagegrund der klagenden Partei in der Rechtssache Nr. 7931 nur gegen die Artikel 3, 5, 8, 9, 10, 11, 13, 24, 25, 26 und 27 des Gesetzes vom 20. Juli 2022 gerichtet.

Zudem legen die klagenden Parteien in der Rechtssache Nr. 7932 nur Klagegründe gegen die Artikel 3, 4, 5, 6, 8, 9, 10, 11, 12, 13, 15, 33, 34 und 37 des Gesetzes vom 20. Juli 2022 dar. Sie beanstanden ebenfalls das Bestehen einer Gesetzeslücke in Bezug auf die vom Berufsgeheimnis abgedeckten Daten.

B.6. Die Prüfung des Gerichtshofes bezieht sich also auf die Artikel 3 bis 6, 8 bis 15, 19, 21, 22, 24 bis 42 und 45 des Gesetzes vom 20. Juli 2022 sowie auf die vorerwähnte Gesetzeslücke.

In Bezug auf das Interesse

B.7.1. Der Ministerrat stellt das Interesse der Kammer der französischsprachigen und deutschsprachigen Rechtsanwaltschaften, klagende Partei in der Rechtssache Nr. 7907, an der Klageerhebung in Abrede.

Das Interesse der Kammer der französischsprachigen und deutschsprachigen Rechtsanwaltschaften wäre auf Artikel 27 Nr. 2 des Gesetzes vom 20. Juli 2022 beschränkt, da sich die gegen die anderen Bestimmungen gerichteten Beschwerdegründe nicht auf das Berufsgeheimnis des Rechtsanwalts beziehen würden.

B.7.2. Die Verfassung und das Sondergesetz vom 6. Januar 1989 über den Verfassungsgerichtshof erfordern, dass jede natürliche oder juristische Person, die eine Nichtigkeitsklage erhebt, ein Interesse nachweist. Das erforderliche Interesse liegt nur bei jenen Personen vor, deren Situation durch die angefochtene Rechtsnorm unmittelbar und ungünstig beeinflusst werden könnte; demzufolge ist die Popularklage nicht zulässig.

B.7.3. Artikel 495 Absätze 1 und 2 des Gerichtsgesetzbuches bestimmt:

« Die Kammer der französischsprachigen und deutschsprachigen Rechtsanwaltschaften und die Kammer der flämischen Rechtsanwaltschaften haben jede, was die Rechtsanwaltschaften betrifft, die ihnen angehören, als Auftrag, auf die Ehre, die Rechte und die gemeinsamen beruflichen Interessen ihrer Mitglieder zu achten, und sind zuständig für das, was den juristischen Beistand, das Praktikum, die berufliche Ausbildung der Rechtsanwaltspraktikanten und die Ausbildung aller Rechtsanwälte der Rechtsanwaltschaften, die ihnen angehören, betrifft.

Sie ergreifen die Initiativen und treffen die Maßnahmen, die in Sachen Ausbildung, Disziplinarvorschriften und berufliche Loyalität sowie für die Verteidigung der Interessen des Rechtsanwalts und des Rechtsuchenden nützlich sind ».

B.7.4. Die Kammern der Rechtsanwaltschaften sind Berufsvereinigungen des öffentlichen Rechts, die vom Gesetz eingerichtet wurden und in denen sich alle, die den Beruf des Rechtsanwalts ausüben, zusammenschließen müssen.

Die Kammern der Rechtsanwaltschaften können abgesehen von den Fällen, in denen sie ihr eigenes Interesse verteidigen, nur im Rahmen des Auftrags, den der Gesetzgeber ihnen

übertragen hat, vor Gericht auftreten. So können sie in erster Linie vor Gericht auftreten, wenn sie die beruflichen Interessen ihrer Mitglieder verteidigen oder wenn es um die Ausübung des Berufs des Rechtsanwalts geht. Nach Artikel 495 Absatz 2 des Gerichtsgesetzbuches können die Kammern ebenfalls die Initiativen ergreifen und die Maßnahmen treffen, die « für die Verteidigung der Interessen des Rechtsanwalts und des Rechtsuchenden nützlich sind ».

B.7.5. Aus Artikel 495 des Gerichtsgesetzbuches in Verbindung mit den Artikeln 2 und 87 des vorerwähnten Sondergesetzes vom 6. Januar 1989 ergibt sich, dass die Rechtsanwaltskammern nur zur Verteidigung des Kollektivinteresses der Rechtsuchenden als klagende oder intervenierende Partei vor dem Gerichtshof auftreten können, sofern dieses mit der Aufgabe und der Rolle des Rechtsanwalts bei der Verteidigung der Interessen des Rechtsuchenden zusammenhängt.

Maßnahmen ohne Auswirkungen auf das Recht auf Zugang zum Richter, die Rechtspflege oder den Beistand, den Rechtsanwälte ihren Mandaten gewähren können, ungeachtet dessen, ob dies im Rahmen eines administrativen Rechtsbehelfs, über eine gütliche Einigung oder einen Rechtsstreit, der den ordentlichen oder administrativen Rechtsprechungsorganen vorgelegt wird, geschieht, fallen daher nicht in den Anwendungsbereich von Artikel 495 des Gerichtsgesetzbuches in Verbindung mit den Artikeln 2 und 87 des vorerwähnten Sondergesetzes vom 6. Januar 1989.

B.7.6. Mit den angefochtenen Bestimmungen soll ein Rechtsrahmen im Bereich der Vorratsspeicherung und des Zugangs zu personenbezogenen Daten in Bereich der elektronischen Kommunikation nach der Nichtigerklärung des Gesetzes vom 1. September 2016 durch den vorerwähnten Entscheid des Gerichtshofes Nr. 57/2021 festgelegt werden.

Aus der Feststellung, dass sich die von der Kammer der französischsprachigen und deutschsprachigen Rechtsanwaltschaften angefochtenen Bestimmungen mit Ausnahme von Artikel 27 Nr. 2 des Gesetzes vom 20. Juli 2022 nicht ausdrücklich auf die elektronischen Kommunikationsmittel von Rechtsanwälten beziehen, kann nicht geschlossen werden, dass diese nicht auf sie anwendbar sind.

Das Gesetz vom 20. Juli 2022 hat eine allgemeine Tragweite und findet auf sämtliche elektronischen Kommunikationsmittel Anwendung, darunter diejenigen, die durch Artikel 458 des Strafgesetzbuches geschützt sind.

Die vertraulichen Informationen, die einem Rechtsanwalt bei der Ausübung seines Berufes anvertraut werden, genießen den Schutz, der sich für den Rechtsuchenden aus den Garantien ergibt, die in Artikel 6 der Europäischen Menschenrechtskonvention festgelegt sind, da die dem Rechtsanwalt auferlegte Regel des Berufsgeheimnisses ein fundamentales Element der Rechte der Verteidigung des Rechtsuchenden, der ihn ins Vertrauen zieht, ist (siehe insbesondere Entscheid Nr. 174/2018 vom 6. Dezember 2018, ECLI:BE:GHCC:2018:ARR.174, B.25).

B.7.7. Aus dem Vorstehenden ergibt sich, dass das Gesetz vom 20. Juli 2022 Maßnahmen vorsieht, die sich auf die Ausübung des Berufes des Rechtsanwalts auswirken können.

B.7.8. Die Einrede der Unzulässigkeit wird abgewiesen.

Zur Hauptsache

B.8.1. Artikel 6 des vorerwähnten Sondergesetzes vom 6. Januar 1989 präzisiert, dass die Klageschrift « den Gegenstand der Klage [angibt] und […] eine Darlegung des Sachverhalts und der Klagegründe [enthält] ».

B.8.2. Um den Erfordernissen nach Artikel 6 des vorerwähnten Sondergesetzes vom 6. Januar 1989 zu entsprechen, müssen die in der Klageschrift vorgebrachten Klagegründe angeben, welche Vorschriften, deren Einhaltung der Gerichtshof gewährleistet, verletzt wären und welche Bestimmungen gegen diese Vorschriften verstoßen würden, und darlegen, in welcher Hinsicht diese Vorschriften durch die fraglichen Bestimmungen verletzt würden.

Dieses Erfordernis ist nicht bloß formeller Art. Es zielt darauf ab, dem Gerichtshof sowie den Einrichtungen und Personen, die einen Schriftsatz an den Gerichtshof richten können, eine klare und eindeutige Darlegung der Klagegründe zu überreichen.

B.8.3. Die Klagegründe in den verbundenen Rechtssachen umfassen eine Vielzahl von Beschwerdegründen, die sich häufig wiederholen und mehrfach aufgeführt sind. Diese Klagegründe beziehen sich hauptsächlich auf die Vereinbarkeit der angefochtenen Bestimmungen mit dem Recht auf Achtung des Privatlebens und dem Recht auf Schutz personenbezogener Daten, die in Artikel 22 der Verfassung, in Artikel 8 der Europäischen Menschenrechtskonvention, in den Artikeln 7 und 8 der Charta und in mehreren Bestimmungen des Rechts der Europäischen Union gewährleistet sind. Andere Referenznormen werden ebenfalls geltend gemacht, jedoch ohne dass ihre Verletzung systematisch begründet wird. Der Gerichtshof beschränkt seine Prüfung gemäß den in B.8.2 erwähnten Anforderungen auf die Referenznormen, die Gegenstand der Darlegungen der Parteien sind.

B.8.4. Soweit die Klagegründe in den verbundenen Rechtssachen den vorstehenden Anforderungen genügen, prüft der Gerichtshof die Beschwerdegründe der klagenden Parteien in der folgenden Reihenfolge:

1. Die Verwendung der Kryptografie (Artikel 3);

2. die Maßnahmen, die auf der Ebene des Netzes oder des Endnutzers eingesetzt werden, um Betrug und böswillige Nutzungen der Netze und Dienste zu erkennen (Artikel 4);

3. die Vorratsspeicherung von Verkehrsdaten (Artikel 5);

4. die Vorratsspeicherung von Standortdaten (Artikel 6);

5. die Vorratsspeicherung von Abonnements- und Identifizierungsdaten (Artikel 8)*;*

6. die Pflicht zur Identifizierung von Teilnehmern und Endnutzern von elektronischen Kommunikationsdiensten (Artikel 12);

7. die gezielte Vorratsdatenspeicherung aufgrund eines geografischen Kriteriums (Artikel 9 bis 11);

8. die Aufzählung der zuständigen Behörden und der Zwecke im Rahmen des Zugangs zu den Daten (Artikel 13);

9. die Befugnisse der Gerichtspolizeioffiziere des BIPF (Artikel 24);

10. die Befugnisse des Prokurators des Königs (Artikel 25 und 26);

11. die Befugnisse des Untersuchungsrichters (Artikel 27);

12. die Befugnisse der Nachrichten- und Sicherheitsdienste (Artikel 33, 34 und 37);

13. das Inkrafttreten (Artikel 45);

14. der Schutz des Berufsgeheimnisses.

1. Die Verwendung der Kryptografie (Artikel 3)

B.9. Der einzige Klagegrund in der Rechtsache Nr. 7931 und der fünfte Klagegrund in der Rechtssache Nr. 7932 beziehen sich auf Artikel 3 des Gesetzes vom 20. Juli 2022, der Artikel 107/5 des Gesetzes vom 13. Juni 2005 wie folgt ersetzt:

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

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

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

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

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

B.10.1. In ihrem einzigen Klagegrund, abgeleitet aus einem Verstoß gegen die Artikel 11, 12, 22 und 29 der Verfassung, an sich oder in Verbindung mit den Artikeln 7, 8, 11, 47 und 52 Absatz 1 der Charta, mit Artikel 8 der Europäischen Menschenrechtskonvention, mit den Artikeln 5, 6 und 15 der Richtlinie 2002/58/EG und mit den Artikeln 13 und 14 der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 « zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates » (nachstehend: Richtlinie (EU) 2016/680), führt die klagende Partei in der Rechtssache Nr. 7931 an, dass Artikel 107/5 §§ 3 und 4 des Gesetzes vom 13. Juni 2005, eingefügt durch Artikel 3 des Gesetzes vom 20. Juli 2022, unverhältnismäßig sei, da die Verschlüsselungsmaßnahmen gerade ermöglichten, den Schutz personenbezogener Daten sicherzustellen und das Recht auf Achtung des Privatlebens zu schützen.

B.10.2. In ihrem fünften Klagegrund, abgeleitet aus einem Verstoß gegen die Artikel 10, 11, 15, 22 und 29 der Verfassung, an sich oder in Verbindung mit den Artikeln 5, 6, 8, 9, 10, 11, 14, 15, 17 und 18 der Europäischen Menschenrechtskonvention, mit den Artikeln 7, 8, 11, 47 und 52 der Charta, mit Artikel 5 Absatz 4 des Vertrags über die Europäische Union und mit der Richtlinie 2002/58/EG, der Richtlinie (EU) 2016/680 und der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 « zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) » (nachstehend: DSGVO), führen die klagenden Parteien in der Rechtssache Nr. 7932 an, dass Artikel 107/5 § 3 des Gesetzes vom 13. Juni 2005, eingefügt durch Artikel 3 des Gesetzes vom 20. Juli 2022, einen unverhältnismäßigen Eingriff in das Recht auf Achtung des Privatlebens darstelle und eine Maßnahme vorsehe, die in einer demokratischen Gesellschaft nicht notwendig sei.

B.11.1. Aus dem Vorstehenden geht hervor, dass die klagende Partei in der Rechtssache Nr. 7931 und die klagenden Parteien in de Rechtssache Nr. 7932 Beschwerdegründe gegen Artikel 107/5 des Gesetzes vom 13. Juni 2005, ersetzt durch Artikel 3 des Gesetzes vom 20. Juli 2022, nur in Bezug auf die Verletzung des Rechts auf Achtung des Privatlebens und des Rechts auf Schutz personenbezogener Daten anführen, die in Artikel 22 der Verfassung, in Artikel 8

der Europäischen Menschenrechtskonvention und in den Artikeln 7, 8 und 52 der Charta gewährleistet sind. Der Gerichtshof beschränkt seine Prüfung auf diese Bestimmungen.

B.11.2. Artikel 22 der Verfassung bestimmt:

« Jeder hat ein Recht auf Achtung vor seinem Privat- und Familienleben, außer in den Fällen und unter den Bedingungen, die durch Gesetz festgelegt sind.

Das Gesetz, das Dekret oder die in Artikel 134 erwähnte Regel gewährleistet den Schutz dieses Rechtes ».

Artikel 8 der Europäischen Menschenrechtskonvention bestimmt:

« (1) Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.

(2) Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer ».

Artikel 7 der Charta bestimmt:

« Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation ».

Artikel 8 der Charta bestimmt:

« (1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht ».

Artikel 52 Absatz 1 der Charta bestimmt:

« Jede Einschränkung der Ausübung der in dieser Charta anerkannten Rechte und Freiheiten muss gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten

achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie notwendig sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen ».

Artikel 52 Absatz 3 der Charta bestimmt:

« So weit diese Charta Rechte enthält, die den durch die Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten garantierten Rechten entsprechen, haben sie die gleiche Bedeutung und Tragweite, wie sie ihnen in der genannten Konvention verliehen wird. Diese Bestimmung steht dem nicht entgegen, dass das Recht der Union einen weiter gehenden Schutz gewährt ».

B.11.3. Der Verfassungsgeber hat eine möglichst weitgehende Übereinstimmung zwischen Artikel 22 der Verfassung und Artikel 8 der Europäischen Menschenrechtskonvention angestrebt (*Parl. Dok.*, Kammer, 1992-1993, Nr. 997/5, S. 2).

Die Tragweite dieses Artikels 8 entspricht derjenigen der vorerwähnten Verfassungsbestimmung, sodass die durch die beiden Bestimmungen gebotenen Garantien ein untrennbares Ganzes bilden.

Wenn die Charta Rechte enthält, die den durch die Europäische Menschenrechtskonvention garantierten Rechten entsprechen, « haben sie die gleiche Bedeutung und Tragweite, wie sie ihnen in der genannten Konvention verliehen wird ». Diese Bestimmung bringt die Bedeutung und Tragweite der in der Charta garantierten Rechte mit den entsprechenden durch die Europäische Menschenrechtskonvention garantierten Rechten in Einklang.

In den Erläuterungen zur Charta (2007/C-303/02), veröffentlicht im *Amtsblatt* vom 14. Dezember 2007, wird ausgeführt, dass unter den Artikeln mit « [derselben] Bedeutung und Tragweite wie die entsprechenden Artikel der Europäischen Menschenrechtskonvention » Artikel 7 der Charta Artikel 8 der Europäischen Menschenrechtskonvention entspricht.

Der Gerichtshof der Europäischen Union erinnert in diesem Zusammenhang daran, dass « Art. 7 der Charta, der das Recht auf Achtung des Privat- und Familienlebens betrifft, Rechte enthält, die den in Art. 8 Abs. 1 der am 4. November 1950 in Rom unterzeichneten Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (im Folgenden: EMRK) gewährleisteten Rechten entsprechen, und dass diesem Art. 7 gemäß

Art. 52 Abs. 3 der Charta somit die gleiche Bedeutung und Tragweite beizumessen ist wie Art. 8 Abs. 1 EMRK in seiner Auslegung durch die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte » (EuGH, 17. Dezember 2015, C-419/14, *WebMindLicenses Kft.*, ECLI:EU:C:2015:832, Randnr. 70; 14. Februar 2019, C-345/17, *Buivids*, ECLI:EU:C:2019:122, Randnr. 65).

In Bezug auf Artikel 8 der Charta ist der Gerichtshof der Auffassung, dass « wie aus Art. 52 Abs. 3 Satz 2 der Charta hervorgeht, Art. 52 Abs. 3 Satz 1 der Charta dem nicht [entgegensteht], dass das Recht der Union einen weiter gehenden Schutz gewährt als die EMRK », und dass « Art. 8 der Charta ein anderes als das in ihrem Art. 7 verankerte Grundrecht [betrifft], für das es in der EMRK keine Entsprechung gibt » (EuGH, Große Kammer, 21. Dezember 2016, C-203/15 und C-698/15, *Tele2 Sverige AB*, ECLI:EU:C:2016:970, Randnr. 129).

Aus dem Vorstehenden ergibt sich, dass innerhalb des Geltungsbereichs des Rechts der Europäischen Union Artikel 22 der Verfassung, Artikel 8 der Europäischen Menschenrechtskonvention und Artikel 7 der Charta analoge Grundrechte gewährleisten, genauso wie Artikel 8 der Charta, der einen spezifischen Rechtsschutz in Bezug auf personenbezogene Daten bietet.

B.12.1. Artikel 107/5 des Gesetzes vom 13. Juni 2005, eingefügt durch Artikel 3 des Gesetzes vom 20. Juli 2022, sieht vor, dass die Kryptgrafie frei verwendet werden kann, vorbehaltlich der drei Ausnahmen, die darin aufgezählt sind.

B.12.2. Die Vorarbeiten zu der angefochtenen Bestimmung zeigen, dass der Gesetzgeber die Verwendung der Kryptografie fördern wollte, da es sich um ein wirkungsvolles System handelt, um die Sicherheit der Kommunikation zu gewährleisten, was es ermöglicht, das Privatleben, das wissenschaftliche und wirtschaftliche Potenzial, die Wettbewerbsfähigkeit der Unternehmen, das Arztgeheimnis und das Geschäftsgeheimnis zu schützen (*Parl. Dok.*, Kammer, 2021-2022, DOC 55-2572/001, S. 17).

B.12.3. Artikel 107/5 des Gesetzes vom 13. Juni 2005, ersetzt durch Artikel 3 des Gesetzes vom 20. Juli 2022, legt die Ausnahmen von der freien Verwendung der Kryptografie fest, um es zu vermeiden, dass der Einsatz dieses Verfahrens die Notfallkommunikation,

darunter die Anzeige des rufenden Anschlusses oder die Bereitstellung der Identifizierungsdaten des Anrufers verhindert (§ 2), um es zu vermeiden, dass ein Betreiber ein gezieltes Ersuchen einer zuständigen Behörde mit dem Ziel, den Endnutzer zu identifizieren, der Öffentlichkeit nicht zugängliche Nachrichten zu erkennen und zu lokalisieren, nicht unter den gesetzlich vorgesehenen Bedingungen erledigen kann (§ 3), und um es zu vermeiden, dass ein ausländischer Betreiber, dessen Endnutzer oder Teilnehmer sich auf belgischem Staatsgebiet befindet, die Erledigung eines Ersuchens einer zuständigen Behörde verhindert, wobei in diesem letztgenannten Fall jede anders lautende Vertragsklausel nichtig ist (§ 4).

B.12.4. Wie in B.10.1 und B.10.2 erwähnt, beziehen sich die Beschwerdegründe der klagenden Parteien auf die beiden letzten Ausnahmen.

B.12.5. Mit diesen Ausnahmen soll es vermieden werden, dass der Einsatz der Kryptografie einen Betreiber daran hindert, seine Pflichten auf dem Gebiet der Vorratsdatenspeicherung, die vom Gesetz festgelegt sind, insbesondere im Fall eines Nutzers, der die Dienste eines ausländischen Betreibers in Anspruch nimmt, zu erfüllen (ebenda, SS. 19 bis 21). Dies sind legitime Ziele im Sinne von Artikel 8 der Europäischen Menschenrechtskonvention, von Artikel 52 Absatz 1 der Charta und von Artikel 15 Absatz 1 der Richtlinie 2002/58/EG, der durch das Gesetz vom 20. Juli 2022 umgesetzt wird.

B.13.1. Es geht sowohl aus dem vorerwähnten Entscheid des Gerichtshofes Nr. 57/2021 als auch aus dem vorerwähnten Urteil des Gerichtshofes der Europäischen Union in Sachen *La Quadrature du Net u.a.*, auf dem er beruht, hervor, dass Artikel 15 Absatz 1 der Richtlinie 2002/58/EG, gelesen im Lichte der Artikel 7, 8 und 52 Absatz 1 der Charta, der Vorratsspeicherung von Identifizierungsdaten, von Verkehrsdaten und von Standortdaten unter Einhaltung bestimmter Bedingungen nicht entgegensteht, insbesondere, dass die betreffenden Maßnahmen durch klare und präzise Regeln vorsehen, dass bei der Vorratsspeicherung der fraglichen Daten die für sie geltenden materiellen und prozeduralen Voraussetzungen erfüllt werden und dass die Betroffenen über wirksame Garantien zum Schutz vor Missbrauchsrisiken verfügen.

B.13.2. Bezüglich der Vorratsspeicherung von verschlüsselter Internet-Kommunikation und den Zugriff darauf hat der Europäische Gerichtshof für Menschenrechte im Urteil

Podchasov gegen Russland (EuGHMR, 13. Februar 2024, ECLI:CE:ECHR:2024:0213JUD003369619) erkannt:

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

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

65. La Cour rappelle enfin que la confidentialité des communications est un élément fondamental du droit au respect de la vie privée et de la correspondance, tel que garanti parl'article 8. Les utilisateurs de services de télécommunications et de services internet doivent se voir garantir le respect de leur vie privée et de leur liberté d'expression, même si cette garantie ne peut être absolue et doit parfois s'effacer devant d'autres impératifs légitimes, tels que la prévention des troubles à l'ordre public ou la lutte contre la criminalité, ou encore la protection des droits et des libertés d'autrui (voy. *K.U. c. Finlande*, n° 2872/02, § 49, CEDH 2008, et *Delfi AS c. Estonie* [GC], n° 64569/09, § 149, CEDH 2015) » (freie französische Übersetzung).

In diesem Urteil hat der Europäische Gerichtshof für Menschenrechte für Recht erkannt, dass die fraglichen russischen Rechtsvorschriften nicht in einem angemessenen Verhältnis zu den verfolgten legitimen Zielen, nämlich dem Schutz der nationalen Sicherheit, der Aufrechterhaltung der Ordnung und der Verbrechensverhütung sowie dem Schutz der Rechte

anderer, steht. In der vom Europäischen Gerichtshof für Menschenrechte vorgenommenen Abwägung wurde die Verpflichtung der Organisatoren der digitalen Kommunikation gemäß den russischen Rechtsvorschriften, alle gespeicherten Daten auf Ersuchen der zuständigen Behörden zu entschlüsseln, einschließlich der Inhalte von Ende-zu-Ende (end-to-end) verschlüsselten Verbindungen, aufgrund der Gefahr, dass dies den Verschlüsselungsmechanismus für alle Nutzer von digitalen Kommunikationsdiensten schwächt, als unverhältnismäßig angesehen (EuGHMR, 13. Februar 2024, *Podchasov gegen Russland*, vorerwähnt, §§ 68-80).

B.13.3. Im Unterschied zu den russischen Rechtsvorschriften, um die es im vorerwähnten Urteil *Podchasov gegen Russland* ging, fördert Artikel 107/5 §§ 3 und 4 des Gesetzes vom 13. Juni 2005 den Einsatz der Kryptografie (§ 1) und beschränkt sich darauf, Modalitäten für den Umfang der Befugnisse der Betreiber bezüglich der Nutzung dieser Kryptografie festzulegen, damit ein gezieltes Ersuchen einer zuständigen Behörde mit dem Ziel, den Endnutzer zu identifizieren und der Öffentlichkeit nicht zugängliche Nachrichten zu ermitteln und zu lokalisieren, in einem von einer anderen Gesetzesbestimmung vorgesehenen Fall und unter den von Artikel 15 Absatz 1 der Richtlinie 2002/58/EG vorgesehenen Bedingungen tatsächlich möglich ist.

Zudem sind die Daten, die auf Vorrat gespeichert werden müssen, um einem gezielten Ersuchen einer zuständigen Behörde nachkommen zu können, genau bestimmt und beziehen sich nicht auf den Inhalt der Nachricht. Es ist nicht ersichtlich, inwiefern die in Artikel 107/5 §§ 3 und 4 des Gesetzes vom 13. Juni 2005 erwähnten Bedingungen unverhältnismäßige Folgen für die Nutzer nach sich ziehen würden.

B.13.4. Insofern sie sich auf Artikel 3 des Gesetzes vom 20. Juli 2022 beziehen, sind der einzige Klagegrund in der Rechtssache Nr. 7931 und der fünfte Klagegrund in der Rechtssache Nr. 7932 unbegründet.

2. Die Maßnahmen, die auf der Ebene des Netzes oder des Endnutzers eingesetzt werden, um Betrug und böswillige Nutzungen der Netze und Dienste zu erkennen (Artikel 4)

B.14. Der sechste Klagegrund in der Rechtssache Nr. 7932 bezieht sich auf Artikel 4 des Gesetzes vom 20. Juli 2022, mit dem in das Gesetz vom 13. Juni 2005 ein Artikel 121/8 mit folgendem Wortlaut eingefügt wird:

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

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

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

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

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

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

B.15.1. Die klagenden Parteien führen an, dass Artikel 121/8 § 2 des Gesetzes vom 13. Juni 2005, eingefügt durch Artikel 4 des Gesetzes vom 20. Juli 2022, nicht mit den Artikeln 10, 11, 22 und 29 der Verfassung, an sich oder in Verbindung mit den Artikel 5, 6, 8, 9, 10, 11, 14, 15, 17 und 18 des Europäischen Menschenrechtskonvention, mit den Artikeln 7, 8, 11, 47 und 52 der Charta und mit der Richtlinie 2002/58/EG vereinbar sei. Ihrer Auffassung nach können Sperr- und Deaktivierungsmaßnahmen für weitergehende Zwecke als diejenigen, die in Artikel 121/8 § 1 des Gesetzes vom 13. Juni 2005 erwähnt sind, insbesondere zu Zensurzwecken, durchgeführt werden. Außerdem sei weder eine Bewertung durch ein unabhängiges Organ noch ein Bewertungskriterium festgelegt, um zu prüfen, ob diese Maßnahmen sich im Rahmen der von dem vorerwähnten Artikel 121/8 § 1 vorgesehenen Zwecke bewegen. Somit verstößt laut den klagenden Parteien Artikel 121/8 § 2 des Gesetzes vom 13. Juni 2005 gegen die Freiheit der Meinungsäußerung und der Information.

B.15.2. Aus dem Vorstehenden geht hervor, dass die klagenden Parteien Beschwerdegründe gegen Artikel 4 des Gesetzes vom 20. Juli 2022 in Bezug auf die Freiheit der Meinungsäußerung und der Information anführen.

B.15.3. Artikel 10 der Europäischen Menschenrechtskonvention bestimmt:

« (1) Jede Person hat das Recht auf freie Meinungsäußerung. Dieses Recht schließt die Meinungsfreiheit und die Freiheit ein, Informationen und Ideen ohne behördliche Eingriffe und ohne Rücksicht auf Staatsgrenzen zu empfangen und weiterzugeben. Dieser Artikel hindert die Staaten nicht, für Hörfunk-, Fernseh- oder Kinounternehmen eine Genehmigung vorzuschreiben.

(2) Die Ausübung dieser Freiheiten ist mit Pflichten und Verantwortung verbunden; sie kann daher Formvorschriften, Bedingungen, Einschränkungen oder Strafdrohungen unterworfen werden, die gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig sind für die nationale Sicherheit, die territoriale Unversehrtheit oder die öffentliche Sicherheit, zur Aufrechterhaltung der Ordnung oder zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral, zum Schutz des guten Rufes oder der Rechte anderer, zur Verhinderung der Verbreitung vertraulicher Informationen oder zur Wahrung der Autorität und der Unparteilichkeit der Rechtsprechung ».

Artikel 11 der Charta bestimmt:

« (1) Jede Person hat das Recht auf freie Meinungsäußerung. Dieses Recht schließt die Meinungsfreiheit und die Freiheit ein, Informationen und Ideen ohne behördliche Eingriffe und ohne Rücksicht auf Staatsgrenzen zu empfangen und weiterzugeben.

(2) Die Freiheit der Medien und ihre Pluralität werden geachtet ».

B.15.4. Insofern darin das Recht auf Freiheit der Meinungsäußerung anerkannt wird, haben Artikel 10 der Europäischen Menschenrechtskonvention und Artikel 11 Absatz 1 der Charta eine gleichartige Tragweite wie Artikel 19 der Verfassung, in dem die Freiheit anerkannt wird, zu allem seine Ansichten kundzutun.

Folglich bilden die durch diese Bestimmungen gewährten Garantien ein untrennbares Ganzes.

B.15.5. Artikel 19 der Verfassung bestimmt:

« Die Freiheit der Kulte, diejenige ihrer öffentlichen Ausübung sowie die Freiheit, zu allem seine Ansichten kundzutun, werden gewährleistet, unbeschadet der Ahndung der bei der Ausübung dieser Freiheiten begangenen Delikte ».

Artikel 19 der Verfassung verbietet es, dass der Freiheit der Meinungsäußerung präventive Einschränkungen auferlegt werden, jedoch nicht, dass Straftaten, die anlässlich der Inanspruchnahme dieser Freiheit begangen werden, bestraft werden.

B.15.6. Der Gerichtshof verbindet seine Prüfung von Artikel 19 der Verfassung nur mit Artikel 10 der Europäischen Menschenrechtskonvention und den Artikeln 11 und 52 der Charta, da der Verstoß gegen die anderen in B.15.1 genannten Bestimmungen in keiner Weise dargelegt wird.

B.16.1. Der Freiheit der Meinungsäußerung können aufgrund von Artikel 10 Absatz 2 der Europäischen Menschenrechtskonvention unter bestimmten Bedingungen Formalitäten, Bedingungen, Einschränkungen oder Sanktionen auferlegt werden, im Hinblick auf die nationale Sicherheit, die territoriale Unversehrtheit, die öffentliche Sicherheit, die Aufrechterhaltung der Ordnung und die Verbrechensverhütung, den Schutz der Gesundheit oder der Moral, den Schutz des guten Rufes und der Rechte anderer, um die Verbreitung von vertraulichen Informationen zu verhindern oder das Ansehen und die Unparteilichkeit der Rechtsprechung zu gewährleisten. Die Ausnahmen, mit denen sie einhergehen, sind jedoch « in engem Sinne auszulegen und die Notwendigkeit, sie einzuschränken, muss auf überzeugende Weise bewiesen werden » (EuGHMR, Große Kammer, 20. Oktober 2015, *Pentikäinen gegen Finnland*, ECLI:CE:ECHR:2015:1020JUD001188210, § 87).

B.16.2. Ein Eingriff in die Freiheit der Meinungsäußerung muss in einem ausreichend zugänglichen und genauen Gesetz geregelt sein. Der Eingriff muss folglich klar und ausreichend genau formuliert sein, sodass es möglich ist, dass jeder - notfalls nach passender Beratung - im gegebenen Kontext in angemessenem Maße die Folgen seines Handelns vorhersehen kann. Diese Anforderungen sollten gleichwohl nicht zu einer übertriebenen Rigidität führen, die verhindern würde, veränderte Umstände oder Anschauungen bei der Auslegung einer Gesetzesnorm zu berücksichtigen (EuGHMR, Große Kammer, 22. Oktober 2007, Lindon, *Otchakovsky-Laurens und July gegen Frankreich*, ECLI:CE:ECHR:2007:1022JUD002127902, § 41; Große Kammer, 7. Juni 2012, *Centro Europa 7 S.R.L. und Di Stefano gegen Italien*, ECLI:CE:ECHR:2012:0607JUD003843309,

§§ 141-142; Große Kammer, 15. Oktober 2015, *Perinçek gegen Schweiz*, ECLI:CE:ECHR:2015:1015JUD002751008, §§ 131-133). Ferner muss der Nachweis erbracht werden, dass diese Einschränkung in einer demokratischen Gesellschaft notwendig ist, einem zwingenden gesellschaftlichen Bedürfnis entspricht und im Verhältnis zu den legitimen Zielen steht, die damit verfolgt werden.

B.17. Aus den Vorarbeiten geht hervor, dass der Gesetzgeber mit Artikel 121/8 § 2 des Gesetzes vom 13. Juni 2005, eingefügt durch Artikel 4 des Gesetzes vom 20. Juli 2022, der Situation begegnen wollte, in der ein Endnutzer des Kommunikationsnetzes Opfer eines Betrugs ist, indem er die Betreiber dazu bewegt, zugunsten dieses Nutzers zu reagieren, und indem er vorsieht, dass in schwerwiegenden Fällen von Betrug oder böswilliger Nutzung des Netzes schnelle und « wirkungsvolle Maßnahmen » ergriffen werden können. In diesem Rahmen hat die Aufzählung der in diesem Artikel erwähnten Sperr- und Deaktivierungsmaßnahmen auch das Ziel, den Betreibern eine größere Rechtssicherheit zu bieten (*Parl. Dok.*, Kammer, 2021-2022, DOC 55-2572/001, SS. 21-22).

Diese Ziele sind legitim und können eine Einschränkung der Freiheit der Meinungsäußerung begründen. Es ist ferner zu prüfen, ob die angefochtene Maßnahme sachdienlich und im Hinblick auf diese Ziele verhältnismäßig ist.

B.18. Um schwerwiegende Fällen von Betrug und böswilliger Nutzung des Netzes zum Nachteil des Endnutzers zu verhindern, konnte der Gesetzgeber die Möglichkeit vorsehen, die in Artikel 121/8 § 2 erwähnten Maßnahmen zu ergreifen, da diese geeignet sind, die vorerwähnten Ziele zu erreichen. Im Übrigen weisen die klagenden Parteien nicht nach, inwiefern diese Maßnahmen im Hinblick auf diese Ziele nicht sachdienlich sind.

B.19.1. Schließlich gehen die in Artikel 121/8 § 2 des Gesetzes vom 13. Juni 2005 erwähnten Maßnahmen nicht über das hinaus, was zur Erreichung der vom Gesetzgeber verfolgten Ziele notwendig ist.

B.19.2. Zunächst sind die Begriffe « Betrug » und « böswillige Nutzung des Netzes oder des Dienstes » in Artikel 2 Nrn. 5/5 und 5/6 des Gesetzes vom 13. Juni 2005, abgeändert durch Artikel 2 des Gesetzes vom 20. Juli 2022, definiert. Gemäß diesen Bestimmungen verweist Betrug auf « eine unredliche Handlung unter Verstoß gegen das Gesetz, Verordnungen oder

gegen den Vertrag in der Absicht zu täuschen und sich selbst oder einem anderen einen unrechtmäßigen Vorteil zum Nachteil des Betreibers oder des Endnutzers zu verschaffen, die über die Nutzung eines elektronischen Kommunikationsdienstes begangen wird » (Nr. 5/5), während die böswillige Nutzung des Netzes oder des Dienstes in einer « Nutzung des Netzes oder des elektronischen Kommunikationsdienstes, um seinen Austauschpartner zu belästigen oder Schäden zu verursachen » (Nr. 5/6) besteht.

B.19.3. Es obliegt den Betreibern, das Vorliegen eines Betrugs oder einer böswilligen Nutzung des Netzes oder des Dienstes zu prüfen und im Einzelfall die « Schwere der Umstände » zu beurteilen, bevor die von Artikel 121/8 § 2 des Gesetzes vom 13. Juni 2005, eingefügt durch Artikel 4 des Gesetzes vom 20. Juli 2022, vorgesehenen Maßnahmen ergriffen werden können. Aus den Vorarbeiten zu der angefochtenen Bestimmung geht hervor, dass in diesem Fall die Betreiber auf eigene Initiative oder nach der Meldung eines Endnutzers oder eines Dritten tätig werden; in jedem Fall ist es den Betreibern untersagt, vom Inhalt der Nachrichten Kenntnis zu nehmen (*Parl. Dok.*, Kammer, 2021-2022, DOC 55-2572/003, SS. 85 bis 87).

In diesem Rahmen handeln die Betreiber unter der Aufsicht des Belgischen Instituts für Post- und Fernmeldewesen (nachstehend: BIPF), das aufgrund von Artikel 14 § 1 Nr. 3 Buchstabe *a)* des Gesetzes vom 17. Januar 2003 mit der Kontrolle der Einhaltung des Gesetzes vom 13. Juni 2005 und seiner Ausführungserlasse betraut ist. Artikel 121/8 des Gesetzes vom 13. Juni 2005 fügt hinzu, dass das BIPF « befugt [ist], verbindliche Anweisungen zu erteilen, auch Anweisungen zu den Ausführungsfristen » (§ 1 Absatz 3), in Bezug auf die von den Betreibern auf der Grundlage dieser Bestimmung ergriffenen Maßnahmen.

Bei der Aufsicht, die es über die von den Betreibern auf der Grundlage von Artikel 121/8 § 2 des Gesetzes vom 13. Juni 2005 ergriffenen Maßnahmen ausübt, prüft das BIPF insbesondere das Vorliegen eines Betrugs oder einer böswilligen Nutzung des Netzes, die Angemessenheit und Verhältnismäßigkeit der Maßnahme sowie die Schwere der Umstände des Falles.

Schließlich kann aufgrund von Artikel 2 § 1 des Gesetzes vom 17. Januar 2003 « über Beschwerden und die Behandlung von Streitsachen in Zusammenhang mit dem Gesetz vom 17. Januar 2003 über das Statut der Regulierungsinstanz des belgischen Post- und

Telekommunikationssektors » gegen die Entscheidungen des BIPF « eine Beschwerde im Verfahren mit unbeschränkter Rechtsprechung beim Märktegerichtshof, der wie im Eilverfahren urteilt, erhoben werden », wobei « jede Person, die ein Interesse an der Erhebung der Beschwerde hat, die Beschwerde einreichen kann ».

B.20. Der sechste Klagegrund in der Rechtssache Nr. 7932 ist unbegründet.

3. Die Vorratsspeicherung von Verkehrsdaten (*Artikel 5)*

B.21.1. Der erste und der zweite Klagegrund in der Rechtssache Nr. 7930, der einzige Klagegrund in der Rechtssache Nr. 7931 und der erste Teil des ersten Klagegrunds und der erste Teil des dritten Klagegrunds in der Rechtssache Nr. 7932 beziehen sich auf Artikel 5 des Gesetzes vom 20. Juli 2022, der bestimmt:

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

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

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

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

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

b) dans l'alinéa 2, les mots ' de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel ' sont remplacés par les mots ' du RGPD et de la loi du 30 juillet 2018 ';

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

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

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

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

c) dans l'alinéa 2, les mots ' de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel ' sont remplacés par les mots ' du RGPD et de la loi du 30 juillet 2018 ';

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

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

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

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

- l'identifiant de la destination de la communication;

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

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

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

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

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

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

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

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

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

Par dérogation au paragraphe 1er, de manière à pouvoir prendre les mesures appropriées visées à l'article 121/8, § 1er, de permettre d'établir la fraude ou l'utilisation malveillante du

réseau ou du service ou d'identifier son auteur et son origine, l'opérateur peut conserver et traiter d'autres données que celles visées à l'alinéa 1er considérées nécessaires à ces fins.

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

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

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

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

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

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

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

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

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

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

' § 5. Les données énumérées dans le présent article ne peuvent être traitées que par les personnes chargées par l'opérateur de la facturation ou de la gestion du trafic, du traitement des demandes de renseignements des abonnés, de la lutte contre les fraudes ou l'utilisation malveillante du réseau, de la sécurité du réseau, du respect de ses obligations légales, du marketing des services de communications électroniques propres ou de la fourniture de services qui font usage de données de trafic ou de localisation et par les membres de sa Cellule de coordination visée à l'article 127/3. ';

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

B.21.2. Infolge dieser Abänderung bestimmt Artikel 122 des Gesetzes vom 13. Juni 2005:

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

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

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

1° des types de données de trafic traitées;

2° des objectifs précis du traitement;

3° de la durée du traitement.

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

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

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

a) des types de données de trafic traitées;

b) des objectifs précis du traitement;

c) de la durée du traitement.

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

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

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

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

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

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

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

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

- l'identifiant de la destination de la communication;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§ 5. Les données énumérées dans le présent article ne peuvent être traitées que par les personnes chargées par l'opérateur de la facturation ou de la gestion du trafic, du traitement des demandes de renseignements des abonnés, de la lutte contre les fraudes ou l'utilisation malveillante du réseau, de la sécurité du réseau, du respect de ses obligations légales, du marketing des services de communications électroniques propres ou de la fourniture de services qui font usage de données de trafic ou de localisation et par les membres de sa Cellule de coordination visée à l'article 127/3.

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

B.22.1. Die klagende Partei in der Rechtssache Nr. 7930 leitet einen ersten und einen zweiten Klagegrund ab aus einem Verstoß gegen die Artikel 11, 12, 22 und 29 der Verfassung, gegen Artikel 15 Absatz 1 und gegen die Artikel 5, 6 und 9 der Richtlinie 2002/58/EG, gelesen im Lichte der Artikel 7, 8, 11, 47 und 52 Absatz 1 der Charta, der Artikel 6, 8, 10, 11 und 18 der Europäischen Menschenrechtskonvention und der Artikel 13 und 54 der Richtlinie (EU) 2016/680, insofern Artikel 5 Nrn. 4 und 5 des Gesetzes vom 20. Juli 2022 eine allgemeine Vorratsspeicherungspflicht für Kommunikationsdaten einführe, ohne dass diese Vorratsspeicherung notwendig und im Hinblick auf das verfolgte Ziel strikt begrenzt sei. Die klagende Partei führt nicht ausdrücklich einen Beschwerdegrund gegen Artikel 5 Nrn. 1 bis 3 und Nrn. 6 bis 8 an.

B.22.2. Die klagende Partei in der Rechtssache Nr. 7931 leitet einen einzigen Klagegrund ab aus einem Verstoß gegen die Artikel 11, 12, 22 und 29 der Verfassung, an sich oder in Verbindung mit den Artikeln 7, 8, 11, 47 und 52 Absatz 1 der Charta, mit Artikel 8 der Europäischen Menschenrechtskonvention, mit den Artikeln 5, 6 und 15 der Richtlinie 2002/58/EG und mit den Artikeln 13 und 54 der Richtlinie (EU) 2016/680. Sie führt an, dass Artikel 5 Nr. 4 des Gesetzes vom 20. Juli 2022 eine Pflicht zur systematischen und unterschiedslosen Vorratsspeicherung bestimmter Daten vorsehe, um die Kriminalität allgemein zu bekämpfen, obgleich eine solche Vorratsspeicherung nur im Rahmen der Bekämpfung der schweren Kriminalität zulässig sei, und insofern die darin festgelegte Vorratsspeicherungspflicht in jedem Fall unverhältnismäßig sei.

Hilfsweise beantragt die klagende Partei, dem Gerichtshof der Europäischen Union eine Vorabentscheidungsfrage zu stellen. Außerdem ist nach Auffassung der klagenden Partei Artikel 5 Nr. 5 des Gesetzes vom 20. Juli 2022 angesichts der anderen Pflichten, die den Betreibern obliegen, nicht notwendig und sieht eine zu lange Speicherfrist vor.

B.22.3. Die klagenden Parteien in der Rechtssache Nr. 7932 leiten einen ersten Klagegrund ab aus einem Verstoß gegen die Artikel 10, 11, 13, 15, 22, 23 und 29 der Verfassung, an sich oder in Verbindung mit den Artikeln 5, 6, 8, 9, 10, 11, 14 und 18 der Europäischen Menschenrechtskonvention, mit den Artikeln 7, 8, 11, 47 und 52 der Charta, mit Artikel 5 Absatz 4 des Vertrags über die Europäische Union und mit Artikel 6 der Richtlinie 2002/58/EG, mit der Richtlinie (EU) 2016/680 und mit der DSGVO. Im ersten Teil dieses Klagegrunds führen die klagenden Parteien an, dass Artikel 5 Nrn. 4 und 5 des Gesetzes vom

20. Juli 2022 eine allgemeine und unterschiedslose Vorratsdatenspeicherung vorsehe, die nur im Rahmen des Schutzes der nationalen Sicherheit zulässig sei, ohne dass vorgesehen sei, dass die gespeicherten Daten gelöscht oder anonymisiert würden, wenn die Speicherung nicht mehr notwendig sei. Außerdem sehe Artikel 5 des Gesetzes vom 20. Juli 2022 eine Gleichbehandlung sämtlicher Daten vor, ohne eine Unterscheidung nach dem Zweck (Bekämpfung der schweren Kriminalität) vorzunehmen.

Dieselben klagenden Parteien leiten einen dritten Klagegrund ab aus einem Verstoß gegen die Artikel 10, 11, 15, 22 und 29 der Verfassung, an sich oder in Verbindung mit den Artikeln 5, 6, 8, 9, 10, 11, 14 und 18 der Europäischen Menschenrechtskonvention, mit den Artikeln 7, 8, 11, 47 und 52 der Charta, mit Artikel 5 Absatz 4 des Vertrags über die Europäische Union, sowie mit der Richtlinie 2002/58/EG, mit der Richtlinie (EU) 2016/680 und mit der DSGVO. Im ersten Teil dieses Klagegrunds behaupten sie, dass Artikel 5 Nr. 4 des Gesetzes vom 20. Juli 2022 eine Pflicht zu einer allgemeinen und unterschiedslosen Vorratsdatenspeicherung schaffe, um Betrug und böswillige Nutzungen des Netzes oder des Dienstes zu bekämpfen, und zwar für die Betreiber im Rahmen ihrer Aufträge, was zu vage und zu weit gefasst sei.

B.23. Aus dem Vorstehenden geht hervor, dass sich die Beschwerdegründe der klagenden Parteien auf Artikel 5 Nrn. 4 und 5 des Gesetzes vom 20. Juli 2022 beziehen. Außerdem sind diese Beschwerdegründe hauptsächlich abgeleitet aus einem Verstoß gegen das Recht auf Achtung des Privatlebens und das Recht auf Schutz personenbezogener Daten, die in Artikel 22 der Verfassung, in Artikel 8 der Europäischen Menschenrechtskonvention, in den Artikeln 7, 8 und 52 Absatz 1 der Charta, in der Richtlinie 2002/58/EG, in der Richtlinie (EU) 2016/680 und in der DSGVO gewährleistet sind.

B.24.1. Artikel 22 der Verfassung behält dem zuständigen Gesetzgeber die Befugnis vor, festzulegen, in welchen Fällen und unter welchen Bedingungen das Recht auf Achtung des Privatlebens beeinträchtigt werden kann. Somit garantiert er jedem Bürger, dass eine Einmischung in die Ausübung dieses Rechts nur aufgrund von Regeln erfolgen darf, die durch eine demokratisch gewählte beratende Versammlung angenommen wurden.

Eine Ermächtigung einer anderen Gewalt steht jedoch nicht im Widerspruch zum Legalitätsprinzip, sofern die Ermächtigung ausreichend präzise beschrieben ist und sich auf die

Ausführung von Maßnahmen bezieht, deren wesentliche Elemente vorher durch den Gesetzgeber festgelegt wurden.

Folglich müssen die wesentlichen Elemente der Verarbeitung personenbezogener Daten im Gesetz, im Dekret oder in der Ordonnanz selbst festgelegt sein. Diesbezüglich sind die wesentlichen Elemente unabhängig von dem betroffenen Bereich grundsätzlich die folgenden Elemente: (1) die Kategorie der verarbeiteten Daten, (2) die betroffene Personenkategorie, (3) der mit der Verarbeitung verfolgte Zweck, (4) die Kategorie der Personen, die Zugriff auf die verarbeiteten Daten haben, und (5) die maximale Dauer der Aufbewahrung der Daten.

B.24.2. Neben dem formalen Erfordernis der Legalität wird durch Artikel 22 der Verfassung in Verbindung mit Artikel 8 der Europäischen Menschenrechtskonvention und mit den Artikeln 7, 8 und 52 der Charta ebenfalls die Verpflichtung auferlegt, dass die Einmischung in die Ausübung des Rechts auf Achtung des Privatlebens und des Rechts auf den Schutz personenbezogener Daten deutlich und ausreichend präzise formuliert wird, damit es möglich ist, die Fälle vorherzusehen, in denen der Gesetzgeber eine solche Einmischung erlaubt.

Auf dem Gebiet des Schutzes personenbezogener Daten bedeutet dieses Erfordernis der Vorhersehbarkeit, dass ausreichend präzise vorgesehen werden muss, unter welchen Umständen Verarbeitungen von personenbezogenen Daten erlaubt sind (EuGHMR, Große Kammer, 4. Mai 2000, *Rotaru gegen Rumänien*, ECLI:CE:ECHR:2000:0504JUD002834195, § 57; Große Kammer, 4. Dezember 2008, *S. und Marper gegen Vereinigtes Königreich*, ECLI:CE:ECHR:2008:1204JUD003056204, § 99). Das Erfordernis, dass die Einschränkung gesetzlich vorgesehen sein muss, bedeutet insbesondere, dass die gesetzliche Grundlage für den Eingriff in diese Rechte den Umfang, in dem die Ausübung des betreffenden Rechts eingeschränkt wird, selbst festlegen muss (EuGH, 6. Oktober 2020, C-623/17, *Privacy International*, ECLI:EU:C:2020:790, Randnr. 65).

Deshalb muss es jeder Person möglich sein, sich ein ausreichend klares Bild von den verarbeiteten Daten, den an einer bestimmten Datenverarbeitung beteiligten Personen sowie den Bedingungen und den Zwecken der Verarbeitung zu machen.

B.25. Aus den Vorarbeiten zu Artikel 5 Nrn. 4 und 5 des Gesetzes vom 20. Juli 2022 geht hervor, dass dieser insbesondere bezweckt, Artikel 15 der Richtlinie 2002/58/EG umzusetzen,

insofern dieser Artikel 15 von Artikel 6 Absatz 5 dieser Richtlinie abweicht und es den Mitgliedstaaten erlaubt, Maßnahmen zu ergreifen, um die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen sicherzustellen (*Parl. Dok.*, Kammer, 2021-2022, DOC 55-2572/001, SS. 28, 29, 36 und 37).

Diese Ziele sind legitim im Sinne von Artikel 8 der Europäischen Menschenrechtskonvention und von Artikel 52 der Charta.

In diesem Rahmen hat der Gesetzgeber präzisiert, dass es wegen der Struktur der betroffenen Netze und Dienste selbst nicht möglich ist, eine « von Anfang an reaktive und gezielte » Datenspeicherung vorzusehen (ebenda, SS. 27-28). Er hat zudem die Auffassung vertreten, dass das von Artikel 5 Nrn. 4 und 5 des Gesetzes vom 20. Juli 2022 vorgesehene System zur Vorratsspeicherung von Verkehrsdaten « im Interesse der Endnutzer der Dienste des Betreibers » ist (ebenda, S. 26) und bezweckt, es den Opfern eines Betrugs oder einer böswilligen Nutzung des Netzes zu ermöglichen, deren Urheber zu identifizieren (ebenda, S. 28). Überdies wird dieses System so dargestellt, dass es « von seiner Beschaffenheit eng mit der Bereitstellung des elektronischen Kommunikationsdienstes zusammenhängt » (ebenda, S. 26) und es ermöglicht, das Gesetz vom 13. Juni 2005 in Anbetracht der zunehmenden Bedeutung des Ziels der Bekämpfung von Betrug und böswilliger Nutzung des Netzes im Recht der Europäischen Union zu modernisieren (ebenda, S. 29).

B.26. Der Gerichtshof hat zu prüfen, ob die von Artikel 122 §§ 4 und 4/1 des Gesetzes vom 13. Juni 2005, eingefügt durch Artikel 5 Nrn. 4 und 5 des Gesetzes vom 20. Juli 2022, herbeigeführte Einmischung in das Recht auf Achtung des Privatlebens und in das Recht auf Schutz personenbezogener Daten nicht für die Personen, die Gegenstand der von dieser Bestimmung erwähnten Maßnahmen sind, unverhältnismäßige Folgen hat.

B.27.1. Artikel 122 § 4 des Gesetzes vom 13. Juni 2005 sieht zulasten der Betreiber eine Pflicht zur Vorratsspeicherung mehrerer Verkehrsdaten im Hinblick darauf vor, « die in Artikel 121/8 § 1 erwähnten angemessenen Maßnahmen zu ergreifen, Betrug oder böswilligen Nutzungen des Netzes oder des Dienstes feststellen zu können oder ihren Urheber und ihren Ursprung zu identifizieren », sofern die Betreiber diese Daten « im Rahmen der Bereitstellung dieses Netzes oder dieses Dienstes » verarbeiten.

B.27.2. Die erwähnten Verkehrsdaten sind « die Kennung des Ursprungs der Kommunikation », « die Kennung des Ziels der Kommunikation », « die genauen Tage und Uhrzeiten des Beginns und des Endes der Kommunikation » und « der Standort der Endgeräte der Beteiligten an der Kommunikation zu Beginn und am Ende der Kommunikation » (Absatz 1 Nr. 1). Es ist auch vorgesehen, dass die Betreiber mehrere Verkehrsdaten über die eingehenden Kommunikationen auf Vorrat speichern, um den Urheber der Kommunikation, das heißt « die Telefonnummern, von der die eingehende Kommunikation ausgeht », « die IP-Adresse, die zum Versand der eingehenden Kommunikation gedient hat, die Zeitstempelung und den verwendeten Port » sowie « die genauen Tage und Uhrzeiten des Beginns und des Endes der eingehenden Kommunikation », zu identifizieren (Absatz 1 Nr. 2).

Aufgrund von Artikel 122 § 4 Absatz 1 Nr. 5 des Gesetzes vom 13. Juni 2005 verarbeiten die Betreiber die verschiedenen erwähnten Daten im Hinblick auf die vorerwähnten Zwecke.

B.27.3. Die Liste der Verkehrsdaten, die in Artikel 122 § 4 Absatz 1 des Gesetzes vom 13. Juni 2005 aufgezählt sind, ist nicht abschließend.

Zunächst heißt es in Artikel 122 § 4 Absatz 2, dass der Betreiber, « um die in Artikel 121/8 § 1 erwähnten angemessenen Maßnahmen ergreifen zu können, um Betrug oder böswilligen Nutzungen des Netzes oder des Dienstes feststellen zu können oder um ihren Urheber und ihren Ursprung zu identifizieren », andere als die in Absatz 1 erwähnten Daten, die für diesen Zweck als notwendig erachtet werden, auf Vorrat speichern und verarbeiten [kann] ». Diese den Betreibern eingeräumte Befugnis, andere als die in Artikel 122 § 4 Absatz 1 erwähnten Daten auf Vorrat zu speichern und zu verarbeiten, unterliegt nicht einer vorherigen Stellungnahme des BIPF und der Datenschutzbehörde oder einer Notifizierung an diese Behörden. In den Vorarbeiten zu der angefochtenen Bestimmung ist keine Rechtfertigung für diese Befugnis enthalten (*Parl. Dok.*, Kammer, 2021-2022, DOC 55-2572/003, SS. 87-92).

Sodann sieht Artikel 122 § 4 Absatz 3 vor, dass « der König […] die Verkehrsdaten, deren Vorratsspeicherung für die Verfolgung der im vorliegenden Paragraphen vorgesehenen Zwecke als notwendig angesehen werden muss, durch einen im Ministerrat beratenen Erlass und nach Stellungnahme des BIPF und der Datenschutzbehörde präzisieren und erweitern [kann] ». In den Vorarbeiten zu der angefochtenen Bestimmung wird diese Ermächtigung damit

gerechtfertigt, dass sich die Betrugsfälle mit der Zeit erheblich ändern und dass sich die auf Vorrat gespeicherten Daten je nach Art des elektronischen Kommunikationsdienstes, der Größe des Betreibers, der Werkzeuge, über die dieser verfügt, und den Nutzern des Dienstes unterscheiden können (*Parl. Dok.*, Kammer, 2021-2022, DOC 55-2572/001, S. 35).

B.27.4. Die in Artikel 122 § 4 Absatz 1 Nr. 1 des Gesetzes vom 13. Juni 2005 erwähnten Verkehrsdaten werden grundsätzlich vier Monate auf Vorrat gespeichert. Die in Artikel 122 § 4 Absatz 1 Nr. 2 erwähnten Verkehrsdaten werden grundsätzlich zwölf Monate auf Vorrat gespeichert.

B.27.5. Diese Speicherfristen für die Daten können verlängert werden. Artikel 122 § 4 Absatz 1 Nr. 3 des Gesetzes vom 13. Juni 2005 bestimmt, dass die in Nr. 1 erwähnten Daten, die sich auf einen spezifischen Betrugsfall oder eine spezifische böswillige Nutzung des Netzes beziehen, « die für deren Analyse und Lösung notwendige Zeit, gegebenenfalls über die in Nr. 1 erwähnte Frist von vier Monaten hinaus » auf Vorrat gespeichert werden dürfen. Artikel 122 § 4 Nr. 4 präzisiert, dass die in Nr. 2 erwähnten Daten, die sich auf eine spezifische böswillige Nutzung des Netzes beziehen, « die für deren Bearbeitung notwendige Zeit, gegebenenfalls über die in Nr. 2 erwähnte Frist von zwölf Monaten hinaus » auf Vorrat gespeichert werden dürfen.

B.28.1. Artikel 122 § 4/1 des Gesetzes vom 13. Juni 2005 sieht wiederum zulasten der Betreiber die Möglichkeit vor, die Verkehrsdaten auf Vorrat zu speichern und zu verarbeiten, « die notwendig sind, um die Sicherheit und das ordnungsgemäße Funktionieren ihrer Netze und elektronischen Kommunikationsdienste sicherzustellen und insbesondere um eine potenzielle oder tatsächliche Beeinträchtigung dieser Sicherheit zu erkennen und zu analysieren und auch den Ursprung dieser Beeinträchtigung zu identifizieren ». Diese den Betreibern eingeräumte Befugnis unterliegt nicht einer vorherigen Stellungnahme des BIPF und der Datenschutzbehörde oder einer Notifizierung an diese Behörden.

B.28.2. Die Verkehrsdaten, um die es in Artikel 122 § 4/1 Absatz 1 des Gesetzes vom 13. Juni 2005 geht, dürfen für eine Dauer von grundsätzlich zwölf Monaten gespeichert werden. Die Daten über eine « spezifische » Beeinträchtigung der Sicherheit des Netzes dürfen jedoch « während der für ihre Bearbeitung notwendigen Dauer, gegebenenfalls über die in Absatz 2 erwähnte Frist von zwölf Monaten hinaus » gespeichert werden (Artikel 122 § 4/1 Absatz 3).

B.29. Artikel 122 § 4 des Gesetzes vom 13. Juni 2005 sieht einerseits eine allgemeine und systematische Vorratsspeicherung der darin erwähnten Verkehrsdaten vor und erlegt andererseits den Betreibern eine Pflicht zur Vorratsspeicherung und Verarbeitung auf, wobei er es ihnen überlässt, unter denjenigen, die in Artikel 122 § 4 Absatz 1 Nrn. 1 und 2 erwähnt sind, die Daten zu identifizieren, die gespeichert werden müssen. Mit anderen Worten: Die Pflicht zur Vorratsdatenspeicherung stellt im Rahmen von Artikel 122 § 4 des Gesetzes vom 13. Juni 2005 nicht die Ausnahme, sondern die Regel dar.

Diese Feststellung gilt umso mehr als aufgrund von Artikel 122 § 4 Absatz 4 des Gesetzes vom 13. Juni 2005 die von den Betreibern auf Vorrat gespeicherten Verkehrsdaten, die mit einem mutmaßlichen Betrug oder mit einer mutmaßlichen böswilligen Nutzung im Zusammenhang stehen, an die zuständigen Behörden übermittelt werden können, insbesondere an die Gerichtsbehörden, die Polizeidienste und die Gerichtspolizeioffiziere des BIPF (*Parl. Dok.*, Kammer, 2021-2022, DOC 55-2572/001, S. 35), sodass die von den Betreibern auf der Grundlage von Artikel 122 § 4 des Gesetzes vom 13. Juni 2005 vorgenommenen Datenspeicherungen und -verarbeitungen zu einer Strafverfolgung führen können.

B.30.1. In Bezug auf Artikel 122 § 4/1 des Gesetzes vom 13. Juni 2005 ist festzustellen, dass in dieser Bestimmung nicht präzisiert ist, welche Daten auf Vorrat gespeichert werden dürfen. Außerdem dürfen die Daten über eine « spezifische » Beeinträchtigung der Sicherheit des Netzes « über die in Absatz 2 erwähnte Frist von zwölf Monaten hinaus » auf Vorrat gespeichert werden, ohne dass weder in der Formulierung von Artikel 122 § 4/1 des Gesetzes vom 13. Juni 2005 noch in den Vorarbeiten zum Gesetz vom 20. Juli 2022 präzisiert ist, was der Fall einer spezifischen Beeinträchtigung umfasst.

B.30.2. Zum Datum der Verkündung dieses Entscheids hatte der Gerichtshof der Europäischen Union noch nicht über die Auslegung von Artikel 15 der Richtlinie 2002/58/EG zu befinden, insofern er den Mitgliedstaaten gestattet, Maßnahmen zur Vorratsspeicherung von Daten der elektronischen Kommunikation zu erlassen, um die Verhütung, Ermittlung, Feststellung und Verfolgung des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen sicherzustellen.

B.30.3. Die Meinungen der Parteien vor dem Gerichtshof gehen in Bezug auf die Auslegung von Artikel 15 der Richtlinie 2002/58/EG auseinander, insofern er sich auf den vorerwähnten Zweck bezieht und in diesem Rahmen, ob er dahin auszulegen ist oder nicht, dass er die Annahme von nationalen Maßnahmen wie den von Artikel 5 Nrn. 4 und 5 des Gesetzes vom 20. Juli 2022 vorgesehenen gestattet.

B.31. Wenn eine Frage zur Auslegung des Unionsrechts in einem schwebenden Verfahren bei einem einzelstaatlichen Gericht gestellt wird, dessen Entscheidungen selbst nicht mehr mit Rechtsmitteln des innerstaatlichen Rechts angefochten werden können, so ist dieses Gericht nach Artikel 267 Absatz 3 des Vertrags über die Arbeitsweise der Europäischen Union verpflichtet, bezüglich dieser Frage den Gerichtshof der Europäischen Union anzurufen.

Ein solches Vorabentscheidungsersuchen ist gleichwohl nicht erforderlich, wenn dieses Gericht feststellt, dass die gestellte Frage nicht entscheidungserheblich ist, dass die betreffende unionsrechtliche Bestimmung bereits Gegenstand einer Auslegung durch den Gerichtshof der Europäischen Union war oder dass die richtige Auslegung des Unionsrechts derart offenkundig ist, dass für einen vernünftigen Zweifel keinerlei Raum bleibt (EuGH, 6. Oktober 1982, C-283/81, *CILFIT*, ECLI:EU:C:1982:335, Randnr. 21; Große Kammer, 6. Oktober 2021, C-561/19, *Consorzio Italian Management und Catania Multiservizi SpA*, ECLI:EU:C:2021:799, Randnr. 33). Diese Gründe müssen im Lichte von Artikel 47 der Charta die Begründung der Entscheidung ausreichend erkennen lassen, in der das Gericht es ablehnt, die Vorabentscheidungsfrage zu stellen (EuGH, Große Kammer, 6. Oktober 2021, C-561/19, vorerwähnt, Randnr. 51).

Die Ausnahme der fehlenden Entscheidungserheblichkeit beinhaltet, dass das nationale Gericht von der Vorlagepflicht befreit ist, wenn « die Frage nicht entscheidungserheblich ist, d.h., wenn die Antwort auf diese Frage, wie auch immer sie ausfällt, keinerlei Einfluss auf die Entscheidung des Rechtsstreits haben kann » (EuGH, 15. März 2017, C-3/16, *Aquino*, ECLI:EU:C:2017:209, Randnr. 43; Große Kammer, 6. Oktober 2021, C-561/19, vorerwähnt, Randnr. 34).

Die Ausnahme, dass die richtige Auslegung des Unionsrechts offenkundig ist, beinhaltet, dass das einzelstaatliche Gericht davon überzeugt ist, dass auch für die letztinstanzlichen Gerichte der übrigen Mitgliedstaaten und den Gerichtshof der Europäischen Union die gleiche

Gewissheit bestünde. Es muss in diesem Zusammenhang die Eigenheiten des Unionsrechts, die besonderen Schwierigkeiten seiner Auslegung und die Gefahr voneinander abweichender Gerichtsentscheidungen innerhalb der Union berücksichtigen. Ebenso muss es die Unterschiede zwischen den ihm bekannten Sprachfassungen der betreffenden Vorschrift berücksichtigen, insbesondere wenn diese Abweichungen von den Parteien vorgetragen werden und erwiesen sind. Schließlich muss es die eigene Terminologie und die autonomen Begriffe berücksichtigen, die das Unionsrecht verwendet, sowie den Zusammenhang der anzuwendenden Vorschrift im Lichte des gesamten Unionsrechts, seiner Ziele und seines Entwicklungsstands zur Zeit der Anwendung der betreffenden Vorschrift (EuGH, Große Kammer, 6. Oktober 2021, C-561/19, vorerwähnt, Randnrn. 40-46).

Darüber hinaus kann ein in letzter Instanz entscheidendes Gericht « aus Unzulässigkeitsgründen, die dem Verfahren vor diesem Gericht eigen sind », davon absehen, dem Gerichtshof der Europäischen Union eine Frage zur Vorabentscheidung vorzulegen, « sofern die Grundsätze der Äquivalenz und der Effektivität gewahrt bleiben » (EuGH, 14. Dezember 1995, C-430/93 und C-431/93, *Van Schijndel und Van Veen*, ECLI:EU:C:1995:441, Randnr. 17; 15. März 2017, C-3/16, vorerwähnt, Randnr. 56; Große Kammer, 6. Oktober 2021, C-561/19, vorerwähnt, Randnr. 61).

B.32. Da die aktuell geprüfte Rechtssache zu Zweifeln bei der Auslegung von Artikel 15 der Richtlinie 2002/58/EG führt, ist dem Gerichtshof der Europäischen Union die erste Vorabentscheidungsfrage, die im Tenor wiedergegeben ist, zu stellen.

4. Die Vorratsspeicherung von Standortdaten (Artikel 6)

B.33.1. Der erste und der zweite Klagegrund in der Rechtssache Nr. 7930 sowie der zweite Teil des ersten Klagegrunds und der erste Teil des dritten Klagegrunds in der Rechtssache Nr. 7932 beziehen sich auf Artikel 6 des Gesetzes vom 20. Juli 2022, der Artikel 123 des Gesetzes vom 13. Juni 2005 wie folgt abändert:

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

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

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

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

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

3° lorsque les données ont été rendues anonymes;

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

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

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

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

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

B.33.2. Wegen der oben erwähnten Abänderung bestimmt Artikel 123 des Gesetzes vom 13. Juni 2005 nunmehr:

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

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

2° lorsque cela est nécessaire pour détecter ou analyser les fraudes ou l'utilisation malveillante du réseau, les données étant conservées maximum quatre mois à partir de la date

de la communication, sauf en cas de fraude ou d'utilisation malveillante spécifique nécessitant de prolonger la conservation des données concernées au-delà de ce délai;

3° lorsque les données ont été rendues anonymes;

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

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

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

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

a) des types de données de localisation traités;

b) des objectifs précis du traitement;

c) de la durée du traitement;

d) des tiers éventuels auxquels ces données seront transmises;

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

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

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

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

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

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

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

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

Cette annulation est gratuite ».

B.33.3.1. Die klagende Partei in der Rechtssache Nr. 7930 leitet einen ersten und einen zweiten Klagegrund ab aus einem Verstoß gegen die Artikel 11, 12, 22 und 29 der Verfassung, gegen Artikel 15 Absatz 1 und gegen die Artikel 5, 6 und 9 der Richtlinie 2002/58/EG, gelesen im Lichte der Artikel 7, 8, 11, 47 und 52 Absatz 1 der Charta, der Artikel 6, 8, 10, 11 und 18 der Europäischen Menschenrechtskonvention und der Artikel 13 und 54 der Richtlinie (EU) 2016/680, insofern Artikel 6 des Gesetzes vom 20. Juli 2022 eine allgemeine Vorratsspeicherungspflicht für Kommunikationsdaten einführe, ohne dass diese Vorratsspeicherung notwendig erscheine oder im Hinblick auf das verfolgte Ziel strikt begrenzt sei.

B.33.3.2. Die klagenden Parteien in der Rechtssache Nr. 7932 leiten einen ersten Klagegrund ab aus einem Verstoß gegen die Artikel 10, 11, 13, 15, 22, 23 und 29 der Verfassung, an sich oder in Verbindung mit den Artikeln 5, 6, 8, 9, 10, 11, 14 und 18 der Europäischen Menschenrechtskonvention, mit den Artikeln 7, 8, 11, 47 und 52 der Charta, mit Artikel 5 Absatz 4 des Vertrags über die Europäische Union, sowie mit Artikel 6 der Richtlinie 2002/58/EG, mit der Richtlinie (EU) 2016/680 und mit der DSGVO. In einem zweiten Teil bringen sie vor, dass Artikel 6 des Gesetzes vom 20. Juli 2022 die Vorratsspeicherung der darin erwähnten Daten während zwölf Monaten erlaube, um das ordnungsgemäße Funktionieren der Sicherheit des Netzes sicherzustellen, obgleich Artikel 9 der Richtlinie 2002/58/EG eine solche Verarbeitung ausschließe.

Die klagenden Parteien leiten einen dritten Klagegrund ab aus einem Verstoß gegen die Artikel 10, 11, 15, 22 und 29 der Verfassung, an sich oder in Verbindung mit den Artikeln 5, 6, 8, 9, 10, 11, 14 und 18 der Europäischen Menschenrechtskonvention, mit den Artikeln 7, 8, 11, 47 und 52 der Charta, mit Artikel 5 Absatz 4 des Vertrags über die Europäische Union, sowie mit der Richtlinie 2002/58/EG, mit der Richtlinie (EU) 2016/680 und mit der DSGVO. In einem ersten Teil führen sie an, dass Artikel 6 des Gesetzes vom 20. Juli 2022 eine Pflicht

zu einer allgemeinen und unterschiedslosen Vorratsdatenspeicherung für die Betreiber schaffe, die im Rahmen ihrer Aufträge handelten, was zu vage und zu weit gefasst sei.

B.34. Aus dem Vorstehenden geht hervor, dass sich die Beschwerdegründe der klagenden Parteien auf Artikel 123 § 1 des Gesetzes vom 13. Juni 2005, ersetzt durch Artikel 6 Nr. 1 des Gesetzes vom 20. Juli 2022, beziehen. Diese Beschwerdegründe sind hauptsächlich aus einem Verstoß gegen das Recht auf Achtung des Privatlebens und das Recht auf Schutz personenbezogener Daten abgeleitet, die in Artikel 22 der Verfassung, in Artikel 8 der Europäischen Menschenrechtskonvention, in den Artikeln 7, 8 und 52 Absatz 1 der Charta, in der Richtlinie 2002/58/EG, in der Richtlinie (EU) 2016/680 und in der DSGVO gewährleistet sind.

B.35.1. Aus den Vorarbeiten zu Artikel 6 Nr. 1 des Gesetzes vom 20. Juli 2022 geht hervor, dass dieser bezweckt, Artikel 9 der Richtlinie 2002/58/EG umzusetzen (*Parl. Dok.*, Kammer, 2021-2022, DOC 55-2572/001, SS. 39 und 40), der bestimmt:

« *Andere Standortdaten als Verkehrsdaten*

(1) Können andere Standortdaten als Verkehrsdaten in Bezug auf die Nutzer oder Teilnehmer von öffentlichen Kommunikationsnetzen oder öffentlich zugänglichen Kommunikationsdiensten verarbeitet werden, so dürfen diese Daten nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Maß und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn die Nutzer oder Teilnehmer ihre Einwilligung gegeben haben. Der Diensteanbieter muss den Nutzern oder Teilnehmern vor Einholung ihrer Einwilligung mitteilen, welche Arten anderer Standortdaten als Verkehrsdaten verarbeitet werden, für welche Zwecke und wie lange das geschieht, und ob die Daten zum Zwecke der Bereitstellung des Dienstes mit Zusatznutzen an einen Dritten weitergegeben werden. Die Nutzer oder Teilnehmer können ihre Einwilligung zur Verarbeitung anderer Standortdaten als Verkehrsdaten jederzeit zurückziehen.

(2) Haben die Nutzer oder Teilnehmer ihre Einwilligung zur Verarbeitung von anderen Standortdaten als Verkehrsdaten gegeben, dann müssen sie auch weiterhin die Möglichkeit haben, die Verarbeitung solcher Daten für jede Verbindung zum Netz oder für jede Übertragung einer Nachricht auf einfache Weise und gebührenfrei zeitweise zu untersagen.

(3) Die Verarbeitung anderer Standortdaten als Verkehrsdaten gemäß den Absätzen 1 und 2 muss auf das für die Bereitstellung des Dienstes mit Zusatznutzen erforderliche Maß sowie auf Personen beschränkt werden, die im Auftrag des Betreibers des öffentlichen Kommunikationsnetzes oder öffentlich zugänglichen Kommunikationsdienstes oder des Dritten, der den Dienst mit Zusatznutzen anbietet, handeln ».

B.35.2. Insofern Artikel 123 § 1 des Gesetzes vom 13. Juni 2005 die Speicherung von anderen Standortdaten als Verkehrsdaten, die sich auf einen Teilnehmer oder einen Endnutzer beziehen, vorsieht, wenn die Daten anonymisiert wurden (Nr. 3) und wenn die Verarbeitung im Rahmen der Bereitstellung eines Dienstes, der Verkehrs- oder Standortdaten nutzt, erfolgt (Nr. 4) - vorausgesetzt, der Teilnehmer oder Endnutzer hat im letztgenannten Fall vorher seine Einwilligung nach Artikel 123 § 2 erteilt -, fällt diese Bestimmung unter die von Artikel 9 Absatz 1 der Richtlinie 2002/58/EG erwähnten Fälle.

B.35.3. Artikel 123 § 1 des Gesetzes vom 13. Juni 2005 bezieht sich jedoch auch auf andere Fälle der Speicherung von anderen Standortdaten als Verkehrsdaten als diejenigen, die nach Artikel 9 der Richtlinie 2002/58/EG erlaubt sind, wie es die Gesetzgebungsabteilung des Staatsrates und die Datenschutzbehörde in ihrem Gutachten bzw. in ihrer Stellungnahme zum Vorentwurf des Gesetzes, der dem Gesetz vom 20. Juli 2022 zugrunde liegt, festgestellt haben (ebenda, SS. 306 bis 308 und 677 bis 678).

Was diese anderen Fälle betrifft, ist auf Artikel 15 Absatz 1 der Richtlinie 2002/58/EG Bezug zu nehmen, der es erlaubt, die Rechte, die unter anderem in ihrem Artikel 9 vorgesehen sind, zu beschränken, « sofern eine solche Beschränkung […] für die nationale Sicherheit, (d.h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist ».

B.36. Die Beschwerdegründe der klagenden Parteien beziehen sich insbesondere auf die Fälle der Speicherung von anderen Standortdaten als Verkehrsdaten, die unter die Beschränkungsregelung fallen, die in Artikel 15 Absatz 1 der Richtlinie 2002/58/EG vorgesehen ist, und die in Artikel 123 § 1 Nrn. 1, 2 und 5 des Gesetzes vom 13. Juni 2005, ersetzt durch Artikel 6 des Gesetzes vom 20. Juli 2022, erwähnt sind.

B.37.1. Artikel 123 § 1 des Gesetzes vom 13. Juni 2005 sieht vor, dass die Mobilfunknetzbetreiber die vorerwähnten Standortdaten, die sich auf einen Teilnehmer oder einen Endnutzer beziehen, nur speichern und verarbeiten dürfen, « wenn dies für das ordnungsgemäße Funktionieren und die Sicherheit des Netzes oder des Dienstes notwendig

ist » (Nr. 1) und « wenn dies notwendig ist, um Betrugsfälle oder eine böswillige Nutzung des Netzes zu erkennen oder zu analysieren » (Nr. 2).

Die in Artikel 123 § 1 Nr. 1 des Gesetzes vom 13. Juni 2005 erwähnten Daten werden grundsätzlich zwölf Monate ab dem Datum der Kommunikation auf Vorrat gespeichert. Diejenigen, die in Artikel 123 § 1 Nr. 2 des Gesetzes vom 13. Juni 2005 erwähnt sind, werden grundsätzlich vier Monate auf Vorrat gespeichert.

B.37.2. Die in Artikel 123 § 1 Nrn. 1 und 2 des Gesetzes vom 13. Juni 2005 erwähnten Fälle ermöglichen es, die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen im Sinne von Artikel 15 Absatz 1 der Richtlinie 2002/58/EG sicherzustellen.

B.38. Der Gerichtshof hat zu prüfen, ob der von Artikel 123 § 1 Nrn. 1 und 2 des Gesetzes vom 13. Juni 2005, ersetzt durch Artikel 6 Nr. 1 des Gesetzes vom 20. Juli 2022, herbeigeführte Eingriff in das Recht auf Achtung des Privatlebens und in das Recht auf Schutz personenbezogener Daten in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist, um dem unzulässigen Gebrauch von elektronischen Kommunikationssystemen vorzubeugen.

B.39.1. Die Betreiber bestimmen die anderen Standortdaten als die Verkehrsdaten, die auf Vorrat gespeichert und verarbeitet werden können. Sie beurteilen ebenfalls in jedem Einzelfall die Notwendigkeit dieser Speicherung und dieser Verarbeitung.

Außerdem ist in Bezug auf die Speicherfrist für die genannten in Artikel 123 § 1 Nrn. 1 und 2 des Gesetzes vom 13. Juni 2005 erwähnten Daten vorgesehen, dass die vorerwähnte Dauer von zwölf Monaten « im Fall einer spezifischen Beeinträchtigung der Sicherheit des Netzes, die es erfordert, die Speicherung der betreffenden Daten über diese Frist hinaus zu verlängern » verlängert werden kann und dass die vorerwähnte Dauer von vier Monaten « im Fall eines Betrugs oder einer spezifischen böswilligen Nutzung, die es erfordert, die Speicherung der betreffenden Daten über diese Frist hinaus zu verlängern » verlängert werden kann.

B.39.2. Artikel 123 § 1 Nrn. 1 und 2 des Gesetzes vom 13. Juni 2005 überlässt es den Betreibern, unter den Standortdaten die Daten zu identifizieren, die gespeichert und verarbeitet werden müssen, und die Speicherfrist der betreffenden Daten im Fall einer spezifischen Beeinträchtigung der Sicherheit des Netzes zum einen und im Fall eines Betrugs oder einer spezifischen böswilligen Nutzung zum anderen zu verlängern.

B.39.3. Aus den gleichen Gründen wie denen, die in B.30 und B.31 aufgeführt sind, und da die aktuell geprüfte Rechtssache zu Zweifeln bei der Auslegung von Artikel 15 Absatz 1 der Richtlinie 2002/58/EG führt, ist dem Gerichtshof der Europäischen Union die zweite Vorabentscheidungsfrage, die im Tenor wiedergegeben ist, zu stellen.

Außerdem ist die dritte Vorabentscheidungsfrage, die im Tenor aufgeführt ist, zu stellen.

B.40.1. Schließlich erlaubt Artikel 123 § 1 Nr. 5 des Gesetzes vom 13. Juni 2005 die Vorratsspeicherung von anderen Standortdaten als Verkehrsdaten, die sich auf einen Teilnehmer oder einen Endnutzer beziehen, « wenn die Verarbeitung notwendig ist, um einer durch eine formelle Gesetzesnorm vorgeschriebenen Pflicht nachzukommen ».

In diesem Fall können die Beschwerdegründe der klagenden Parteien nicht auf Artikel 123 des Gesetzes vom 13. Juni 2005 an sich zurückgeführt werden, sondern gegebenenfalls auf die durch eine formelle Gesetzesnorm vorgeschriebenen Pflichten, auf die Bezug genommen wird.

B.40.2. Der erste und der zweite Klagegrund in der Rechtssache Nr. 7930 sowie der zweite Teil des ersten Klagegrunds und der erste Teil des dritten Klagegrunds in der Rechtssache Nr. 7932 in Bezug auf Artikel 123 § 1 Nr. 5 des Gesetzes vom 13. Juni 2005 sind unbegründet, insofern sie aus einem Verstoß gegen die in B.34 genannten Bestimmungen abgeleitet sind. Die Prüfung anhand der anderen in B.33.3.1 und B.33.3.2 genannten Referenznormen - vorausgesetzt, dass ein Verstoß gegen sie von den klagenden Parteien zu Recht geltend gemacht würde - kann in jedem Fall nicht zu einer anderen Schlussfolgerung führen.

5. Die Vorratsspeicherung von Abonnements- und Identifizierungsdaten (Artikel 8)

B.41.1. Der erste und der zweite Klagegrund in der Rechtssache Nr. 7930, der einzige Klagegrund in der Rechtssache Nr. 7931 sowie der erste, der zweite und der fünfte Teil des zweiten Klagegrunds in der Rechtssache Nr. 7932 beziehen sich auf Artikel 8 des Gesetzes vom 20. Juli 2022, der bestimmt:

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

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

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

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

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

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

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

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

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

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

5° l'adresse physique de livraison du service;

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

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

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

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

10° le numéro de téléphone attribué;

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

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

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

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

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

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

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

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

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

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

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

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

Le Roi :

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

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

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

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

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

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

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

B.41.2.1. Die klagende Partei in der Rechtssache Nr. 7930 leitet einen ersten und einen zweiten Klagegrund ab aus einem Verstoß gegen die Artikel 11, 12, 22 und 29 der Verfassung, gegen Artikel 15 Absatz 1 und gegen die Artikel 5, 6 und 9 der Richtlinie 2002/58/EG, gelesen im Lichte der Artikel 7, 8, 11, 47 und 52 Absatz 1 der Charta, der Artikel 6, 8, 10, 11 und 18 der Europäischen Menschenrechtskonvention und der Artikel 13 und 54 der Richtlinie (EU) 2016/680, insofern Artikel 8 des Gesetzes vom 20. Juli 2022 eine allgemeine Vorratsspeicherungspflicht für Kommunikationsdaten einführe, ohne dass diese Vorratsspeicherung notwendig erscheine oder im Hinblick auf das verfolgte Ziel strikt begrenzt sei.

B.41.2.2. Die klagende Partei in der Rechtssache Nr. 7931 leitet einen einzigen Klagegrund ab aus einem Verstoß gegen die Artikel 11, 12, 22 und 29 der Verfassung, an sich oder in Verbindung mit den Artikeln 7, 8, 11, 47 und 52 Absatz 1 der Charta, mit Artikel 8 der Europäischen Menschenrechtskonvention, mit den Artikel 5, 6 und 15 der Richtlinie 2002/58/EG und mit den Artikeln 13 und 54 der Richtlinie (EU) 2016/680. Sie führt an, dass Artikel 8 des Gesetzes vom 20. Juli 2022 eine Pflicht zur systematischen und unterschiedslosen Vorratsspeicherung von Identifizierungsdaten vorsehe, die im Hinblick auf das verfolgte Ziel nicht notwendig sei. Hilfsweise beantragt die klagende Partei, dem Gerichtshof der Europäischen Union eine Vorabentscheidungsfrage zu stellen.

B.41.2.3. Die klagenden Parteien in der Rechtssache Nr. 7932 leiten einen zweiten Klagegrund ab aus einem Verstoß gegen die Artikel 10, 11, 15, 22 und 29 der Verfassung, an sich oder in Verbindung mit den Artikeln 5, 6, 8, 9, 10, 11, 14 und 18 der Europäischen Menschenrechtskonvention, mit den Artikeln 7, 8, 11, 47 und 52 der Charta, mit Artikel 5 Absatz 4 des Vertrags über die Europäische Union, mit der Richtlinie 2002/58/EG, mit der Richtlinie (EU) 2016/680 und mit der DSGVO. Im ersten und im dritten Teil führen sie an, dass Artikel 8 des Gesetzes vom 20. Juli 2022 eine Vorratsdatenspeicherung, die nicht notwendig sei, sowie eine zu lange Speicherfrist vorsehe, sodass er nicht mit dem Recht auf Achtung des Privatlebens und mit Artikel 5 § 1 Buchstaben *c)* und *d)* der DSGVO vereinbar sei. In einem zweiten Teil bringen sie vor, dass Artikel 8 des Gesetzes vom 20. Juli 2022, insofern als er auf elektronische « *Over-the-top* »-Kommunikationsdienste (nachstehend: OTT-Dienste) wie « *WhatsApp* » und « *Skype* » Anwendung finde, eine Gleichbehandlung herbeiführe, die gegen den Grundsatz der Gleichheit und Nichtdiskriminierung und gegen das Legalitätsprinzip verstoße.

B.42. Der erste und der zweite Klagegrund in der Rechtssache Nr. 7930, der einzige Klagegrund in der Rechtssache Nr. 7931 sowie der erste und der dritte Teil des zweiten Klagegrunds in der Rechtssache Nr. 7932 sind hauptsächlich abgeleitet aus einem Verstoß gegen das Recht auf Achtung des Privatlebens und das Recht auf Schutz personenbezogener Daten, die in Artikel 22 der Verfassung, in Artikel 8 der Europäischen Menschenrechtskonvention, in den Artikeln 7, 8 und 52 Absatz 1 der Charta, in der Richtlinie 2002/58/EG, in der Richtlinie (EU) 2016/680 und in der DSGVO gewährleistet sind.

B.43.1. Aus den Vorarbeiten zu Artikel 8 des Gesetzes vom 20. Juli 2022 geht hervor, dass der Gesetzgeber mit dieser Bestimmung dem Entscheid des Gerichtshofes Nr. 158/2021 Rechnung tragen wollte, indem er selbst die verschiedenen Identifizierungsdaten aufzählt, die auf Vorrat zu speichern sind (*Parl. Dok.*, Kammer, 2021-2022, DOC 55-2572/002, SS. 5 bis 7).

B.43.2. Zudem geht aus diesen Vorarbeiten hervor, dass der Gesetzgeber auch anstrebte, für die in Artikel 126 § 1 Absatz 1 erwähnten Betreiber die Pflicht einzuführen, die vorerwähnten Identifizierungsdaten auf Vorrat zu speichern (ebenda, SS. 7 bis 10).

Diesbezüglich hat die Datenschutzbehörde in ihrer Stellungnahme zu dem Abänderungsantrag, der Artikel 8 des Gesetzes vom 20. Juli 2022 zugrunde liegt, festgestellt:

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

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

permettent ainsi potentiellement de suivre les déplacements des utilisateurs de ces services; ce qui constitue une ingérence particulièrement importante dans le droit au respect de la vie privée de ces utilisateurs.

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

B.44.1. Im Tenor seines Urteils vom 6. Oktober 2020 in Sachen *La Quadrature du Net u.a.* hat der Gerichtshof der Europäischen Union für Recht erkannt, dass Artikel 15 Absatz 1 der Richtlinie 2002/58/EG im Licht der Artikel 7, 8 und 11 sowie Artikel 52 Absatz 1 der Charta unter anderem gesetzgeberischen Maßnahmen nicht entgegensteht, die « zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit für einen auf das absolut Notwendige begrenzten Zeitraum eine allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, vorsehen » einerseits und « zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zum Schutz der öffentlichen Sicherheit eine allgemeine und unterschiedslose Vorratsspeicherung der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten vorsehen » andererseits.

B.44.2. Wie die Gesetzgebungsabteilung des Staatsrates in ihrem Gutachten zum Vorentwurf des Gesetzes, der dem Gesetz vom 20. Juli 2022 zugrunde liegt, angemerkt hat, nimmt der Gerichtshof der Europäischen Union folglich eine Unterscheidung vor zwischen einerseits der allgemeinen und unterschiedslosen Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, die den Betreibern nur zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit auferlegt werden kann, und zwar für einen auf das absolut Notwendige begrenzten Zeitraum, und andererseits der allgemeinen und unterschiedslosen Vorratsspeicherung der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten, die den Betreibern zu weiter gefassten Zwecken auferlegt werden kann, nämlich zum Schutz der nationalen Sicherheit, zur Bekämpfung der Kriminalität, unabhängig davon, ob diese schwer ist oder nicht, und zum Schutz der öffentlichen Sicherheit, auch wenn diese Sicherheit nicht Gegenstand schwerer Bedrohungen ist, und zwar ohne dass diese Daten

für einen auf das absolut Notwendige begrenzten Zeitraum gespeichert werden sollen (*Parl. Dok.*, Kammer, 2021-2022, DOC 55-2572/001, S. 296).

B.44.3. Außerdem ist der Gerichtshof der Europäischen Union der Auffassung, dass für die IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, eine besondere Regelung gelten muss, da diese « insbesondere zur umfassenden Nachverfolgung der von einem Internetnutzer besuchten Internetseiten und infolgedessen seiner Online-Aktivität genutzt werden können, [und] sie die Erstellung eines detaillierten Profils dieses Nutzers [ermöglichen]. Die für eine solche Nachverfolgung erforderliche Vorratsspeicherung und Analyse der IP-Adressen stellen daher schwere Eingriffe in die Grundrechte des Internetnutzers aus den Art. 7 und 8 der Charta dar » (EuGH, Urteil vom 6. Oktober 2020, vorerwähnt, C-511/18, C-512/18 und C-520/18, Randnr. 153).

B.45. In seinem Urteil des Plenums vom 30. April 2024 in Sachen *La Quadrature du Net u.a. (Personenbezogene Daten und Bekämpfung der Nachahmung)* (C-470/21, ECLI:EU:C:2024:370) hat der Gerichtshof der Europäischen Union dies wie folgt präzisiert:

« 75. [Es] ist festzustellen, dass nach der Rechtsprechung des Gerichtshofs IP-Adressen zwar […] Verkehrsdaten im Sinne der Richtlinie 2002/58 darstellen, sich aber von den anderen Kategorien von Verkehrs- und Standortdaten unterscheiden.

76. Hierzu hat der Gerichtshof ausgeführt, dass IP-Adressen ohne Anknüpfung an eine bestimmte Kommunikation erzeugt werden und in erster Linie dazu dienen, über die Betreiber elektronischer Kommunikationsdienste den Besitzer eines Endgeräts zu ermitteln, von dem aus eine Kommunikation über das Internet stattfindet. Sofern im Bereich von E-Mail und Internettelefonie nur die IP-Adressen der Kommunikationsquelle gespeichert werden und nicht die des Adressaten einer Kommunikation, lässt sich diesen Adressen als solchen somit keine Information über die Dritten entnehmen, mit denen die Person, von der die Kommunikation ausging, in Kontakt stand. Diese Datenkategorie weist daher einen geringeren Sensibilitätsgrad als die übrigen Verkehrsdaten auf (vgl. in diesem Sinne Urteil vom 6. Oktober 2020, *La Quadrature du Net u. a.*, C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 152).

77. Zwar hat der Gerichtshof in Rn. 156 des Urteils vom 6. Oktober 2020, *La Quadrature du Net u. a.* (C-511/18, C-512/18 und C-520/18, EU:C:2020:791), entschieden, dass Art. 15 Abs. 1 der Richtlinie 2002/58 trotz des geringeren Sensibilitätsgrads, den IP-Adressen haben, wenn sie ausschließlich zur Identifizierung des Nutzers eines elektronischen Kommunikationsdiensts dienen, einer allgemeinen und unterschiedslosen Vorratsspeicherung allein der IP-Adressen der Quelle einer Verbindung für andere Zwecke als denen der Bekämpfung schwerer Kriminalität, der Verhütung schwerer Bedrohungen der öffentlichen Sicherheit oder des Schutzes der nationalen Sicherheit entgegensteht. Er hat sich bei dieser Schlussfolgerung jedoch ausdrücklich auf die Schwere des Eingriffs in die in den Art. 7, 8 und

11 der Charta verankerten Grundrechte gestützt, der mit einer solchen Speicherung der IP-Adressen verbunden sein kann.

78. Der Gerichtshof hat nämlich in Rn. 153 dieses Urteils ausgeführt, dass die IP-Adressen, da sie insbesondere zur ‘ umfassenden Nachverfolgung der von einem Internetnutzer besuchten Internetseiten ’ und infolgedessen seiner Online-Aktivität genutzt werden können, die Erstellung eines ‘ detaillierten Profils ’ dieses Nutzers ermöglichen, so dass ihre für eine solche Nachverfolgung erforderliche Vorratsspeicherung und Analyse schwere Eingriffe in die Grundrechte des Betroffenen aus den Art. 7 und 8 der Charta darstellen, was auch abschreckende Wirkungen auf die Ausübung der durch Art. 11 der Charta garantierten Freiheit der Meinungsäußerung durch die Nutzer elektronischer Kommunikationsmittel entfalten kann.

79. Hervorzuheben ist jedoch, dass nicht jede allgemeine und unterschiedslose Vorratsspeicherung eines unter Umständen umfangreichen Bestands der von einer Person innerhalb eines bestimmten Zeitraums genutzten statischen und dynamischen IP-Adressen zwangsläufig einen schweren Eingriff in die durch die Art. 7, 8 und 11 der Charta garantierten Grundrechte darstellt.

80. Insoweit betrafen zunächst die Rechtssachen, in denen das Urteil vom 6. Oktober 2020, *La Quadrature du Net u. a.* (C-511/18, C-512/18 und C-520/18, EU:C:2020:791), ergangen ist, nationale Regelungen, die eine Pflicht zur Vorratsspeicherung eines Datensatzes vorsahen, der benötigt wurde, um Datum, Uhrzeit, Dauer und Art der Kommunikation zu ermitteln, das verwendete Kommunikationsmaterial zu identifizieren sowie den Ort der Endgeräte und der Kommunikation zu bestimmen; dazu gehörten u. a. Name und Adresse des Nutzers, die Telefonnummern des Anrufers und des Angerufenen sowie die IP-Adresse für die Internetdienste. Überdies erfassten die in zwei dieser Rechtssachen in Rede stehenden nationalen Regelungen Daten in Bezug auf die Weiterleitung der elektronischen Kommunikation durch die Netze, die es ermöglichten, auch die Art online konsultierter Informationen zu identifizieren (vgl. in diesem Sinne Urteil vom 6. Oktober 2020, *La Quadrature du Net u. a.*, C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 82 und 83).

81. Die im Rahmen solcher nationaler Regelungen erfolgte Vorratsspeicherung der IP-Adressen war daher angesichts der übrigen Daten, deren Vorratsspeicherung sie vorschrieben, und der Möglichkeit, diese verschiedenen Daten zu kombinieren, geeignet, genaue Schlüsse auf das Privatleben der Personen zu ermöglichen, deren Daten betroffen waren, und konnte damit zu einem schweren Eingriff in ihre in den Art. 7 und 8 der Charta verankerten, den Schutz ihres Privatlebens und ihrer personenbezogenen Daten betreffenden Grundrechte sowie in ihre in Art. 11 der Charta verankerte Freiheit der Meinungsäußerung führen.

82. Dagegen kann die den Betreibern elektronischer Kommunikationsdienste durch eine Rechtsvorschrift im Sinne von Art. 15 Abs. 1 der Richtlinie 2002/58 auferlegte Pflicht, die allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen sicherzustellen, gegebenenfalls durch das Ziel der Bekämpfung von Straftaten im Allgemeinen gerechtfertigt sein, wenn tatsächlich ausgeschlossen ist, dass diese Speicherung schwere Eingriffe in das Privatleben des Betroffenen zur Folge haben kann, die darauf beruhen, dass insbesondere durch eine Verknüpfung dieser IP-Adressen mit einem von den Betreibern ebenfalls gespeicherten Satz von Verkehrs- oder Standortdaten die Möglichkeit besteht, genaue Schlüsse in Bezug auf ihn zu ziehen.

83. Daher muss sich ein Mitgliedstaat, der den Betreibern elektronischer Kommunikationsdienste eine Pflicht zur allgemeinen und unterschiedslosen Vorratsspeicherung von IP-Adressen auferlegen möchte, um ein mit der Bekämpfung von Straftaten im Allgemeinen verbundenes Ziel zu erreichen, vergewissern, dass die Modalitäten der Vorratsspeicherung dieser Daten zu gewährleisten vermögen, dass jede Kombination der IP-Adressen mit anderen unter Beachtung der Richtlinie 2002/58 auf Vorrat gespeicherten Daten ausgeschlossen ist, die es ermöglichen würde, genaue Schlüsse auf das Privatleben der Personen zu ziehen, deren Daten in dieser Weise gespeichert wurden.

84. Um sicherzustellen, dass eine solche, genaue Schlüsse auf das Privatleben der betreffenden Person ermöglichende Kombination von Daten ausgeschlossen ist, müssen die Modalitäten der Vorratsspeicherung die Struktur der Speicherung als solche betreffen, die im Wesentlichen so gestaltet sein muss, dass eine wirksame strikte Trennung der verschiedenen Kategorien auf Vorrat gespeicherter Daten gewährleistet ist.

85. Insoweit ist es zwar Sache des Mitgliedstaats, der den Betreibern elektronischer Kommunikationsdienste zur Erreichung eines mit der Bekämpfung von Straftaten im Allgemeinen verbundenen Ziels eine Pflicht zur allgemeinen und unterschiedslosen Vorratsspeicherung der IP-Adressen auferlegen will, in seinen Rechtsvorschriften klare und präzise Regeln für die Modalitäten der Speicherung vorzusehen, die strengen Anforderungen genügen müssen. Der Gerichtshof kann jedoch Erläuterungen zu diesen Modalitäten geben.

86. Erstens müssen die in der vorstehenden Randnummer genannten nationalen Regeln sicherstellen, dass jede Kategorie von Daten, einschließlich der Identitätsdaten und der IP-Adressen, völlig getrennt von den übrigen Kategorien auf Vorrat gespeicherter Daten gespeichert wird.

87. Zweitens müssen diese Regeln gewährleisten, dass in technischer Hinsicht eine wirksame strikte Trennung zwischen den verschiedenen Kategorien auf Vorrat gespeicherter Daten, u. a. den Identitätsdaten, den IP-Adressen, den verschiedenen Verkehrsdaten außer den IP-Adressen und den verschiedenen Standortdaten durch eine abgesicherte und zuverlässige Datenverarbeitungseinrichtung stattfindet.

88. Drittens dürfen die Regeln, soweit sie die Möglichkeit vorsehen, die auf Vorrat gespeicherten IP-Adressen mit der Identität des Betroffenen zu verknüpfen, unter Beachtung der Anforderungen, die sich aus Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 der Charta ergeben, eine solche Verknüpfung nur unter Verwendung eines leistungsfähigen technischen Verfahrens erlauben, das die Wirksamkeit der strikten Trennung dieser Datenkategorien nicht in Frage stellt.

89. Viertens muss die Zuverlässigkeit dieser strikten Trennung regelmäßig Gegenstand einer Kontrolle durch eine andere Behörde als die sein, die Zugang zu den von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten personenbezogenen Daten begehrt.

90. Soweit im anwendbaren nationalen Recht solche strengen Anforderungen an die Modalitäten der allgemeinen und unterschiedslosen Vorratsspeicherung von IP-Adressen und anderen von den Betreibern elektronischer Kommunikationsdienste gespeicherten Daten

vorgesehen sind, kann der Eingriff, der sich aus dieser Speicherung der IP-Adressen ergibt, schon aufgrund der Struktur ihrer Speicherung nicht als ‘ schwer ’ eingestuft werden.

91. Falls eine solche gesetzliche Regelung geschaffen wird, schließen die durch sie vorgeschriebenen Modalitäten der Speicherung der IP-Adressen nämlich eine Kombination dieser Daten mit anderen unter Beachtung der Richtlinie 2002/58 gespeicherten Daten aus, die es ermöglichen würde, genaue Schlüsse auf das Privatleben des Betroffenen zu ziehen.

92. Folglich hindert, sofern es eine den oben in den Rn. 86 bis 89 dargelegten Anforderungen entsprechende gesetzliche Regelung gibt, die gewährleistet, dass keine Kombination von Daten genaue Schlüsse auf das Privatleben der fraglichen Person zulassen wird, Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8 und 11 der Charta den betreffenden Mitgliedstaat nicht daran, mit dem Ziel der Bekämpfung von Straftaten im Allgemeinen eine Pflicht zur allgemeinen und unterschiedslosen Vorratsspeicherung von IP-Adressen aufzustellen.

93. Schließlich muss eine solche gesetzliche Regelung, wie sich aus Rn. 168 des Urteils vom 6. Oktober 2020, *La Quadrature du Net u. a.* (C-511/18, C-512/18 und C-520/18, EU:C:2020:791), ergibt, eine auf das absolut Notwendige begrenzte Dauer der Speicherung vorsehen und durch klare und präzise Regeln sicherstellen, dass bei der Speicherung der fraglichen Daten die für sie geltenden materiellen und prozeduralen Voraussetzungen eingehalten werden und dass die Betroffenen über wirksame Garantien zum Schutz vor Missbrauchsgefahren sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung verfügen ».

B.46.1. Artikel 126 § 1 Absatz 1 des Gesetzes vom 13. Juni 2005 bezieht sich auf siebzehn Identifizierungsdaten, die die vorerwähnten Betreiber auf Vorrat speichern müssen, wenn sie diese Daten im Rahmen der Dienste und Netze, die sie bereitstellen, verarbeiten oder erzeugen. Es handelt sich um die Nationalregisternummer oder eine gleichwertige Nummer, den Vor- und Nachnamen des Endnutzers, der eine natürliche Person ist, oder die Bezeichnung des Teilnehmers, der eine juristische Person ist (Nr. 1); den eventuell vom Endnutzer beim Abschluss des Dienstes oder der Aktivierung des Dienstes gewählten Aliasnamen (Nr. 2); die Kontaktdaten des Teilnehmers, die beim Abschluss des Dienstes angegeben wurden, insbesondere seine Telefonnummer, seine E-Mail-Adresse und seine Postadresse (Nr. 3); das Datum und die Uhrzeit des Abschlusses des Dienstes und der Aktivierung des Dienstes sowie die Angaben, mit denen der Ort bestimmt werden kann, von dem aus dieser Abschluss und diese Aktivierung durchgeführt worden sind, das heißt insbesondere die physische Adresse der Verkaufsstelle, wo der Abschluss oder die Aktivierung stattgefunden haben, oder die physische Adresse des Netzabschlusspunktes, der für den Abschluss oder die Aktivierung gedient hat, oder die IP-Adresse, die für den Abschluss oder die Aktivierung gedient hat, sowie der Quellport der Verbindung und die Zeitstempelung oder im Rahmen eines Mobilfunknetzes der geografische Standort des Endgeräts, das den Abschluss oder die Aktivierung mittels einer

Telefonnummer ermöglicht hat (Nr. 4); die physische Adresse der Bereitstellung des Dienstes (Nr. 5); die Rechnungsadresse des Dienstes und die Daten über die Zahlungsart und das Zahlungsmittel, das Datum der Zahlungen und die Bezugsangabe des Zahlungsvorgangs im Fall einer Online-Zahlung (Nr. 6); den Hauptdienst und zusätzliche Dienste, die der Teilnehmer nutzen kann (Nr. 7); das Datum, ab dem diese Dienste genutzt werden können, das Datum der ersten Nutzung dieser Dienste und das Datum des Endes dieser Dienste (Nr. 8); im Fall der Übertragung der Kennung des Teilnehmers wie seiner Telefonnummer die Identität des Betreibers, der die Kennung überträgt und die Identität des Betreibers, an den die Kennung übertragen wird und das Datum, an dem die Übertragung vorgenommen wird (Nr. 9); die zugeteilte Telefonnummer (Nr. 10); die Haupt-E-Mail-Adresse und die als E-Mail-Aliasse verwendeten Adressen (Nr. 11); die internationale Mobilfunk-Teilnehmerkennung, « *International Mobile Subscriber Identity* » (abgekürzt « IMSI ») (Nr. 12); die permanente Kennung eines Teilnehmers, « *Subscription Permanent Identifier* » (abgekürzt « SUPI ») (Nr. 13); die verborgene Teilnehmerkennung, « *Subscription Concealed Identifier* » (abgekürzt « SUCI ») (Nr. 14); die IP-Adresse an der Quelle der Verbindung, die Zeitstempelung der Zuweisung sowie im Fall einer gemeinsamen Nutzung einer IP-Adresse des Endnutzers die Ports, die ihm zugewiesen worden sind (Nr. 15); die Kennung des Endgeräts des Endnutzers oder, wenn der Betreiber sie nicht verarbeitet oder erzeugt, die Kennung des Geräts, das diesem Endgerät am nächsten ist, das heißt insbesondere die internationale Kennung für mobile Geräte, « *International Mobile Equipment Identity* » (abgekürzt « IMEI »), die permanente Kennung des Geräts, « *Permanent Equipment Identifier* » (abgekürzt « PEI »), und die Adresse der Netzwerkschnittstelle, « *Media Access Control address* » (abgekürzt « MAC ») (Nr. 16); die anderen Kennungen des Endnutzers, des Endgeräts oder des Geräts, das diesem Endgerät am nächsten ist, die sich aus der technologischen Entwicklung ergeben und die vom König bestimmt werden, sofern dieser Erlass binnen sechs Monaten nach der Veröffentlichung dieses Erlasses gesetzlich bestätigt wird, vorausgesetzt, dass diese anderen Kennungen weder den Inhalt der elektronischen Kommunikation noch die Metadaten der elektronischen Kommunikation betreffen, die Aufschluss geben über den Empfänger der Kommunikation, wie die IP-Adresse des Empfängers der Kommunikation, oder über den Standort des Endgeräts.

B.46.2. Aufgrund von Artikel 126 § 1 Absatz 4 des Gesetzes vom 13. Juni 2005 kann der König die vorerwähnten Daten präzisieren und Anforderungen an die Genauigkeit und Zuverlässigkeit festlegen, denen diese Daten genügen müssen.

B.46.3. Artikel 126 des Gesetzes vom 13. Juni 2005 gibt nicht selbst die Zwecke an, zu denen diese Daten auf Vorrat gespeichert werden müssen. Es wird diesbezüglich auf Artikel 127/1 § 3 des Gesetzes vom 13. Juni 2005, eingefügt durch Artikel 13 des Gesetzes vom 20. Juli 2022 verwiesen, der bestimmt:

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

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

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

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

Artikel 127/1 § 2 des Gesetzes vom 13. Juni 2005 lautet:

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

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

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

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

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

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

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

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

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

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

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

B.46.4. Was die Speicherfrist der vorerwähnten Daten betrifft, sieht Artikel 126 § 2 des Gesetzes vom 13. Juni 2005 vor, dass die in Paragraph 1 Absatz 1 Nrn. 1 bis 14 erwähnten Daten solange auf Vorrat gespeichert werden, wie der elektronische Kommunikationsdienst genutzt wird, und zwölf Monate nach dem Ende dieses Dienstes. Was die in Paragraph 1 Absatz 1 Nrn. 15 und 16 desselben Artikels erwähnten Daten betrifft, werden diese zwölf Monate nach dem Ende der Sitzung auf Vorrat gespeichert. Die Adresse der Netzwerkschnittstelle (MAC) wird jedoch sechs Monate nach dem Ende der Sitzung auf Vorrat gespeichert, wenn der Betreiber eine andere in Paragraph 1 Absatz 1 Nr. 16 desselben Artikels erwähnte Datenangabe auf Vorrat speichert. Schließlich werden die in Paragraph 1 Absatz 1 Nr. 17 dieses Artikels erwähnten Daten für eine vom König festgelegte Dauer auf Vorrat gespeichert, ohne dass diese zwölf Monate nach dem Ende des Dienstes übersteigen darf.

B.47.1. Sämtliche in Artikel 126 § 1 Absatz 1 des Gesetzes vom 13. Juni 2005 erwähnten Daten, darunter die « IP-Adresse an der Quelle der Verbindung » (Nrn. 4 und 15), können für die in Artikel 127/1 § 2 Nrn. 1 bis 8 dieses Gesetzes aufgezählten Zwecke auf Vorrat gespeichert werden. Diese Zwecke sind weit gefasst und decken insbesondere ab die Prüfung einer Sicherheitspanne des Netzes oder des elektronischen Kommunikationsdienstes oder der Informationssysteme (Nr. 4), die Verhütung, Ermittlung, Feststellung und Verfolgung von online oder über ein Netz oder einen elektronischen Kommunikationsdienst begangenen Straftaten (Nr. 5) und die Verhütung, Ermittlung, Feststellung und Verfolgung von Taten, die eine Straftat sind, aber nicht unter die schwere Kriminalität fallen (Nr. 8).

B.47.2. Artikel 126 § 1 Absatz 1 des Gesetzes vom 13. Juni 2005 bezieht sich auf bestimmte die Identität der Nutzer elektronischer Kommunikationsmittel betreffende Daten. Wie in B.44.2 erwähnt, dürfen diese Daten zum Schutz der nationalen Sicherheit, zur Bekämpfung der Kriminalität, unabhängig davon, ob diese schwer ist oder nicht, und zum Schutz der öffentlichen Sicherheit allgemein und unterschiedslos auf Vorrat gespeichert werden. Bei den in Artikel 127/1 § 2 Nrn. 1 bis 8 aufgezählten Zwecken kann davon ausgegangen werden, dass sie dieser Anforderung entsprechen.

B.47.3. Wie in B.44.3 erwähnt, ist es zu vermeiden, dass die fraglichen Daten mit anderen auf Vorrat gespeichert Daten kombiniert werden können, die genaue Schlüsse auf das Privatleben der betroffenen Personen ermöglichen.

B.48.1. Der Ministerrat bringt diesbezüglich in seinem Ergänzungsschriftsatz vom 30. Mai 2024 vor, dass die Anforderung einer strikten Trennung zwischen den betroffenen Datenkategorien, wie sie im vorerwähnten Urteil des Gerichtshofes der Europäischen Union vom 30. April 2024 erwähnt ist, im Rahmen des Zugangs einer Behörde zu den von den Betreibern elektronischer Kommunikationsdienste gespeicherten Datenbanken wegen des Risikos, dass diese Behörde diese Daten analysiert und die von dieser Datenbank gebotenen Möglichkeiten nutzt, diese Daten miteinander zu kombinieren, um daraus genaue Schlüsse auf das Privatleben der betroffenen Personen zu ziehen, erforderlich ist.

Gemäß Artikel 127/1 § 2 des Gesetzes vom 13. Juni 2005 greifen aber die Behörden, die die Daten erhalten können, die die Betreiber aufgrund der Artikel 122 und 123 desselben Gesetzes auf Vorrat speichern, nicht selbst auf die Datenbanken der Betreiber elektronischer Kommunikationsdienste mit der Möglichkeit, sie zu analysieren und zu kombinieren, zu (Datenextraktion nach der « Pull »-Methode). Diese Behörden müssen unter den von dem angefochtenen Gesetz und den Organgesetzen, die auf sie anwendbar sind, ein gezieltes Ersuchen über die Bereitstellung von bestimmten, vom Betreiber elektronischer Kommunikationsdienste auf Vorrat gespeicherten Daten stellen (Datenbereitstellung nach der « Push »-Methode), ohne dass dieser diesen Behörden Zugang zu der Datenbank gewährt.

B.48.2. Artikel 124 des Gesetzes vom 13. Juni 2005 bestimmt diesbezüglich:

« Niemand darf ohne Einwilligung aller mittelbar oder unmittelbar betroffenen Personen:

1. vorsätzlich Kenntnis von Informationen jeder Art nehmen, die im Wege der elektronischen Kommunikation übermittelt werden und sich nicht an sie persönlich richten,

2. vorsätzlich Personen ermitteln, die von der Übertragung der Information und deren Inhalt betroffen sind,

3. unbeschadet der Anwendung der Artikel 122 und 123 vorsätzlich Kenntnis von Daten im Bereich der elektronischen Kommunikation nehmen, die sich auf andere Personen beziehen,

4. Informationen, Identifizierungsdaten oder Daten, ob vorsätzlich erhalten oder nicht, ändern, löschen, veröffentlichen, speichern oder auf gleich welche Weise nutzen ».

Die Artikel 127/2 und 127/3 bestimmen:

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

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

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

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

2° mettent en œuvre des mesures de protection technologique qui rendent les données conservées, dès leur enregistrement, illisibles et inutilisables par toute personne qui n'est pas autorisée à y avoir accès;

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

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

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

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

3° veillent à ce que les données conservées fassent l'objet de mesures techniques et organisationnelles appropriées afin de les protéger contre la destruction accidentelle ou illicite,

la perte ou l'altération accidentelle, ou le stockage, le traitement, l'accès ou la divulgation non autorisés ou illicites, conformément à l'article 107/2;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Ces autorités adressent leurs demandes à cette cellule.

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

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

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

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

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

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

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

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

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

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

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

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

§ 3. Chaque opérateur établit une procédure interne permettant de répondre aux demandes d'accès des autorités aux données à caractère personnel concernant les utilisateurs finaux. Il met, sur demande, à la disposition de l'Institut, des informations sur ces procédures, sur le nombre de demandes reçues, sur la base juridique invoquée et sur sa réponse.

Chaque opérateur est considéré comme responsable du traitement au sens du RGDP pour les données traitées sur la base des articles 122, 123, 126, 126/1, 126/2, 126/3 et 127.

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

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

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

c) le délai de réponse;

d) la disponibilité requise du service;

e) les modalités de test de la collaboration;

f) les tarifs de rétribution de cette collaboration.

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

B.48.3. Wie der Ministerrat in seinem Ergänzungsschriftsatz vom 30. Mai 2024 anführt, legt das angefochtene Gesetz dadurch strikte Bedingungen fest, die es verhindern, dass sowohl die Betreiber als auch die zuständigen Behörden die IP-Adressen nutzen können, um eine umfassende Nachverfolgung der von einem Internetnutzer besuchten Internetseiten und

infolgedessen seiner Online-Aktivität vorzunehmen sowie um mit Hilfe dieser Daten ein detailliertes Profil dieses Nutzers zu erstellen.

B.48.4. Im Übrigen ist nicht erkennbar, inwiefern die Anwendbarkeit von Artikel 8 des Gesetzes vom 20. Juli 2022 auf die OTT-Dienste gegen den Grundsatz der Gleichheit und Nichtdiskriminierung und das Legalitätsprinzip verstoßen würde.

B.49. Der erste und der zweite Klagegrund in der Rechtssache Nr. 7930, der einzige Klagegrund in der Rechtssache Nr. 7931 sowie der erste und der dritte Teil des zweiten Klagegrunds in der Rechtssache Nr. 7932 sind unbegründet, sofern sie aus einem Verstoß gegen Artikel 22 der Verfassung in Verbindung mit Artikel 8 der Europäischen Menschenrechtskonvention, mit den Artikeln 7, 8 und 52 Absatz 1 der Charta und mit Artikel 15 Absatz 1 der Richtlinie 2002/58/EG abgeleitet sind.

6. Die Pflicht zur Identifizierung von Teilnehmern und Endnutzern von elektronischen Kommunikationsdiensten (Artikel 12)

B.50. Der erste und der zweite Klagegrund in der Rechtssache Nr. 7930 sowie der dritte, der vierte und der sechste Teil des zweiten Klagegrunds in der Rechtssache Nr. 7932 beziehen sich auf Artikel 12 des Gesetzes vom 20. Juli 2022, der Artikel 127 des Gesetzes vom 13. Juni 2005 wie folgt abändert:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- les autres services déterminés par le Roi.

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

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

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

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

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

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

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

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

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

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

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

- que ce document est relatif à la personne identifiée.

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

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

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

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

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

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

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

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

1° la carte d'identité électronique belge;

2° le passeport belge;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

19° la carte bleue européenne (carte H);

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

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

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

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

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

25° l’acte de notoriété;

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

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

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

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

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

31° le passeport étranger;

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

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

Par dérogation à l'alinéa 2, un opérateur peut refuser d'identifier un abonné sur base d'un document d'identification visé à l'alinéa 1er autre que la carte d'identité électronique belge s'il lui offre la possibilité de s'identifier selon une des manières alternatives visées à l'arrêté royal du 27 novembre 2016 relatif à l'identification de l'utilisateur final de services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée et pour autant que l'abonné soit en mesure de mettre en œuvre cette alternative.

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

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

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

Sans préjudice de l'article 126, lorsqu'un opérateur identifie l'abonné à partir d'un autre document que la carte d'identité électronique belge ou au moyen d'une autre méthode d'identification directe que la présentation d'un document d'identification, il conserve parmi les données suivantes celles qui se trouvent sur le document d'identification présenté ou qui sont traitées lors de la mise en œuvre de la méthode d'identification directe :

1° le nom et le prénom;

2° la nationalité;

3° la date de naissance;

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

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

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

§ 8. Lorsqu'un opérateur fournit à un abonné qui est une personne morale un service de communications électroniques mobile sur la base d'une carte prépayée et qu'il l'identifie par le

biais d'une méthode d'identification directe, il collecte et conserve, en respectant les exigences visées aux paragraphes 4 à 7, l'identité civile d'une personne physique qui agit pour le compte de la personne morale.

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

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

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

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

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

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

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

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

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

- le nom, le prénom, l'adresse du domicile et la date de naissance déclarés par la personne physique qui est l'abonné de l'opérateur ou qui agit pour le compte d'une personne morale qui est l'abonnée de l'opérateur afin de remplir son obligation en matière d'identification, ou;

4° en cas de carte SIM (' subscriber identity/identification module ') ou toute autre carte équivalente intégrée dans un véhicule, en collectant et conservant le numéro de châssis de ce véhicule ainsi que le lien entre ce numéro et le numéro de cette carte;

5° en cas de souscription d'un abonné qui réside dans un centre fermé ou un lieu d'hébergement au sens des articles 74/8 et 74/9 de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers à un service de communications électroniques mobile fourni au moyen d'une carte prépayée, en collectant et conservant le nom et le prénom de l'abonné, son numéro de sécurité publique, à savoir le numéro de dossier attribué par l'Office des Etrangers et les coordonnées du centre ou du lieu d'hébergement où la souscription a eu lieu, ou;

6° en cas de souscription à un service de communications électroniques par une personne morale au nom et pour le compte d'une personne physique qui rencontre des difficultés à

effectuer cette souscription, en collectant et conservant la dénomination précise de cette personne morale et, pour ce qui concerne cette personne physique, au minimum son nom, son prénom, son adresse de résidence, lorsqu'elle en dispose, sa date de naissance et le numéro par lequel elle est identifiée, tel un numéro de registre national, ces informations lui étant transmises par cette personne morale.

Pour l'application de l'alinéa 1er, 6°, la personne morale :

1° doit, avant de pouvoir souscrire à un service de communications électroniques pour la personne physique, obtenir un agrément, délivré par le ministre et le ministre de la Justice, et ayant pour objet de vérifier qu'elle respecte les valeurs démocratiques inscrites dans la Constitution ainsi que le présent article;

2° s'identifie auprès de l'opérateur conformément au présent article;

3° identifie les abonnés à l'aide d'un des documents d'identification visés au paragraphe 6, conformément aux exigences de fiabilité visées au paragraphe 5, ou à l'aide d'une autre méthode autorisée dans l'agrément visé au 1°;

4° conserve une copie du document d'identification des abonnés autre que la carte d'identité électronique belge, sauf dérogation accordée dans l'agrément visé au 1°;

5° conserve une liste actualisée permettant de faire le lien entre le service de communications électroniques et les abonnés, comprenant au minimum le nom, le prénom, l'adresse de la résidence, lorsque la personne en dispose, la date de naissance et le numéro par lequel elle est identifiée, tel le numéro de registre national.

Le Roi peut :

1° prévoir par méthode visée à l'alinéa 1er les conditions à respecter, une condition pouvant être l'obtention d'une autorisation préalable du ministre et du ministre de la Justice;

2° imposer des obligations aux opérateurs, aux personnes morales visées à l'alinéa 1er, aux entreprises fournissant un service d'identification et aux abonnés, en vue de l'identification de ces derniers.

§ 11. Sauf preuve contraire, la personne identifiée est présumée utiliser elle-même le service de communications électroniques.

Pour les services de communications électroniques mobiles fournis au moyen d'une carte prépayée, le Roi :

1° restreint la possibilité pour l'abonné de permettre à des tiers de bénéficier du service;

2° impose des obligations aux abonnés qui sont des personnes morales afin de déterminer les utilisateurs habituels du service.

L'opérateur qui offre une carte SIM ou toute carte équivalente, destinée à être intégrée dans un véhicule, conserve le numéro de châssis de ce véhicule ainsi que le lien entre ce numéro et

le numéro de cette carte. À la demande d'une autorité, l'opérateur ne lui communique que ce numéro de châssis ou le numéro de cette carte.

Le Roi peut fixer les modalités de l'obligation visée à l'alinéa 3 et peut imposer aux entreprises qui disposent du numéro de châssis de le transmettre aux opérateurs.

§ 12. Si un opérateur ne respecte pas les mesures qui lui sont imposées par le présent article ou par le Roi, il lui est interdit de fournir le service pour lequel les mesures en question n'ont pas été prises.

Les opérateurs déconnectent les abonnés qui ne respectent pas les mesures qui leur sont imposées par le présent article ou par le Roi, des réseaux et services auxquels les mesures imposées s'appliquent. Ces abonnés ne sont en aucune manière indemnisés pour la déconnexion.

L'arrêté royal visé dans le présent article est proposé par le ministre de la Justice, le ministre de l'Intérieur, le ministre de la Défense et le ministre, fait l'objet d'un avis de l'Autorité de protection des données et de l'Institut et est délibéré en Conseil des ministres. ' ».

B.51.1. Die klagende Partei in der Rechtssache Nr. 7930 leitet einen ersten und einen zweiten Klagegrund ab aus einem Verstoß gegen die Artikel 11, 12, 22 und 29 der Verfassung, gegen Artikel 15 Absatz 1 und gegen die Artikel 5, 6 und 9 der Richtlinie 2002/58/EG, gelesen im Lichte der Artikel 7, 8, 11, 47 und 52 Absatz 1 der Charta, der Artikel 6, 8, 10, 11 und 18 der Europäischen Menschenrechtskonvention und der Artikel 13 und 54 der Richtlinie (EU) 2016/680, insofern Artikel 12 des Gesetzes vom 20. Juli 2022 eine allgemeine Vorratsspeicherungspflicht für Identifizierungsdaten einführe, ohne dass diese Vorratsspeicherung notwendig erscheine oder im Hinblick auf das verfolgte Ziel strikt begrenzt sei. Insbesondere führt sie an, dass dieses System nicht mit der Rechtsprechung des Gerichtshofes der Europäischen Union bezüglich Artikel 15 der Richtlinie 2002/58/EG und der Artikel 7, 8 und 52 der Charta im Einklang stehe, die eine solche Vorratsspeicherung nur zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit erlaube.

Aus den Darlegungen des ersten und des zweiten Klagegrunds zu Artikel 12 des Gesetzes vom 20. Juli 2022 geht hervor, dass die Beschwerdegründe dieser klagenden Partei dahin auszulegen sind, dass sie sich in diesem Rahmen nur auf die Liste der in dieser Bestimmung erwähnten Identifizierungsdaten und ihre Speicherfrist beziehen, insofern diese Maßnahmen nicht mit dem Recht auf Achtung des Privatlebens und dem Recht auf Schutz personenbezogener Daten, die in den in B.11.2 genannten Bestimmungen gewährleistet sind, vereinbar seien.

Die klagende Partei führt keinen Beschwerdegrund an, der im Rahmen von Artikel 12 des Gesetzes vom 20. Juli 2022 aus einem Verstoß gegen die anderen im ersten und im zweiten Klagegrund genannten Referenznormen abgeleitet ist.

B.51.2. Die klagenden Parteien in der Rechtssache Nr. 7932 leiten einen zweiten Klagegrund ab aus einem Verstoß gegen die Artikel 10, 11, 15, 22 und 29 der Verfassung, an sich oder in Verbindung mit den Artikeln 5, 6, 8, 9, 10, 11, 14 und 18 der Europäischen Menschenrechtskonvention, mit den Artikeln 7, 8, 11, 47 und 52 der Charta, mit Artikel 5 Absatz 4 des Vertrags über die Europäische Union, sowie mit der Richtlinie 2002/58/EG, mit der Richtlinie (EU) 2016/680 und mit der DSGVO.

Die Beschwerdegründe der klagenden Parteien beziehen sich zunächst auf Artikel 127 § 5 Absatz 3 des Gesetzes vom 13. Juni 2005, insofern er die Nutzung der Technologie der Gesichtserkennung erlauben würde, was gegen das Recht auf Achtung des Privatlebens und das Recht auf Schutz personenbezogener Daten verstoßen würde (dritter Teil). Sodann beanstanden die klagenden Parteien die Maßnahme, die in Artikel 127 § 10 Nr. 4 des Gesetzes vom 13. Juni 2005 vorgesehen ist, der im Fall einer SIM-Karte oder einer in ein Fahrzeug eingebauten gleichwertigen Karte die Sammlung und Speicherung der Fahrgestellnummer dieses Fahrzeugs und die Verknüpfung zwischen dieser Nummer und der Nummer der Karte vorsieht. Ihrer Auffassung nach ist diese Maßnahme unverhältnismäßig, insbesondere durch ihre Kombination mit der obligatorischen Speicherung der Standortdaten auf den Autobahnen. Dieser Beschwerdegrund ist dahin auszulegen, dass er sich auf die Vereinbarkeit der vorerwähnten Maßnahme mit dem Recht auf Achtung des Privatlebens bezieht (vierter Teil). Schließlich führen die klagenden Parteien an, dass Artikel 127 § 11 des Gesetzes vom 13. Juni 2005 nicht mit dem Recht auf ein faires Verfahren, das in Artikel 6 der Europäischen Menschenrechtskonvention gewährleistet ist, vereinbar sei, insofern er eine Vermutung einführe, dass ein elektronischer Kommunikationsdienst von der Person genutzt werde, die auf der Grundlage dieser Bestimmung identifiziert worden sei (sechster Teil).

B.52. Der Gerichtshof prüft zunächst die Liste der aufgrund von Artikel 12 des Gesetzes vom 20. Juli 2022 auf Vorrat gespeicherten Daten - darunter die Maßnahme zu den SIM-Karten oder den gleichwertigen Karten - und ihrer Speicherfrist (erster und zweiter Klagegrund in der Rechtssache Nr. 7930, vierter Teil des zweiter Klagegrunds in der Rechtssache Nr. 7932), dann

die Vermutung der Nutzung des elektronischen Kommunikationsdienstes (sechster Teil des zweiten Klagegrunds in der Rechtssache Nr. 7932) und schließlich die Nutzung der Technologie der Gesichtserkennung (dritter Teil des zweiten Klagegrunds in der Rechtssache Nr. 7932).

B.53.1. Aufgrund von Artikel 127 des Gesetzes vom 13. Juni 2005, ersetzt durch Artikel 12 des Gesetzes vom 20. Juli 2022, obliegt es den « Betreibern, die in Belgien den Endnutzern einen elektronischen Kommunikationsdienst bereitstellen », die Teilnehmer dieses Dienstes zu identifizieren (Artikel 127 § 3), und zwar mithilfe einer direkten oder indirekten Identifizierungsmethode (Artikel 127 § 10).

Die direkte Identifizierungsmethode ist die Methode, mit der der Betreiber einerseits « verlässliche Daten über die Identität einer natürlichen Person, die sein Teilnehmer ist oder die im Auftrag einer juristischen Person handelt, die die Teilnehmerin des Betreibers ist » sammelt und speichert, « um die Pflicht zur Identifizierung der juristischen Person zu erfüllen », und andererseits « eine Kopie des Identifizierungsdokuments dieser natürlichen Person » sammelt und speichert, und zwar für die Zwecke der in Artikel 127/1 § 3 Absatz 1 des Gesetzes vom 13. Juni 2005 erwähnten Behörden (Artikel 127 § 2 Nr. 3).

Die indirekte Identifizierungsmethode ist « die Methode, mit der der Betreiber Daten sammelt und speichert, die es den in Artikel 127/1 § 3 Absatz 1 erwähnten Behörden ermöglichen, von einem Dritten die Identität seiner Teilnehmer zu erhalten » (Artikel 127 § 2 Nr. 4).

B.53.2.1. Die zulässigen Dokumente, um die Identifizierung des Teilnehmers vorzunehmen, sind in Artikel 127 § 6 Absatz 1 des Gesetzes vom 13. Juni 2005 erwähnt. Es handelt sich um den belgischen elektronischen Personalausweis (Nr. 1), den belgischen Reisepass (Nr. 2), die gültige Bescheinigung über die Eintragung im Fremdenregister - zeitweiliger Aufenthalt, ausgestellt vor dem 11. Oktober 2021 (Karte A) (Nr. 3), den begrenzten Aufenthaltstitel (Karte A) (Nr. 4), die gültige Bescheinigung über die Eintragung im Fremdenregister, ausgestellt vor dem 11. Oktober 2021 (Karte B) (Nr. 5), den unbegrenzten Aufenthaltstitel (Karte B) (Nr. 6), den gültigen Personalausweis für Ausländer, ausgestellt vor dem 11. Oktober 2021 (Karte C) (Nr. 7), den Niederlassungsschein (Karte K) (Nr. 8), den gültigen Aufenthaltstitel für langfristig

Aufenthaltsberechtigte - EU, ausgestellt vor dem 11. Oktober 2021 (Karte D) (Nr. 9), den Aufenthaltstitel für langfristig Aufenthaltsberechtigte - EU (Karte L) (Nr. 10), die gültige Anmeldebescheinigung, ausgestellt vor dem 10. Mai 2021 (Karte E) (Nr. 11), die Anmeldebescheinigung « Art.8 RL 2004/38/EG » E (Karte EU) (Nr. 12), das gültige Dokument zur Bescheinigung des Daueraufenthalts, ausgestellt vor dem 10 Mai 2021 (Karte E+) (Nr. 13), das Dokument zur Bescheinigung des Daueraufenthalts « Art.19 RL 2004/38/EG » (Karte EU+) (Nr. 14), die gültige Aufenthaltskarte für Familienangehörige eines Unionsbürgers, ausgestellt vor dem 11. Oktober 2021 (Karte F) (Nr. 15), die Aufenthaltskarte für Familienangehörige eines Unionsbürgers « EU-Familienangehöriger – Art.10 RL 2004/38/EG » (Karte F) (Nr. 16), die gültige Daueraufenthaltskarte für Familienangehörige eines Unionsbürgers, ausgestellt vor dem 11. Oktober 2021 (Karte F+) (Nr. 17), die Daueraufenthaltskarte für Familienangehörige eines Unionsbürgers « EU-Familienangehöriger – Art.20 RL 2004/38/EG » (Karte F+) (Nr. 18), die Blaue Karte EU (Karte H) (Nr. 19), die Erlaubnis für unternehmensintern transferierte Arbeitnehmer « ICT » (Karte I) (Nr. 20), die Erlaubnis für langfristige Mobilität « Mobile ICT » (Karte J) (Nr. 21), die Aufenthaltskarte für Begünstigte des Austrittsabkommens « Art.50 EUV » (Karte M) (Nr. 22), die Daueraufenthaltskarte für Begünstigte des Austrittsabkommens « Art.50 EUV » (Karte M) (Nr. 23), die Karte für kleinen Grenzverkehr für Begünstigte des Austrittsabkommens « Art.50 EUV – Grenzgänger » (Karte N) (Nr. 24), die Offenkundigkeitsurkunde (Nr. 25), die Anlage 12, ausgestellt in Anwendung von Artikel 6 des königlichen Erlasses vom 25. März 2003 « über die Personalausweise » oder in Anwendung von Artikel 36*bis* des königlichen Erlasses vom 8. Oktober 1981 « über die Einreise ins Staatsgebiet, den Aufenthalt, die Niederlassung und das Ausweisen von Ausländern » (Nr. 26), die Registrierungsbescheinigung (orange Karte) (Nr. 27), den ausländischen Personalausweis, wenn ein internationaler Reisepass nicht erforderlich ist, um sich in Belgien aufzuhalten (Nr. 28), die besonderen Personalausweise, die den in den diplomatischen und konsularischen Missionen tätigen Personenkategorien und ihren Familienangehörigen aufgrund der Wiener Übereinkommen von 1961 und 1963 und des königlichen Erlasses vom 30. Oktober 1991 « über die Dokumente für den Aufenthalt bestimmter Ausländer in Belgien » ausgestellt werden (Nr. 29), den Personalweis, der gemäß dem Genfer Abkommen vom 12. August 1949 über den Schutz der Opfer internationaler bewaffneter Konflikte ausgestellt wird (Nr. 30), den ausländischen Reisepass (Nr. 31) und schließlich um jedes andere Dokument, das vom König bestimmt wird, sofern der königliche

Erlass binnen sechs Monaten nach der Veröffentlichung dieses Erlasses gesetzlich bestätigt wird (Nr. 32).

B.53.2.2. Aufgrund von Artikel 127 § 6 Absatz 2 des Gesetzes vom 13. Juni 2005 erlaubt der Betreiber, der über eine Verkaufsstelle verfügt, seinem Teilnehmer, sich mit dem Identifizierungsdokument seiner Wahl von denjenigen, die in Absatz 1 aufgezählt sind, auszuweisen. Aufgrund von Absatz 3 kann der Betreiber es jedoch verweigern, den Teilnehmer anhand einer der vorerwähnten Identifizierungsdokumente zu identifizieren, wenn der Teilnehmer die Möglichkeit hat, sich in einer der anderen Weisen auszuweisen, die im königlichen Erlass vom 27. November 2016 « über die Identifizierung des Endnutzers öffentlich zugänglicher elektronischer Mobilfunkdienste, die über eine Guthabenkarte abgerechnet werden » erwähnt sind. Diese Lösung ist nicht möglich, wenn der Teilnehmer wünscht, anhand seines belgischen elektronischen Personalausweises identifiziert zu werden.

B.53.2.3. In dem Fall, dass der Teilnehmer anhand eines der vorerwähnten Identifizierungsdokumente identifiziert wird, speichert der Betreiber eine Kopie dieses Dokuments, außer wenn es sich um den belgischen elektronischen Personalausweis handelt (Artikel 127 § 6 Absatz 4).

B.53.3.1. Nach der Identifizierung des Teilnehmers obliegt es dem Betreiber, bestimmte personenbezogene Daten in Anwendung von Artikel 127 §§ 7 und 8 des Gesetzes vom 13. Juni 2005 zu speichern.

B.53.3.2. Wenn der Teilnehmer eine natürliche Person ist und die Identifizierung anhand des belgischen elektronischen Personalausweises vorgenommen wird, speichert der Betreiber die Nationalregisternummer, den Vor- und Nachnamen des Teilnehmers (Artikel 127 § 7 Absatz 1).

B.53.3.3. Wenn der Teilnehmer eine natürliche Person ist und die Identifizierung anhand eines anderen Dokuments als des belgischen elektronischen Personalausweises, das in Artikel 127 § 6 Absatz 1 Nrn. 2 bis 32 erwähnt ist, oder anhand einer anderen direkten Identifizierungsmethode als der Vorlage eines Identifizierungsdokuments vorgenommen wird, speichert der Betreiber von den Daten, die sich auf dem Identifizierungsdokument befinden oder die bei der Durchführung der direkten Identifizierungsmethode verarbeitet werden, den

Vor- und Nachnamen, die Staatsangehörigkeit, das Geburtsdatum, die Adresse des Wohnsitzes, die E-Mail-Adresse, die Telefonnummer, die Nummer des Identifizierungsdokuments und das Ausstellungsland des Dokuments, wenn es sich um ein ausländisches Dokument handelt, und schließlich die Verknüpfung zwischen dem neuen elektronischen Kommunikationsdienst, den der Teilnehmer abschließt, und dem Dienst, für den er bereits identifiziert wurde (Artikel 127 § 7 Absatz 2).

B.53.3.4. Wenn der Teilnehmer eine juristische Person ist, der elektronische Kommunikationsdienst über eine Guthabenkarte abgerechnet wird und die Identifizierung anhand einer direkten Identifizierungsmethode vorgenommen wird, sammelt und speichert der Betreiber die in Artikel 127 §§ 4 bis 7 des Gesetzes vom 13. Juni 2005 erwähnten Daten, die sich auf die Identität einer natürlichen Person beziehen, die im Auftrag der juristischen Person handelt (Artikel 127 § 8).

B.53.4. Schließlich obliegt es aufgrund von Artikel 127 § 10 des Gesetzes vom 13. Juni 2005 den Betreibern, es den in Artikel 127/1 § 3 Absatz 1 desselben Gesetzes erwähnten Behörden zu ermöglichen, ihre Teilnehmer anhand einer indirekten Identifizierungsmethode zu identifizieren.

Dafür sieht Artikel 127 § 10 Absatz 1 vor, dass die Betreiber in Ausführung von Artikel 126 des Gesetzes vom 13. Juni 2005 und für die von diesem Artikel vorgesehenen Zeiträume die IP-Adresse, die für den Abschluss des elektronischen Kommunikationsdienstes oder seine Aktivierung gedient hat, die IP-Adresse an der Quelle der Verbindung und die Daten, die mit diesen Adressen gespeichert werden müssen (Nr. 1) oder die Telefonnummer des Teilnehmers, die im Rahmen eines zahlungspflichtigen elektronischen Kommunikationsdienstes zugewiesen wurde, für den ein Betreiber den Teilnehmer gemäß Artikel 127 des Gesetzes vom 13. Juni 2005 identifizieren muss, auf Vorrat speichern (Nr. 2); dass die Betreiber im Fall einer spezifischen Online-Zahlung für den Abschluss eines elektronischen Kommunikationsdienstes die Bezugsangabe des Zahlungsvorgangs, den Vor- und Nachnamen, die Adresse des Wohnsitzes und das Geburtsdatum sammeln und speichern, die von der natürlichen Person angegeben wurden, die der Teilnehmer des Betreibers ist oder die im Auftrag einer juristischen Person handelt, die die Teilnehmerin des Betreibers ist, um die Pflicht zur Identifizierung der juristischen Person zu erfüllen (Nr. 3) oder im Fall einer SIM-Karte oder einer anderen in ein Fahrzeug eingebauten gleichwertigen Karte die

Fahrgestellnummer des Fahrzeugs und die Verknüpfung zwischen dieser Nummer und der Nummer der Karte (Nr. 4); dass die Betreiber im Fall eines Abschlusses durch einen Teilnehmer, der in einem geschlossenen Zentrum oder einem Unterbringungsort im Sinne der Artikel 74/8 und 74/9 des Gesetzes vom 15. Dezember 1980 «über die Einreise ins Staatsgebiet, den Aufenthalt, die Niederlassung und das Ausweisen von Ausländern » wohnt, von einem mobilen über eine Guthabenkarte abgerechneten elektronischen Kommunikationsdienst den Vor- und Nachnamen und die Nummer der Öffentlichen Sicherheit sammeln und auf Vorrat speichern (Nr. 5) oder im Fall des Abschlusses eines elektronischen Kommunikationsdienstes durch eine juristische Person im Namen und im Auftrag einer natürlichen Person, die Schwierigkeiten hat, diesen Abschluss zu tätigen, die genaue Bezeichnung dieser juristischen Person und in Bezug auf diese natürliche Person mindestens ihren Vor- und Nachnamen, die Adresse ihres Wohnortes, sofern sie über einen verfügt, ihr Geburtsdatum und die Nummer, mit der sie identifiziert wird, wie zum Beispiel eine Nationalregisternummer, wobei ihnen diese Informationen von dieser juristischen Person übermittelt werden (Nr. 6).

B.53.5. Die in B.53.2.1 bis B.53.4 erwähnten Daten werden, außer im Fall anderslautender gesetzlicher Bestimmungen, « ab dem Datum der Aktivierung des Dienstes bis zu zwölf Monate nach dem Ende des elektronischen Kommunikationsdienstes » auf Vorrat gespeichert (Artikel 127 § 4 Absatz 4).

B.54.1. Die in Artikel 127 des Gesetzes vom 13. Juni 2005 aufgezählten Daten haben zum Ziel, die Teilnehmer der Betreiber, auf die diese Bestimmung abzielt, zu identifizieren. In den Vorarbeiten zum Gesetz vom 20. Juli 2022 heißt es diesbezüglich:

« Un principe essentiel est qu'une personne doit rendre compte de ses actes, tant sur le plan civil que pénal. L'anonymat met en péril ce principe. La possibilité d'identifier l'abonné permet de le mettre en œuvre. Il est également essentiel qu'il soit possible pour les autorités (autorités judiciaires, services de renseignement et de sécurité et autres autorités qui peuvent demander des données de trafic ou d'identification aux opérateurs) de pouvoir retrouver l'identité de l'abonné » (*Parl. Dok.*, Kammer, 2021-2022, DOC 55-2572/002, S. 71).

In diesem Rahmen ist das Ziel auch, den Identitätsbetrug zu bekämpfen (ebenda, SS. 96 und 97).

B.54.2. Wie in B.44.2 erwähnt, ist bei den Identifizierungsdaten eine Unterscheidung zwischen den IP-Adressen an der Quelle einerseits und den die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten andererseits vorzunehmen.

B.55.1. Artikel 127 § 10 Absatz 1 Nr. 1 des Gesetzes vom 13. Juni 2005 weist auf die in Artikel 126 § 1 Absatz 1 Nrn. 4 und 15 enthaltene Pflicht hin, die den Betreibern obliegt, « die IP-Adresse, die für den Abschluss des elektronischen Kommunikationsdienstes oder seine Aktivierung gedient hat, die IP-Adresse an der Quelle der Verbindung und die Daten, die mit diesen Adressen gespeichert werden müssen » auf Vorrat zu speichern.

B.55.2. Da aus den in B.48.1 bis B.48.4 erwähnten Gründen Artikel 126 des Gesetzes vom 13. Juni 2005, eingefügt durch Artikel 8 des Gesetzes vom 20. Juli 2022, nicht gegen die in B.49 genannten Referenznormen verstößt und die aktuell geprüften Beschwerdegründe im Wesentlichen aus einem Verstoß gegen dieselben Referenznormen abgeleitet sind, gilt das Gleiche in Bezug auf Artikel 127 § 10 Absatz 1 Nr. 1 des Gesetzes vom 13. Juni 2005.

B.55.3. Der erste und der zweite Klagegrund in der Rechtssache Nr. 7930 sind unbegründet, insofern sie sich auf die Maßnahme der Vorratsspeicherung der in B.55.1 erwähnten Daten beziehen.

B.56. Die anderen in Artikel 127 §§ 4, 6 bis 8 und 10 des Gesetzes vom 13. Juni 2005 erwähnten Identifizierungsdaten können den die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten gleichgesetzt werden, da sie es für sich genommen weder ermöglichen, das Datum, die Uhrzeit, die Dauer und die Adressaten einer Kommunikation in Erfahrung zu bringen, noch die Orte, an denen sie stattfand, oder wie häufig dies mit bestimmten Personen innerhalb eines gegebenen Zeitraums geschah. Der Europäische Gerichtshof für Menschenrechte und der Gerichtshof der Europäischen Union sind nämlich der Auffassung, dass diese Daten keine Informationen über die konkreten Kommunikationen dieser Personen oder über ihr Privatleben liefern. Diese Daten allein ermöglichen es weder, ein Profil des Nutzers zu erstellen, noch seine Bewegungen zu verfolgen (EuGHMR, 30. Januar 2020, *Breyer gegen Deutschland*, ECLI:CE:ECHR:2020:0130JUD005000112, §§ 92-95; EuGH, Große Kammer, 2. Oktober 2018, C-207/16, *Ministerio Fiscal*, ECLI:EU:C:2018:788, Randnr. 62; Große Kammer, 6. Oktober 2020, C-511/18, C-512/18 und C-520/18, *La Quadrature du Net u.a.*, vorerwähnt, Randnr. 157).

Der Gerichtshof der Europäischen Union leitet daraus ab, dass das Recht auf Achtung des Privatlebens einem allgemeinen und unterschiedslosen Sammeln, Verarbeiten und Aufbewahren von Identifizierungsdaten von Nutzern elektronischer Kommunikationsnetzwerke zur Ermittlung, Feststellung und Verfolgung von Straftaten sowie zum Schutz der öffentlichen Sicherheit nicht entgegensteht. Dabei muss es sich nicht um schwere Straftaten, Bedrohungen oder Beeinträchtigungen der öffentlichen Sicherheit handeln (EuGH, Große Kammer, 6. Oktober 2020, C-511/18, C-512/18 und C-520/18, vorerwähnt). Allerdings muss der Nachweis erbracht werden, dass « diese Rechtsvorschriften […] durch klare und präzise Regeln sicherstellen, dass bei der Speicherung der fraglichen Daten die für sie geltenden materiellen und prozeduralen Voraussetzungen eingehalten werden und dass die Betroffenen über wirksame Garantien zum Schutz vor Missbrauchsrisiken verfügen » (ebenda, Randnr. 168).

Der Europäische Gerichtshof für Menschenrechte prüft das allgemeine und unterschiedslose Sammeln, Verarbeiten und Aufbewahren dieser Identifizierungsdaten auf weniger intensive Weise als das Sammeln, Verarbeiten und Aufbewahren von Verkehrs- und Standortdaten. Er prüft, ob die Aufbewahrungsfrist unter Berücksichtigung der üblichen Dauer einer strafrechtlichen Untersuchung angemessen ist. Der Europäische Gerichtshof für Menschenrechte verlangt nicht, dass für das Sammeln und Aufbewahren von bloßen Identifizierungsdaten eine vorherige Kontrolle vorgesehen wird; ein nachträglicher Zugang zu einer unabhängigen Gerichts- oder Verwaltungsinstanz verbunden mit gemeinrechtlichen Rechtsmitteln, über die ein Angeklagter im Laufe eines Strafverfahrens verfügt, ist ausreichend (EuGHMR, 30. Januar 2020, *Breyer gegen Deutschland*, vorerwähnt, §§ 96-107).

B.57.1. Die klagenden Parteien in der Rechtssache Nr. 7932 führen an, dass die in Artikel 127 § 10 Absatz 1 Nr. 4 des Gesetzes vom 13. Juni 2005 im Fall einer SIM-Karte oder einer in ein Fahrzeug eingebauten gleichwertigen Karte vorgesehene Maßnahme, die die Sammlung und Speicherung der Fahrgestellnummer des Fahrzeugs und die Verknüpfung zwischen dieser Nummer und der Nummer der Karte erlaubt, die ständige Nachverfolgung dieses Fahrzeugs über die Internetverbindung ermögliche, insbesondere über die Kombination dieser Identifizierungsdaten mit den Standortdaten auf den Autobahnen, deren Vorratsspeicherung aufgrund von Artikel 126/3 § 4 Buchstabe *c)* des Gesetzes vom 13. Juni 2005 erlaubt sei.

B.57.2. Artikel 127 § 10 Absatz 4 Nr. 4 des Gesetzes vom 13. Juni 2005 erlaubt weder die Vorratsspeicherung noch das Sammeln von Daten über die Internetverbindung der in dieser Bestimmung erwähnten Fahrzeuge.

Zudem ist es weder möglich, mithilfe der Fahrgestellnummer des Fahrzeugs, der Nummer der SIM-Karte oder der in das Fahrzeug eingebauten gleichwertigen Karte und der Verknüpfung zwischen den vorerwähnten Nummern die Fahrten, die Kommunikation, die Aktivitäten oder die sozialen Beziehungen einer Person nachzuverfolgen noch ein persönliches Profil zu erstellen, das genaue Schlüsse auf ihre sexuelle Orientierung, ihre Überzeugungen und ihren Gesundheitszustand ermöglicht. Für sich genommen offenbaren die vorerwähnten Daten keine sensiblen Informationen über das Privatleben.

Schließlich ist es zwar richtig, dass diese Identifizierungsdaten anschließend mit anderen Daten verknüpft werden und in dieser Weise zur Offenlegung von solchen sensiblen Informationen über das Privatleben einer Person beitragen können, aber diese anderen Daten werden in anderer Weise gesammelt und dieses Sammeln muss auch unter Einhaltung der geltenden Rechtsvorschriften und der Grundrechte des Betreffenden erfolgen.

B.57.3. Der vierte Teil des zweiten Klagegrunds in der Rechtssache Nr. 7932 ist unbegründet.

B.58.1. Was die Beschwerdegründe der klagenden Parteien in der Rechtssache Nr. 7930 betrifft, die in ihrem ersten und zweiten Klagegrund dargelegt werden, ist die Vereinbarkeit der Maßnahmen des Sammelns und der Vorratsspeicherung von Daten, die in Artikel 127 §§ 6 bis 8 und 10 Absatz 1 Nrn. 2 bis 6 des Gesetzes vom 13. Juni 2005 vorgesehen sind, mit dem Recht auf Achtung des Privatlebens anhand der in B.56 erwähnten Kriterien zu beurteilen.

B.58.2. Aus den in B.54.1 zitierten Vorarbeiten geht hervor, dass der Gesetzgeber mit Artikel 127 des Gesetzes vom 13. Juni 2005 die Ziele der Ermittlung, Feststellung und Verfolgung von Straftaten sowie den Schutz der öffentlichen Sicherheit im Sinne von Artikel 15 der Richtlinie 2002/58/EG verfolgte.

B.58.3.1. Die materiellen und prozeduralen Voraussetzungen für das Sammeln, die Verarbeitung und die Vorratsspeicherung der Identifizierungsdaten der Teilnehmer eines elektronischen Kommunikationsnetzes werden in den Artikeln 127 und 127/3 des Gesetzes vom 13. Juni 2005 geregelt.

B.58.3.2. Artikel 127 § 1 Absatz 1 des Gesetzes vom 13. Juni 2005 bestimmt die Personen, denen Pflichten in diesem Rahmen auferlegt werden, nämlich die Betreiber, die in Belgien für Endnutzer einen elektronischen Kommunikationsdienst bereitstellen. Artikel 127/3 § 3 Absatz 2 des Gesetzes vom 13. Juni 2005 benennt außerdem die vorerwähnten Betreiber als Verantwortliche für die Verarbeitung der Daten. Artikel 127 des Gesetzes vom 13. Juni 2005 legt überdies den Grundsatz fest, dass alle Teilnehmer identifizierbar sein müssen, und bestimmt, dass die Identifizierung mithilfe einer direkten oder indirekten Identifizierungsmethode erfolgen muss.

B.58.3.3. Artikel 127 des Gesetzes vom 13. Juni 2005 legt die Bedingungen für die Vorratsspeicherung der gesammelten Daten fest. Paragraph 6 dieser Bestimmung zählt die Dokumente auf, die zulässig sind, um die Identifizierung einer natürlichen Person, die gegebenenfalls für eine juristische Person handelt, vorzunehmen.

In den Paragraphen 7 und 8 ist präzisiert, welche Identifizierungsdaten von den Betreibern auf Vorrat gespeichert werden müssen. Paragraph 10 zählt schließlich auf, welche Identifizierungsdaten gesammelt und auf Vorrat gespeichert werden dürfen, um es den in Artikel 127/1 § 3 Absatz 1 erwähnten Behörden zu ermöglichen, die Teilnehmer durch eine indirekte Identifizierungsmethode zu identifizieren.

B.58.3.4. Artikel 127 legt die maximale Speicherfrist für die darin erwähnten Identifizierungsdaten fest. Paragraph 4 Absatz 4 dieser Bestimmung sieht vor, dass diese bis zu zwölf Monate nach dem Ende des elektronischen Kommunikationsdienstes auf Vorrat gespeichert werden, es sei denn, eine Gesetzesbestimmung sieht eine andere Frist vor.

B.58.3.5. Außerdem verbietet es Artikel 127 den Verkaufsstellen ausdrücklich, Identifizierungsdaten oder Kopien von Identifizierungsdokumenten aufzubewahren, sondern sie müssen diese Daten und Kopien direkt in ihre Datenverarbeitungssysteme eingeben, wobei es Aufgabe der Betreiber ist, die geeigneten und verhältnismäßigen technischen und

organisatorischen Maßnahmen zu ergreifen, um das vorerwähnte Verbot umzusetzen, auch indem sie die sofortige Eingabe der Daten und Kopien in die Datenverarbeitungssysteme ermöglichen (§ 4 Absätze 1 und 2). Eine Ausnahme ist im Fall des Ausfalls des Datenverarbeitungssystems, die die vorerwähnte sofortige Eingabe unmöglich macht, vorgesehen. In diesem Fall dürfen die Verkaufsstellen die Daten und die Kopien unter der Bedingung zeitweilig aufbewahren, dass diese spätestens nach der Aktivierung des elektronischen Kommunikationsdienstes vernichtet werden (§ 4 Absatz 3).

B.58.3.6. Schließlich ist vorgesehen, dass es dem Betreiber, wenn er die nach Artikel 127 des Gesetzes vom 13. Juni 2005 auferlegten Maßnahmen nicht einhält, verboten ist, den Dienst bereitzustellen, für den die fraglichen Maßnahmen nicht ergriffen worden sind (Artikel 127 § 12 Absatz 1 des Gesetzes vom 13. Juni 2005).

B.58.3.7. Im Übrigen ist es zwar richtig, dass Artikel 127 des Gesetzes vom 13. Juni 2005 Artikel 127 des Gesetzes vom 13. Juni 2005 sieht keine spezifische richterliche Kontrolle bezüglich der Verarbeitung der aufgrund dieser Bestimmung gesammelten und auf Vorrat gespeicherten Identifizierungsdaten vorsieht, aber es ist darauf hinzuweisen, wie in B.56 erwähnt, dass die gemeinrechtlichen Rechtsmittel bei der Verarbeitung von bloßen Identifizierungsdaten ausreichen (EuGHMR, 30. Januar 2020, *Breyer gegen Deutschland*, vorerwähnt, § 106).

Im Rahmen eines Strafverfahrens verfügt der Angeklagte in diesem Zusammenhang über das Recht, vor den Untersuchungsgerichten oder dem erkennenden Gericht die Nichtigkeit einer Untersuchungshandlung geltend zu machen, die sein Recht auf Achtung des Privatlebens oder sein Reicht auf ein faires Verfahren verletzt.

Im Rahmen der Arbeit der Nachrichten- und Sicherheitsdienste verfügt die betroffene Person nach Artikel 79 des Gesetzes vom 30. Juli 2018 « über den Schutz natürlicher Personen hinsichtlich der Verarbeitung personenbezogener Daten » ferner über das Recht, beim Ständigen Ausschuss N zu beantragen, dass ihre unrichtigen personenbezogenen Daten berichtigt oder gelöscht werden und dass die Einhaltung der einschlägigen Bestimmungen überprüft wird.

Zudem verfügt jeder Teilnehmer eines elektronischen Kommunikationsdienstes, dessen Identifizierungsdaten in Widerspruch zu Artikel 127 des Gesetzes vom 13. Juni 2005 verarbeitet wurden, über eine gemeinrechtliche Haftpflichtklage gegen die Person, die gegen diese Gesetzesbestimmung verstoßen hat.

Schließlich kann die betroffene Person im Falle einer unrechtmäßigen Verarbeitung ihrer personenbezogenen Daten nach Artikel 58 des Gesetzes vom 3. Dezember 2017 « zur Schaffung der Datenschutzbehörde » kostenlos eine Beschwerde bei der Datenschutzbehörde einreichen.

B.59. Der erste und der zweite Klagegrund in der Rechtssache Nr. 7930 sind unbegründet, insofern sie sich auf die in Artikel 127 §§ 6 bis 8 und 10 Absatz 1 Nrn. 2 bis 6 des Gesetzes vom 13. Juni 2005 erwähnten Daten beziehen.

B.60. Artikel 127 § 11 Absatz 1 des Gesetzes vom 13. Juni 2005 bestimmt, dass « außer im Fall des Gegenbeweises […] davon ausgegangen [wird], dass die identifizierte Person den elektronischen Kommunikationsdienst selbst nutzt ».

Nach Auffassung der klagenden Parteien in der Rechtssache Nr. 7932 verstößt diese Bestimmung gegen das Recht auf ein faires Verfahren, insbesondere gegen die von Artikel 6 der Europäischen Menschenrechtskonvention gewährleistete Unschuldsvermutung, insofern der vermutete Endnutzer vor der Unmöglichkeit steht, den Gegenbeweis zu erbringen, insbesondere wenn dieser Nutzer der Öffentlichkeit den Zugriff auf sein WLAN-Netz erlaubt oder im Fall eines unbefugten Zugriffs auf dieses Netz.

B.61.1. Aufgrund von Artikel 6 Absatz 2 der Europäischen Menschenrechtskonvention gilt jede Person, die einer Straftat angeklagt ist, bis zum gesetzlichen Beweis ihrer Schuld als unschuldig.

B.61.2. Als Verfahrensgarantie in Strafsachen stellt die Unschuldsvermutung Anforderungen an - unter anderem - die Beweislast, gesetzliche Vermutungen faktischer und rechtlicher Art, das Recht, sich nicht selbst zu belasten, Bekanntgabe vor dem Prozess und voreilige Äußerungen von Richtern oder anderen Amtsträgern zur Schuld eines Beschuldigten

(EuGHMR, Große Kammer, 12. Juli 2013, *Allen gegen Vereinigtes Königreich,* ECLI:CE:ECHR:2013:0712JUD002542409, § 93).

B.61.3. Das Recht jeder Person, die einer Straftat angeklagt ist, als unschuldig zu gelten und zu verlangen, dass die Staatsanwaltschaft die Beweislast trägt, ist jedoch nicht absolut. In jedem Rechtssystem gibt es nämlich gesetzliche Vermutungen faktischer oder rechtlicher Art. Solche Vermutungen sind grundsätzlich nicht verboten, solange sie sich in angemessenen Grenzen halten, unter Berücksichtigung der schwerwiegenden Beschaffenheit der Sache und der Beachtung der Rechte der Verteidigung. Beim Rückgriff auf Vermutungen in Strafsachen muss also ein gerechtes Gleichgewicht zwischen der Bedeutsamkeit der Sache und der Rechte der Verteidigung gefunden werden. Die eingesetzten Mittel müssen – mit anderen Worten – im Verhältnis zur verfolgten legitimen Zielsetzung stehen (EuGHMR, Entscheidung, 19. Oktober 2004, *Falk gegen Niederlande*, ECLI:CE:ECHR:2004:1019DEC006627301; 23. Juli 2002, *Västberga Taxi Aktiebolag und Vulic gegen Schweden*, ECLI:CE:ECHR:2002:0723JUD003698597, § 113).

B.62.1. Artikel 127 § 11 Absatz 1 des Gesetzes vom 13. Juni 2005 führt keine automatische strafrechtliche Verantwortung oder objektive Haftung des identifizierten Endnutzers einer Mobiltelefon-Guthabenkarte für die Nutzung dieser Karte durch einen Dritten ein. Er hat in erster Linie eine Warnfunktion, da er die Ausgangsvermutung jeder strafrechtlichen Untersuchung und jeder Untersuchung durch die Nachrichten- und Sicherheitsdienste in Erinnerung ruft, nämlich die Vermutung, dass jeder Eigentümer oder jeder gewöhnliche Nutzer eines Gegenstandes derjenige ist, der ihn benutzt hat, um eine Straftat zu begehen oder die nationale Sicherheit zu gefährden. Die Ermittlungspersonen nehmen von dieser Vermutung Abstand, sobald sie durch die gesammelten Beweiselemente widerlegt ist.

B.62.2. Die angefochtene Bestimmung hängt daher mit den in B.54 erwähnten Zielen zusammen, die der Gesetzgeber mit Artikel 127 des Gesetzes vom 13. Juni 2005 verfolgt.

B.62.3. Außerdem verfügt der vermutete Endnutzer über verschiedene Möglichkeiten, um sich gegen strafrechtliche Verfolgungen zu verteidigen, die sich aus der Nutzung des elektronischen Kommunikationsdienstes durch einen Dritten ergeben könnten. Wenn er den Ermittlungspersonen mitteilt, wer diesen Dienst benutzt hat, müssen sie die Beteiligung dieser Person untersuchen. In dem Fall, dass der elektronische Kommunikationsdienst Dritten

zugänglich gemacht wird, obliegt es dem vermuteten Endnutzer, dies den Ermittlungspersonen mitzuteilen, die versuchen müssen, die Person, die den Dienst tatsächlich benutzt hat, sowie ihre Beteiligung zu ermitteln.

Artikel 127, § 11 Absatz 1 des Gesetzes vom 13. Juni 2005 regelt im Übrigen nur eine widerlegbare Vermutung, die der Angeklagte mit allen rechtlichen Mitteln widerlegen kann. Er verbietet ihm nicht, alle tatsächlichen Elemente vorzubringen, die seine Beteiligung an den begangenen Straftaten oder an den untersuchten Bedrohungen für die nationale Sicherheit widerlegen.

Ferner lässt die angefochtene Bestimmung den Grundsatz unberührt, dass es in einem Strafprozess der Staatsanwaltschaft obliegt, die Schuld des Angeklagten zu beweisen. Es ist Aufgabe des Strafrichters, den Beweiswert aller Beweiselemente einschließlich der Erläuterungen des Angeklagten zu untersuchen und dabei dessen Recht auf ein faires Verfahren zu beachten.

B.62.4. Artikel 127 § 11 Absatz 1 des Gesetzes vom 13. Juni 2005 stellt die Unschuldsvermutung nicht in Frage.

B.63. Der sechste Teil des zweiten Klagegrunds in der Rechtssache Nr. 7932 ist unbegründet.

B.64. Artikel 127 § 5 Absatz 4 des Gesetzes vom 13. Juni 2005 sieht vor, dass der Betreiber oder die Verkaufsstelle, um die Verlässlichkeit der Identifizierung des Teilnehmers, der eine natürliche Person ist, sicherzustellen und Identitätsbetrug zu verhindern, automatisch einen Vergleich zwischen den biometrischen Merkmalen auf dem Foto des Identifizierungsdokuments des Teilnehmers einerseits und den Merkmalen seines Gesichts andererseits durchführen kann.

Nach Auffassung der klagenden Parteien in der Rechtssache Nr. 7932 erlaubt diese Bestimmung den Einsatz einer Gesichtserkennungstechnologie, der gegen das Recht auf Achtung des Privatlebens und auf Schutz personenbezogener Daten, wie es insbesondere von der DSGVO gewährleistet ist, verstößt, insofern diese Maßnahme weder notwendig noch

verhältnismäßig sei und auch nicht das Erfordernis der ausdrücklichen und in Kenntnis der Sachlage erteilten Einwilligung des betroffenen Teilnehmers beachte.

B.65.1. Das Recht auf Achtung des Privatlebens ist kein absolutes Recht. Artikel 22 der Verfassung und Artikel 8 der Europäischen Menschenrechtskonvention schließen eine Einmischung der Behörden in die Ausübung dieses Rechts nicht aus, sofern eine solche durch eine ausreichend präzise gesetzliche Bestimmung vorgesehen ist, sie einem zwingenden gesellschaftlichen Bedürfnis in einer demokratischen Gesellschaft entspricht und sie im Verhältnis zu dem damit angestrebten rechtmäßigen Ziel steht.

Der Gesetzgeber verfügt in dem Zusammenhang über einen Ermessensspielraum. Dieser Ermessensspielraum ist gleichwohl nicht grenzenlos; damit eine Norm sich mit dem Recht auf Achtung des Privatlebens vereinbaren lässt, ist es erforderlich, dass der Gesetzgeber ein gerechtes Gleichgewicht zwischen allen betroffenen Rechten und Interessen schafft.

B.65.2. Zudem haben die Artikel 7 und 8 der Charta, wie in B.11.2 erwähnt, in Bezug auf die Verarbeitung personenbezogener Daten eine ähnliche Tragweite wie Artikel 8 der Europäischen Menschenrechtskonvention.

B.66.1. Artikel 5 der DSGVO führt die Grundsätze für die Verarbeitung personenbezogener Daten auf:

« (1) Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (‘ Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz ’);

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken (‘ Zweckbindung ’);

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (‘ Datenminimierung ’);

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die

Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden (‘ Richtigkeit ’);

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden (‘ Speicherbegrenzung ’);

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen (‘ Integrität und Vertraulichkeit ’);

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können (‘ Rechenschaftspflicht ’) ».

Artikel 9 der DSGVO bezieht sich auf die Verarbeitung besonderer Kategorien personenbezogener Daten:

« (1) Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.

(2) Absatz 1 gilt nicht in folgenden Fällen:

a) Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt, es sei denn, nach Unionsrecht oder dem Recht der Mitgliedstaaten kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden,

[…]

g) die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich,

[…] ».

Artikel 9 der Datenschutz-Grundverordnung ist in Verbindung mit Artikel 4 Nummer 14 der Datenschutz-Grundverordnung zu betrachten, der bestimmt:

« Im Sinne dieser Verordnung bezeichnet der Ausdruck:

[…]

14. ' biometrische Daten ' mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten ».

B.66.2. Artikel 9 Absatz 2 Buchstabe g der DSGVO gestattet die Verarbeitung von sensiblen personenbezogenen Daten wie zum Beispiel biometrischen Daten, wenn sie « auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist ».

B.67.1. Aus den Vorarbeiten zu Artikel 127 § 5 Absatz 4 des Gesetzes vom 20. Juli 2022 geht hervor, dass diese Bestimmung darauf abzielt, die möglichst effiziente Identifizierung von Personen zu ermöglichen, unter anderem um die Bekämpfung des Identitätsbetrugs sowohl seitens der Teilnehmer als auch der Verkaufsstellen selbst zu stärken (*Parl. Dok.*, Kammer, 2021-2022, DOC 55-2572/002, SS. 90 und 91).

B.67.2. In seinem Entscheid Nr. 2/2021 vom 14. Januar 2021 (ECLI:BE:GHCC:2021:ARR.002) hat der Gerichtshof entschieden, dass die vorerwähnten Ziele legitim sind, da sie darauf abzielen, die Rechte und Freiheiten anderer zu schützen, dass sie überdies dem Gemeinwohl dienende Ziele, die von der Union anerkannt sind, darstellen und dass sie ebenfalls als Gründe eines erheblichen öffentlichen Interesses im Sinne von Artikel 9 Absatz 2 Buchstabe g der DSGVO angesehen werden können (B.20.2).

B.68. Artikel 127 § 5 Absatz 4 des Gesetzes vom 13. Juni 2005 ist im Hinblick auf die Verwirklichung der verfolgten Ziele sachdienlich, da der Vergleich der biometrischen Merkmale auf dem Foto des Identifizierungsdokuments und den Merkmalen des Gesichts des

Teilnehmers einerseits die Aufgabe der Betreiber, alles dafür zu tun, die Verlässlichkeit der Identifizierung des Teilnehmers, der eine natürliche Person ist, sicherzustellen, erleichtern kann und andererseits die betrügerische Nutzung der erwähnten Identifizierungsdokumente verhüten kann.

Das etwaige Fehlen einer völligen Zuverlässigkeit des Verfahrens und die damit einhergehende Unmöglichkeit, es auszuschließen, dass bestimmte Fälle von Ähnlichkeitsbetrug nicht erkannt werden, führen nicht zu einer anderen Schlussfolgerung.

B.69. Die angefochtene Maßnahme des Gesichtsvergleichs ist außerdem von einer ausreichend präzisen Gesetzesbestimmung vorgesehen, da Artikel 127 § 5 Absatz 4 des Gesetzes vom 13. Juni 2005 die Daten bestimmt, die Gegenstand der strittigen Maßnahme sind, nämlich die biometrischen Merkmale auf dem Foto der in Artikel 127 § 6 dieses Gesetzes erwähnten Identifizierungsdokumente und die Merkmale des Gesichts des Teilnehmers, da es verboten ist, die vorerwähnten biometrischen Daten über das Vergleichsverfahren hinaus aufzubewahren, die Daten ausschließlich elektronisch lesbar sind und es nur den Betreibern und den Verkaufsstelle im Sinne des vorerwähnten Artikels 127 erlaubt ist, diese Daten zu lesen.

Auf diese Weise können die Teilnehmer, auf die diese Bestimmung abzielt, die Bedingungen, unter denen die vorerwähnten biometrischen Daten verarbeitet werden, in ausreichend präziser Weise kennen.

B.70. Der Gerichtshof prüft nun die Notwendigkeit und die Verhältnismäßigkeit der Einmischung.

B.71.1. Im Rahmen der Prüfung der Notwendigkeit ist zu prüfen, ob der Eingriff nicht über das hinausgeht, was zur Erreichung der verfolgten Ziele erforderlich ist und insbesondere ob es Maßnahmen gibt, die weniger stark in die betreffenden Rechte eingreifen und trotzdem den Zielen der in Rede stehenden Regelung wirksam dienen (EuGH, 17. Oktober 2013, C-291/12, *Schwarz gegen Stadt Bochum*, ECLI:EU:C:2013:670, Randnrn. 46-47).

B.71.2. Aus den Vorarbeiten zu der angefochtenen Bestimmung geht hervor, dass der Gesetzgeber den Standpunkt vertreten hat, dass die Maßnahme des Gesichtsvergleichs, die in

Artikel 127 § 5 Absatz 4 des Gesetzes vom 13. Juni 2005 vorgesehen ist, für die Verwirklichung der in B.67.1 erwähnten Ziele notwendig ist:

« La méthode de comparaison faciale est une bonne méthode pour atteindre les finalités visées par le gouvernement.

Avec cette méthode de reconnaissance faciale, les opérateurs peuvent réduire l'usurpation d'identité. Cette méthode permet aussi de ne pas faire intervenir les points de vente, qui sont les ' maillons faibles ' en matière de fiabilité de l'identification de l'abonné. Cette augmentation de la fiabilité de l'identification est bénéfique pour les autorités, pour les opérateurs, qui sont victimes des fraudes (d'où l'intérêt de plusieurs opérateurs de mettre en œuvre cette méthode) et pour l'abonné (éviter un détournement de son identité). Même si une personne parvient à s'identifier avec un faux document d'identification, la copie de ce document d'identification autre que la carte d'identité électronique belge comprendra une photo correcte de l'abonné, ce qui pourrait permettre aux autorités de démarrer une enquête.

La méthode de comparaison faciale permet aux opérateurs de répondre à leur obligation d'effectuer une identification fiable de l'abonné et de s'adapter aux besoins des abonnés (voir infra).

Il s'agit d'une méthode acceptable du point de vue de la vie privée, dès lors que les données de biométrie du visage ne sont pas conservées. Comme déjà indiqué, cela permet de ne pas faire intervenir les points de vente, qui sont parfois eux-mêmes à l'origine de fraude (ex. réutilisation frauduleuse de données d'identification d'une personne pour identifier une autre personne).

Cela permet aussi d'augmenter les possibilités pour un abonné de s'identifier et de faciliter son identification, en particulier pour les identifications en ligne. Pour de nombreux utilisateurs qui maîtrisent la technologie, c'est devenu une habitude quotidienne. La comparaison des paramètres biométriques d'un selfie et de la photo sur un document d'identité offre de nouvelles possibilités d'identification fiable. Cette solution en particulier peut fortement faciliter l'identification de clients, surtout en cas d'identification par smartphone, où l'utilisation du lecteur d'eID belge n'est pas possible » (*Parl. Dok.*, Kammer, 2021-2022, DOC 55-2572/002, SS. 90-91).

B.71.3. Diesbezüglich strebte der Gesetzgeber an, ein System einzuführen, das eine angemessene Antwort in jedem Einzelfall, insbesondere dem Fall der nicht belgischen Gebietsansässigen ohne elektronischen Personalausweis, dem Fall der zu Besuch in Belgien weilenden Ausländer oder auch dem Fall von mit der digitalen Welt nicht so vertrauten Personen, zulässt. Vor diesem Hintergrund heißt es in den Vorarbeiten zum Gesetz vom 20. Juli 2022, dass « die Identifizierung auf der Grundlage des Gesichtsvergleichs ergänzend ist und eine notwendige Zusatzmaßnahme zu den bestehenden Methoden darstellt » (ebenda, S. 84).

B.72.1. Was die Verhältnismäßigkeit der Maßnahme betrifft, legt Artikel 127 § 5 Absatz 4 des Gesetzes vom 13. Juni 2005 selbst mehrere Garantien zugunsten des von der Maßnahme des Gesichtsvergleichs betroffenen Teilnehmers fest.

Das Vergleichswerkzeug muss vom für Angelegenheiten bezüglich der elektronischen Kommunikation zuständigen Minister und vom Minister der Justiz nach der Prüfung, dass das Werkzeug unter Berücksichtigung des Risikos des Identitätsbetrugs eine zuverlässige Identifizierung sicherstellt, genehmigt werden (Nr. 1).

Außerdem bietet der Betreiber dem Teilnehmer mindestens eine andere Weise, sich zu identifizieren, an (Nr. 2), sodass der Teilnehmer nie gezwungen ist, auf die Methode der Gesichtserkennung zurückzugreifen, um einen elektronischen Kommunikationsdienst abzuschließen.

Sodann muss der Teilnehmer seine ausdrückliche Einwilligung im Sinne von Artikel 4 Nummer 11 der DSGVO erteilen (Nr. 3), wobei Artikel 9 Absatz 2 Buchstabe *a)* der DSGVO entgegen den Behauptungen der klagenden Parteien nicht verlangt, dass diese Einwilligung schriftlich gegeben wird.

Schließlich ist es den Betreibern und den Verkaufsstellen verboten, die verarbeiteten biometrischen Daten an einen Dritten weiterzugeben oder sie zu anderen Zwecken als der Identifizierung der Teilnehmer zu verarbeiten (Nr. 4).

B.72.2. Im Übrigen ist nicht ersichtlich, dass die angefochtene Maßnahme den Wesensgehalt des Rechts auf Achtung des Privatlebens und des Rechts auf Schutz personenbezogener Daten beeinträchtigen würde.

B.73. Der dritte Teil des zweiten Klagegrunds in der Rechtssache Nr. 7932 ist unbegründet.

7. Die gezielte Vorratsdatenspeicherung aufgrund eines geografischen Kriteriums (Artikel 9 bis 11)

B.74.1. Der erste, der zweite und der dritte Klagegrund in der Rechtssache Nr. 7930, der einzige Klagegrund in der Rechtssache Nr. 7931 und der dritte Teil des ersten Klagegrunds in der Rechtssache Nr. 7932 beziehen sich auf die Maßnahme der gezielten Vorratsspeicherung von Verkehrs- und Standortdaten, die in den Artikeln 9, 10 und 11 des Gesetzes vom 20. Juli 2022 vorgesehen ist.

B.74.2. Artikel 9 des Gesetzes vom 20. Juli 2022 fügt in das Gesetz vom 13. Juni 2005 einen Artikel 126/1 ein, der bestimmt:

« § 1er. Sans préjudice du RGPD et de la loi du 30 juillet 2018, les opérateurs qui offrent aux utilisateurs finaux des services de communications électroniques, ainsi que les opérateurs fournissant les réseaux de communications électroniques sous-jacents, conservent les données visées à l'article 126/2, § 2, pour les zones géographiques visées à l'article 126/3, pendant douze mois à partir de la date de la communication, sauf si une autre durée est fixée dans l'article 126/3.

Chaque opérateur conserve les données qu'il a générées ou traitées dans le cadre de la fourniture des services et réseaux de communications électroniques concernés.

Ces données sont conservées aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave, de la prévention de menaces graves contre la sécurité publique, et de la sauvegarde des intérêts vitaux d'une personne physique.

§ 2. Les métadonnées de communications électroniques, en ce compris les métadonnées pour les appels infructueux, auxquelles s'applique l'obligation de conservation visée au paragraphe 1er, sont énumérées à l'article 126/2, § 2.

§ 3. Les opérateurs conservent les données de trafic pour toutes les communications ou appels infructueux effectués à partir d'une zone géographique visée à l'article 126/3 ou vers une telle zone.

Lorsque, compte tenu de la technologie utilisée par l'opérateur, celui-ci n'est pas en mesure de localiser l'équipement terminal ayant participé à la communication, y compris l'appel infructueux, de façon plus précise que sa localisation sur le territoire national, l'opérateur conserve les données visées à l'article 126/2, § 2, pour la durée la plus courte fixée en exécution du présent article et de l'article 126/3, à la condition qu'en exécution du présent article et de l'article 126/3 l'ensemble du territoire national soit soumis à une obligation de conservation. Lorsque cette condition n'est pas remplie, l'opérateur concerné par le présent alinéa ne conserve pas ces données.

Lorsque l'utilisateur final se déplace pendant une communication électronique, l'opérateur conserve les données de trafic pour autant que l'utilisateur final se trouve à un moment de la communication dans une zone visée à l'article 126/3.

Les opérateurs conservent les données relatives à la connexion de l'équipement terminal au réseau et au service et à la localisation de cet équipement, y compris le point de terminaison du réseau, énumérées à l'article 126/2, § 2, lorsque cet équipement se trouve dans une zone visée à l'article 126/3.

Pour déterminer si l'équipement terminal se trouve dans une zone géographique visée à l'article 126/3, les opérateurs utilisent les données les plus fiables et précises possibles. Ils utilisent, si disponible à cet effet, la localisation satellitaire d'un équipement terminal.

Lorsque la technologie utilisée par l'opérateur ne permet pas de limiter la conservation de données à une zone visée à l'article 126/3, il conserve les données nécessaires pour couvrir la totalité de la zone concernée tout en limitant la conservation de données en dehors de cette zone au strict nécessaire au regard de ses possibilités techniques.

Lorsqu'un point d'agrégation de l'opérateur, telle une antenne, couvre plusieurs zones géographiques visées à l'article 126/3 qui sont soumises à des durées de conservation différentes, l'opérateur conserve les données pour ce point d'agrégation pendant la durée de conservation la plus courte.

Lorsqu'en application du présent article et de l'article 126/3, différentes durées de conservation sont applicables aux mêmes données, les opérateurs conservent les données pendant la durée la plus courte.

§ 4. Le Roi peut fixer, par arrêté délibéré en Conseil des ministres, sur proposition du ministre de la Justice, du ministre de l'Intérieur, du ministre de la Défense, et du ministre, et après avis des autorités de protection des données compétentes et de l'Institut, les éléments suivants :

- les paramètres techniques et les données que les opérateurs utilisent pour limiter la conservation de données aux zones visées à l'article 126/3;

- la liste des différentes autorités compétentes dans les matières visées à l'article 126/3, §§ 2 à 5;

- les modalités de communication des informations par les autorités compétentes au service désigné par le Roi, les modalités de communication des informations par ce service vers les opérateurs concernés, ainsi que le délai dans lequel les opérateurs mettent en œuvre annuellement la conservation visée au paragraphe 1er;

- s'il échet, les zones géographiques additionnelles visées à l'article 126/3, § 3, *m)*, § 4, *g)*, et § 5, *f)*.

L'arrêté royal visé à l'alinéa 1er, quatrième tiret, est renouvelé tous les trois ans. En l'absence de renouvellement, l'obligation de conservation visée au paragraphe 1er en ce qui concerne ces zones géographiques additionnelles cesse de s'appliquer, et ce jusqu'à l'entrée en vigueur d'un nouvel arrêté royal.

§ 5. Le ministre de la Justice, le ministre de l'Intérieur, le ministre de la Défense et le ministre présentent annuellement, après avis préalable du Comité de coordination du Renseignement et de la Sécurité, et de l'Institut et des autorités de protection des données compétentes, un rapport d'évaluation à la Chambre des représentants, sur la mise en œuvre du présent article et, le cas échéant, de l'arrêté royal visé au paragraphe 4, afin de vérifier si des dispositions doivent être adaptées.

Ce rapport d'évaluation examine en particulier si les catégories de zones géographiques énumérées dans la loi et dans l'arrêté royal visé au paragraphe 4 répondent toujours aux critères visés à l'article 126/3, §§ 3 à 5, et s'il est nécessaire de les maintenir ou si d'autres doivent être incluses.

Des catégories de zones géographiques ne peuvent être incluses que dans le but de sauvegarder la sécurité nationale ou s'il peut être établi, sur la base d'éléments objectifs et non discriminatoires, qu'il existe dans ces zones une situation présentant un risque élevé de préparation ou de commission d'actes criminels graves.

Le rapport d'évaluation comprend également le pourcentage du territoire national auquel s'applique l'obligation de conservation des données en vertu du présent article et de l'article 126/3.

Ce rapport d'évaluation est envoyé à l'Organe de contrôle de l'information policière et au Comité permanent R ».

B.74.3. Artikel 10 des Gesetzes vom 20. Juli 2022 fügt in das Gesetz vom 13. Juni 2005 einen Artikel 126/2 ein, der bestimmt:

« § 1er. Pour l'application du présent article, il y a lieu d'entendre par ' communication ', toute information échangée ou acheminée entre un nombre fini de parties au moyen d'un service de communications électroniques accessible au public, à l'exclusion des informations qui sont acheminées dans le cadre d'un service de radiodiffusion au public par l'intermédiaire d'un réseau de communications électroniques, sauf dans la mesure où un lien peut être établi entre l'information et l'abonné ou utilisateur identifiable qui la reçoit.

§ 2. Les données visées à l'article 126/1, § 2, qui doivent être conservées en exécution des articles 126/1 et 126/3 par les opérateurs qui offrent aux utilisateurs finaux des services de communications électroniques, ainsi que par les opérateurs fournissant les réseaux de communications électroniques sous-jacents qui permettent la fourniture de ces services, sont les suivantes :

1° la description et les caractéristiques techniques du service de communications électroniques utilisé lors de la communication;

2° les données d'identification visées à l'article 126, § 1er, 2°, 10° à 14°, et 16°, du destinataire de la communication;

3° pour les services de communications électroniques à l'exception des services d'accès à Internet, l'adresse IP utilisée par le destinataire de la communication, l'horodatage ainsi que, en cas d'utilisation partagée d'une adresse IP du destinataire, les ports qui lui ont été attribués;

4° en cas d'appel multiple, de déviation ou de renvoi, l'identification de toutes les lignes en ce compris celles vers lesquelles l'appel a été transféré;

5° la date et l'heure exacte du début et de la fin de la session du service de communications électroniques concerné, en ce compris la date et l'heure exacte du début et de la fin de l'appel;

6° les données permettant d'identifier et de localiser les cellules ou d'autres points de terminaison du réseau mobile, qui ont été utilisées pour effectuer la communication, du début jusqu'à la fin de la communication, ainsi que les dates et heures précises de ces différentes localisations;

7° le volume de données envoyées vers le réseau et téléchargées pendant la durée de la session;

8° pour ce qui concerne les services de communications électroniques mobiles, la date et l'heure de la connexion de l'équipement terminal au réseau en raison du démarrage de cet équipement et le moment de la déconnexion de cet équipement terminal au réseau en raison de l'extinction de cet équipement;

9° pour ce qui concerne les services de communications électroniques mobiles, la localisation de l'équipement terminal et la date et l'heure de cette localisation chaque fois que l'opérateur cherche à connaître quels équipements terminaux sont connectés à son réseau;

10° les autres identifiants relatifs au destinataire de la communication électronique, à son équipement terminal ou à l'équipement le plus proche de cet équipement terminal, qui résultent de l'évolution technologique et qui sont déterminés par le Roi, après avis de l'Autorité de protection des données et de l'Institut, pour autant que cet arrêté soit confirmé par la loi dans les six mois suivant la publication de cet arrêté.

Par dérogation aux articles 126/1 et 126/3, la durée de conservation de la donnée visée à l'alinéa 1er, 8°, est de six mois après avoir été générée ou traitée.

L'arrêté royal visé à l'alinéa 1er, 10°, ne porte pas sur le contenu des communications électroniques.

Le Roi peut, après avis de l'Autorité de protection des données et de l'Institut, préciser les données visées à l'alinéa 1er.

§ 3. La combinaison des données conservées en exécution de l'article 126 et du présent article doit permettre d'établir la relation entre l'origine de la communication et sa destination.

Le Roi peut fixer, par arrêté délibéré en Conseil des ministres, sur proposition du ministre de la Justice, du ministre de l'Intérieur, du ministre de la Défense, et du ministre, après avis des autorités de protection des données compétentes et de l'Institut, les exigences en matière de précision et de fiabilité auxquelles les données visées au présent article doivent répondre ».

B.74.4. Artikel 11 des Gesetzes vom 20. Juli 2022 fügt in das Gesetz vom 13. Juni 2005 einen Artikel 126/3 ein, der bestimmt:

« § 1er. Les données visées à l'article 126/2, § 2, sont conservées dans la zone géographique composée des :

- arrondissements judiciaires dans lesquels au moins trois infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par 1 000 habitants par an ont été constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;

- zones de police dans lesquelles au moins trois infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par 1 000 habitants par an ont été constatées sur une moyenne des trois années calendriers qui précèdent celle en cours, et situées dans les arrondissements judiciaires dans lesquels pendant l'année calendrier qui précède celle en cours, moins de trois infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par 1 000 habitants par an sur une moyenne de trois années calendriers qui précèdent celle en cours ont été constatées.

Dans l'hypothèse visée à l'alinéa 1er, premier tiret, le délai de conservation des données visées à l'article 126/2, § 2, est de :

a) six mois, s'il y a trois ou quatre infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;

b) neuf mois, s'il y a cinq ou six infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;

c) douze mois, s'il y a sept ou plus de sept infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours.

Dans l'hypothèse visée à l'alinéa 1er, deuxième tiret, le délai de conservation des données visées à l'article 126/2, § 2, est de :

a) six mois, s'il y a trois ou quatre infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;

b) neuf mois, s'il y a cinq ou six infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours;

c) douze mois, s'il y a sept ou plus de sept infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours.

Le nombre d'infractions ainsi déterminé est arrondi à l'unité supérieure ou inférieure, selon que le chiffre de la première décimale atteint ou non cinq.

Les statistiques relatives au nombre d'infractions visées à l'article 90*ter*, §§ 2 à 4, du Code d'instruction criminelle par an par 1 000 habitants constatées sur une moyenne des trois années calendriers qui précèdent celle en cours sont issues de la Banque de données Nationale Générale visée à l'article 44/7 de la loi du 5 août 1992 sur la fonction de police.

Les périmètres des arrondissements judiciaires visés à l'alinéa 1er, premier tiret, sont fixés par l'article 4 de l'annexe au Code judiciaire.

Les périmètres des zones de police visées à l'alinéa 1er, deuxième tiret, sont ceux fixés à l'annexe de l'arrêté royal du 24 octobre 2001 portant la dénomination des zones de police.

La direction, visée à l'article 44/11 de la loi du 5 août 1992 sur la fonction de police, envoie les statistiques relatives au nombre d'infractions et la durée de conservation pour chaque arrondissement judiciaire et chaque zone de police à l'Organe de contrôle de l'information policière, qui, dans le mois, après que toutes les données nécessaires à cette fin lui aient été communiquées, procède à leur validation. L'Organe de contrôle peut exercer, aux fins de cette validation, toutes ses compétences octroyées par le titre 7 de la loi du 30 juillet 2018.

Les statistiques et les durées de conservation sont transmises par la direction visée à l'article 44/11 de la loi du 5 août 1992 sur la fonction de police au service désigné par le Roi, uniquement après avoir été informé de leur validation par l'Organe de contrôle.

Sur proposition du service désigné par le Roi, chaque année, les ministres de la Justice et de l'Intérieur adoptent la liste des arrondissements judiciaires et des zones de police soumises à l'obligation de conservation de données ainsi que leur durée de conservation.

Après cette adoption, le service désigné par le Roi transmet la liste des arrondissements judiciaires et des zones de police soumises à l'obligation de conservation de données, ainsi que leur durée de conservation, aux opérateurs.

§ 2. Les données visées à l'article 126/2, § 2, sont conservées dans les zones géographiques déterminées par l'Organe de coordination pour l'analyse de la menace, dont le niveau de la menace, déterminé par l'évaluation visée à l'article 8, 1° et 2°, de la loi du 10 juillet 2006 relative à l'analyse de la menace, est au moins de niveau 3, conformément à l'article 11 de l'arrêté royal du 28 novembre 2006 portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace, et, aussi longtemps que le niveau de la menace d'au moins niveau 3 perdure pour ces zones.

Si le niveau de la menace est au moins de niveau 3 et couvre l'ensemble du territoire, l'Organe de coordination pour l'analyse de la menace informe immédiatement le service désigné par le Roi afin que ce service prenne les mesures nécessaires pour informer les opérateurs et procéder à une conservation générale et indifférenciée des données visées à l'article 126/2, § 2, sur l'ensemble du territoire.

L'obligation de conservation visée à l'alinéa 2 est confirmée par arrêté royal, sur proposition conjointe du ministre de l'Intérieur et du ministre de la Justice. En l'absence de confirmation par arrêté royal, publié dans le mois de la décision visée à l'alinéa 2, la

conservation de données prend fin et les opérateurs en sont avertis par le service désigné par le Roi le plus rapidement possible. Après cette notification, les opérateurs suppriment les données qui ont déjà été conservées à cette fin.

§ 3. Les données visées à l'article 126/2, § 2, sont conservées dans les zones particulièrement exposées à des menaces pour la sécurité nationale ou à la commission d'actes de criminalité grave, à savoir :

a) les installations portuaires, les ports et les zones de sûreté portuaire visées à l'article 2.5.2.2, 3° à 5°, du Code de la Navigation belge;

b) les gares au sens de l'article 2, 5°, de la loi du 27 avril 2018 sur la police des chemins de fer;

c) les stations de métro et de pré-métro;

d) les aéroports au sens de l'article 2, point 1), de la directive 2009/12/CE du Parlement européen et du Conseil du 11 mars 2009 sur les redevances aéroportuaires, y compris les aéroports du réseau central énumérés à l'annexe II, section II, du règlement (UE) n° 1315/2013 du Parlement européen et du Conseil du 11 décembre 2013 sur les orientations de l'Union pour le développement du réseau transeuropéen de transport et abrogeant la décision n° 661/2010/UE, et les entités exploitant les installations annexes se trouvant dans les aéroports;

e) les bâtiments affectés à l'administration des douanes et accises;

f) les prisons au sens de l'article 2, 15°, de la loi de principes du 12 janvier 2005 concernant l'administration pénitentiaire ainsi que le statut juridique des détenus, les centres communautaires pour mineurs ayant commis un fait qualifié infraction, visés à l'article 606 du Code d'instruction criminelle, et les centres de psychiatrie légale, visés à l'article 3, 4°, *c)*, de la loi du 5 mai 2014 relative à l'internement;

g) les armuriers et les stands de tir au sens de l'article 2, 1° et 19°, de la loi du 8 juin 2006 réglant des activités économiques et individuelles avec des armes;

h) les établissements visés à l'article 3.1.*a)*, de l'arrêté royal du 20 juillet 2001 portant règlement général de la protection de la population, des travailleurs et de l'environnement contre le danger des rayonnements ionisants;

i) les établissements visés à l'article 2, 1°, de l'accord de coopération du 16 février 2016 entre l'État fédéral, la Région flamande, la Région wallonne et la Région de Bruxelles-Capitale concernant la maîtrise des dangers liés aux accidents majeurs impliquant des substances dangereuses;

j) les communes dans lesquelles il y a un ou plusieurs éléments critiques du réseau ou une ou plusieurs infrastructures critiques, visés dans la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques et ses arrêtés d'exécution; lorsque l'ensemble du réseau a été identifié comme infrastructure critique, seuls les éléments critiques du réseau sont pris en compte pour l'application du présent article;

k) le siège de la SA Astrid et les bâtiments où sont situés ses centres de données centraux et provinciaux ainsi que les bâtiments où sont situés les centres de données centraux et les nœuds de communication du système de communication et d'informations sécurisé et crypté visé à l'article 11, § 7, de l'arrêté royal du 28 novembre 2006 portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace;

l) les systèmes de réseau et d'information qui soutiennent la fourniture des services essentiels des fournisseurs de service essentiels désignés sur la base de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique;

m) le cas échéant, sans préjudice de l'article 126/1, § 5, alinéa 3, les autres zones particulièrement exposées à des menaces pour la sécurité nationale ou à la commission d'actes de criminalité grave fixées par arrêté royal.

§ 4. Les données visées à l'article 126/2, § 2, sont conservées dans les zones où il y a une menace grave potentielle pour les intérêts vitaux du pays ou pour les besoins essentiels de la population, à savoir :

a) en matière d'ordre public, les zones neutres au sens de l'article 3 de la loi du 2 mars 1954 tendant à prévenir et réprimer les atteintes au libre exercice des pouvoirs souverains établis par la Constitution, et les organes stratégiques ministériels;

b) pour ce qui concerne le potentiel scientifique et économique, les bâtiments affectés aux personnes morales dont le potentiel économique et/ou scientifique doit être protégé et repris sur une liste établie annuellement par la Sûreté de l'État et le Service général du Renseignement et de la Sécurité sur proposition du ministre de la Justice et du ministre de la Défense et approuvée par le Conseil national de sécurité;

c) pour le transport, les autoroutes et les parkings publics attenants;

d) pour ce qui concerne la souveraineté nationale et les institutions établies par la Constitution et les lois, les décrets ou les ordonnances :

i) les assemblées législatives visées à l'article 1er de la loi du 2 mars 1954 tendant à prévenir et réprimer les atteintes au libre exercice des pouvoirs souverains établis par la Constitution;

ii) les maisons communales et les hôtels de ville;

iii) le palais royal;

iv) les domaines royaux;

v) les bâtiments affectés aux institutions visées au titre III, chapitres 5 à 7, de la Constitution;

vi) les communes dans lesquelles se trouvent des domaines militaires;

vii) les bâtiments affectés à la police locale, à la police fédérale, ainsi qu'à la Sûreté de l'État;

e) pour ce qui concerne l'intégrité du territoire national, les communes frontalières;

f) pour ce qui concerne les intérêts économiques ou financiers importants, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale :

i) les hôpitaux visés à l'article 2 de la loi coordonnée du 10 juillet 2008 sur les hôpitaux et autres établissements de soins;

ii) la Banque nationale de Belgique;

g) le cas échéant, et sans préjudice de l'article 126/1, § 5, alinéa 3, les autres zones où il y a une menace grave potentielle pour les intérêts vitaux du pays ou pour les besoins essentiels de la population fixées par arrêté royal.

§ 5. Les données visées à l'article 126/2, § 2, sont conservées dans les zones où il y a une menace potentielle grave pour les intérêts des institutions internationales établies sur le territoire national, à savoir :

a) les ambassades et les représentations diplomatiques;

b) les bâtiments affectés à l'Union européenne;

c) les bâtiments et infrastructures affectés à l'OTAN;

d) les institutions de l'Espace économique européen;

e) les institutions des Nations Unies;

f) le cas échéant, et sans préjudice de l'article 126/1, § 5, alinéa 3, les autres zones où il y a une menace potentielle grave pour les intérêts des institutions internationales établies sur le territoire national fixées par arrêté royal.

§ 6. Pour chaque catégorie de zone visée aux paragraphes 3 à 5, le Roi détermine l'étendue du périmètre de la zone.

Chaque autorité compétente dans l'une des matières visées aux paragraphes 3 à 5, transmet chaque année à la date déterminée par le Roi, uniquement au service désigné par le Roi, les informations nécessaires à la détermination concrète des zones géographiques.

Ces autorités informent sans délai uniquement ce service lorsqu'une zone géographique ne correspond plus au critère concerné afin qu'il soit mis fin le plus rapidement possible à l'obligation de conservation visée à l'article 126/1, § 1er, dans cette zone.

À l'exception de la liste des lieux visés au paragraphe 4, *b)*, mise exclusivement à la disposition du Comité permanent R par les services de renseignement et de sécurité, le service désigné par le Roi tient à la disposition de l'Organe de contrôle de l'information policière et du

Comité permanent R, chacun dans le cadre de ses compétences, la liste actualisée des zones visées aux paragraphes 3 à 5, où une conservation de données est obligatoire.

L'Organe de contrôle de l'information policière et le Comité permanent R peuvent, chacun dans le cadre de ses compétences, formuler des recommandations à l'égard de cette liste ou ordonner de manière motivée que certaines zones géographiques visées aux paragraphes 3 à 5 soient retirées de la liste.

Sur proposition du service désigné par le Roi, chaque année et lors de chaque modification visée à l'alinéa 5, le ministre de la Défense, le ministre de la Justice et le ministre de l'Intérieur adoptent la liste des zones géographiques soumises à l'obligation de conservation des données ainsi que leur durée de conservation.

L'arrêté ministériel visé à l'alinéa 6 est publié par voie de mention au *Moniteur belge*.

Après cette approbation, le service désigné par le Roi transmet la liste des zones géographiques soumises à l'obligation de conservation des données, ainsi que leur durée de conservation, aux opérateurs.

Toute personne qui, du chef de sa fonction, a connaissance des données communiquées par les autorités compétentes au service désigné par le Roi ou de la liste des zones géographiques soumises à l'obligation de conservation des données, ou prête son concours à la mise en œuvre du présent article, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal ».

B.75.1. Die klagende Partei in der Rechtssache Nr. 7930 leitet einen ersten, einen zweiten und einen dritten Klagegrund ab aus einem Verstoß gegen die Artikel 11, 12, 22 und 29 der Verfassung, gegen Artikel 15 Absatz 1 und gegen die Artikel 5, 6 und 9 der Richtlinie 2002/58/EG, gelesen im Lichte der Artikel 7, 8, 11, 47 und 52 Absatz 1 der Charta, der Artikel 6, 8, 10, 11 und 18 der Europäischen Menschenrechtskonvention und der Artikel 13 und 54 der Richtlinie (EU) 2016/680. Nach ihrer Auffassung führen die Artikel 9 bis 11 des Gesetzes vom 20. Juli 2022 eine allgemeine Vorratsspeicherungspflicht für Kommunikationsdaten ein, ohne dass diese Vorratsspeicherung notwendig erscheine oder im Hinblick auf das verfolgte Ziel strikt begrenzt sei. Sie führt an, dass Artikel 9 widersprüchlich sei, was die Zwecke der Vorratsspeicherung, die darin aufgeführt seien, betreffe. Außerdem behauptet sie in Bezug auf Artikel 11, dass diese Bestimmung *de facto* eine Vorratsspeicherung im gesamten belgischen Staatsgebiet erlaube, dass die Vorratsdatenspeicherung im Rahmen der nationalen Sicherheit auf der Grundlage der vom KOBA festgelegten Bedrohungsstufe nicht Gegenstand einer unabhängigen Prüfung sei und dass diese Stufe nicht die vom Gerichtshof der Europäischen Union geforderte Schwelle erreiche, dass die vorgesehenen Speicherfristen nicht auf das absolut Notwendige beschränkt seien, dass das System der Gebiete, die auf der Grundlage der Rate der Straftaten bestimmt würden, weder sachdienlich noch verhältnismäßig

sei, insbesondere, was den Begriff der « schweren Kriminalität » und das herangezogene Statistiksystem betreffe, und schließlich dass die erwähnten spezifischen Gebiete in Wirklichkeit das gesamte belgische Staatsgebiet abdeckten. Die klagende Partei beanstandet auch den Umstand, dass die Abgrenzung der Gebiete vom König festgelegt werde, was gegen das formelle Legalitätsprinzip verstoße.

B.75.2. Die klagende Partei in der Rechtssache Nr. 7931 leitet einen einzigen Klagegrund ab aus einem Verstoß gegen die Artikel 11, 12, 22 und 29 der Verfassung, an sich oder in Verbindung mit den Artikeln 7, 8, 11, 47 und 52 Absatz 1 der Charta, mit Artikel 8 der Europäischen Menschenrechtskonvention, mit den Artikeln 5, 6 und 15 der Richtlinie 2002/58/EG und mit den Artikeln 13 und 54 der Richtlinie (EU) 2016/680.

Was die Gebiete mit einer hohen Rate an schwerer Kriminalität betrifft, führt die klagende Partei an, dass die Artikel 9 bis 11 des Gesetzes vom 20. Juli 2022 die Vorratsdatenspeicherung während eines Zeitraums vorsähen, der nicht dem Grundsatz der Notwendigkeit entspreche, und dass sie sich auf einige Straftaten bezögen, die zur gewöhnlichen Kriminalität gehörten. Diesbezüglich beantragt die klagende Partei hilfsweise, dem Gerichtshof der Europäischen Union eine Vorabentscheidungsfrage zu stellen. Sie fügt hinzu, dass sich die herangezogenen Statistiken auf die Qualifizierung der Tatbestände zu Beginn der Untersuchung und nicht auf die Straftaten, die zu einer strafrechtlichen Verurteilung führten, bezögen, was nicht sachdienlich sei, und dass es dem König obliege, die Abgrenzung des Gebiets festzulegen, was nicht mit dem formellen Legalitätsprinzip vereinbar sei.

Was die Gebiete mit einer Bedrohung für die nationale Sicherheit betrifft, bestreitet die klagende Partei die herangezogene Bedrohungsstufe, die nicht mit den Anforderungen des Gerichtshofes der Europäischen Union in Einklang stehe, und beanstandet den Umstand, dass Daten zu anderen Zwecken als dem Schutz der nationalen Sicherheit auf Vorrat gespeichert werden dürften. Die klagende Partei bemängelt auch das Fehlen einer wirksamen durch eine unabhängige Behörde ausgeübten Kontrolle sowie die Möglichkeit des Königs, die Abgrenzung der Gebiete festzulegen und die Liste der Gebiete zu ergänzen, was nicht mit dem formellen Legalitätsprinzip vereinbar sei.

Was die Maßnahmen betrifft, die von den Betreibern ergriffen werden können, ist die klagende Partei der Auffassung, dass Artikel 9 des Gesetzes vom 20. Juli 2022 eine

umfassendere Vorratsdatenspeicherung erlaubt, wenn der Betreiber nicht in der Lage ist, den Standort der Nutzer festzustellen oder die Vorratsspeicherung auf das betroffene Gebiet zu begrenzen, was nicht verhältnismäßig sei.

B.75.3. Die klagenden Parteien in der Rechtssache Nr. 7932 leiten einen ersten Klagegrund ab aus einem Verstoß gegen die Artikel 10, 11, 13, 15, 22, 23 und 29 der Verfassung, an sich oder in Verbindung mit den Artikeln 5, 6, 8, 9, 10, 11, 14 und 18 der Europäischen Menschenrechtskonvention, mit den Artikeln 7, 8, 11, 47 und 52 der Charta, mit Artikel 5 Absatz 4 des Vertrags über die Europäische Union, sowie mit Artikel 6 der Richtlinie 2002/58/EG, mit der Richtlinie (EU) 2016/680 und mit der DSGVO.

Im dritten Teil dieses Klagegrunds führen die klagenden Parteien an, dass die in den Artikeln 9, 10 und 11 des Gesetzes vom 20. Juli 2022 vorgesehenen Maßnahmen zur Vorratsdatenspeicherung *de facto* eine unterschiedslose Vorratsdatenspeicherung zur Folge habe. Diesbezüglich stellen sie fest, dass in diesen Bestimmungen im Gegensatz zu dem, was vom Gerichtshof der Europäischen Union gefordert wird, keine Unterscheidung nach den Zwecken, die sie verfolgen, vorgenommen wird. Die klagenden Parteien führen außerdem an, dass die von den angefochtenen Bestimmungen vorgesehene Speicherfrist für die Daten unverhältnismäßig sei und dass diese Bestimmungen eine Speicherung außerhalb des betreffenden geografischen Gebiets erlaubten. Zudem behaupten sie, dass die verschiedenen geografischen Gebiete, die in Artikel 11 des Gesetzes vom 20. Juli 2022 aufgezählt sind, zu groß seien und nicht den Grundsatz der Notwendigkeit einhielten. Sie beanstanden ebenfalls das Fehlen einer wirksamen Beschwerde gegen die in den Artikeln 9 bis 11 des Gesetzes vom 20. Juli 2022 vorgesehene Maßnahme der Vorratsspeicherung sowie die Ermächtigung des Königs, die Abgrenzung der Gebiete festzulegen. Schließlich sind laut den klagenden Parteien die zusätzlichen Vorratsspeicherungspflichten, die in Artikel 9 des Gesetzes vom 20. Juli 2022 für die OTT-Dienste vorgesehen sind, nicht verhältnismäßig.

B.76. Die Beschwerdegründe der klagenden Parteien sind hauptsächlich aus einem Verstoß gegen das Recht auf Achtung des Privatlebens und das Recht auf Schutz personenbezogener Daten abgeleitet, die in Artikel 22 der Verfassung, in Artikel 8 der Europäischen Menschenrechtskonvention, in den Artikeln 7, 8 und 52 Absatz 1 der Charta, in der Richtlinie 2002/58/EG, in der Richtlinie (EU) 2016/680 und in der DSGVO gewährleistet sind.

B.77. Der Gerichtshof der Europäischen Union hat in seinem vorerwähnten Urteil vom 6. Oktober 2020 geurteilt, dass die Pflicht zur Vorratsspeicherung von Daten über die elektronische Kommunikation die Ausnahme und nicht die Regel sein muss.

B.78.1.1. Die Artikel 126/1 bis 126/3 des Gesetzes vom 13. Juni 2005, eingefügt durch die Artikel 9 bis 11 des Gesetzes vom 20. Juli 2022, verpflichten die darin genannten Betreiber, eine Reihe von Daten auf Vorrat zu speichern (Artikel 126/2), zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität, zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit und zur Wahrung lebenswichtiger Interessen einer natürlichen Person (Artikel 126/1), in fünf Arten von geografischen Gebieten, das heißt erstens denjenigen mit einer Rate von mindestens drei in Artikel 90*ter* §§ 2 bis 4 des Strafprozessgesetzbuches erwähnten Straftaten pro 1 000 Einwohner im Jahr (Artikel 126/3 § 1), zweitens denjenigen, die gemäß der in Artikel 8 Nrn. 1 und 2 des Gesetzes vom 10. Juli 2006 « über die Bedrohungsanalyse » erwähnten Bewertung, gemäß Artikel 11 des königlichen Erlasses vom 28. November 2006 « zur Ausführung des Gesetzes vom 10. Juli 2006 über die Bedrohungsanalyse » eine Bedrohungsstufe von mindestens 3 haben (Artikel 126/3 § 2), drittens denjenigen, die Bedrohungen für die nationale Sicherheit oder der Begehung von Handlungen schwerer Kriminalität besonders ausgesetzt sind, die sich aus einer Reihe von abschließend aufgezählten Orten zusammensetzen (Artikel 126/3 § 3), viertens denjenigen mit einer potenziell schweren Bedrohung für die lebenswichtigen Interessen des Landes oder für die Grundbedürfnisse der Bevölkerung, die sich aus einer Reihe von abschließend aufgezählten Orten zusammensetzen (Artikel 126/3 § 4), und fünftens denjenigen mit einer potenziell schweren Bedrohung für die Interessen der auf dem nationalen Hoheitsgebiet niedergelassenen internationalen Einrichtungen, die sich aus einer Reihe von abschließend aufgezählten Orten zusammensetzen (Artikel 126/3 § 5).

B.78.2. Im Tenor seines vorerwähnten Urteils vom 6. Oktober 2020 hat der Gerichtshof der Europäischen Union für Recht erkannt, dass Artikel 15 Absatz 1 der Richtlinie 2002/58/EG im Licht der Artikel 7, 8 und 11 sowie von Artikel 52 Absatz 1 der Charta Rechtsvorschriften entgegensteht, die zu den in Art. 15 Abs. 1 genannten Zwecken präventiv eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen.

Im selben Urteilstenor hat der Gerichtshof der Europäischen Union für Recht erkannt, dass Artikel 15 Absatz 1 der Richtlinie 2002/58/EG im Licht der Artikel 7, 8 und 11 sowie von Artikel 52 Absatz 1 der Charta Rechtsvorschriften nicht entgegensteht, die

- zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit auf der Grundlage objektiver und nicht diskriminierender Kriterien anhand von Kategorien betroffener Personen oder mittels eines geografischen Kriteriums für einen auf das absolut Notwendige begrenzten, aber verlängerbaren Zeitraum eine gezielte Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen;

- zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit für einen auf das absolut Notwendige begrenzten Zeitraum eine allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, vorsehen;

- zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zum Schutz der öffentlichen Sicherheit eine allgemeine und unterschiedslose Vorratsspeicherung der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten vorsehen.

Die vorgenannten Rechtsvorschriften müssen jedoch durch klare und präzise Regeln sicherstellen, dass bei der Speicherung der fraglichen Daten die materiellen und prozeduralen Voraussetzungen eingehalten werden und dass die Betroffenen über wirksame Garantien zum Schutz vor Missbrauchsrisiken verfügen.

B.79.1. Die in Artikel 126/2 des Gesetzes vom 13. Juni 2005 erwähnten Daten können grundsätzlich Gegenstand einer gezielten präventiven Vorratsspeicherung im Hinblick auf die in Artikel 126/1 § 1 Absatz 3 des Gesetzes vom 13. Juni 2005 erwähnten Zwecke des Schutzes der nationalen Sicherheit, der Bekämpfung schwerer Kriminalität und der Verhütung schwerer Bedrohungen der öffentlichen Sicherheit sein.

Wie die Gesetzgebungsabteilung des Staatsrates in ihrem Gutachten über den Gesetzesvorentwurf, der zum Gesetz vom 20. Juli 2022 geworden ist, angemerkt hat, kann beim Zweck der « Wahrung lebenswichtiger Interessen einer natürlichen Person », der auch in

Artikel 126/1 § 1 Absatz 3 des Gesetzes vom 13. Juni 2005 erwähnt ist, angenommen werden, dass er unter den Zweck des Schutzes der öffentlichen Sicherheit fällt (*Parl. Dok.*, Kammer, 2021-2022, DOC 55-2572/001, S. 279).

B.79.2. Der Gerichtshof hat anhand dieser in B.76 genannten Referenznormen zu prüfen, ob die Artikel 126/1 bis 126/3 des Gesetzes vom 13. Juni 2005 klare und präzise Regeln bezüglich der Tragweite und der Anwendung der Maßnahme der Vorratsspeicherung der vorgesehenen Daten vorsehen und Mindestanforderungen aufstellen. Der Eingriff muss sich auf das absolut Notwendige beschränken und muss objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen. Es obliegt dem Gesetzgeber, die Unterscheidungen vorzunehmen, die zwischen den verschiedenen der Vorratsspeicherung unterliegenden Datenarten notwendig sind, sodass gewährleistet ist, dass sich der Eingriff bei jeder Datenart auf das absolut Notwendige beschränkt.

B.80.1. Was die Maßnahme der Vorratsdatenspeicherung zum Schutz der nationalen Sicherheit betrifft, hat der Gerichtshof der Europäischen Union im vorerwähnten Urteil vom 6. Oktober 2020 erkannt:

« 148. Die erforderliche Begrenzung einer solchen Vorratsdatenspeicherung kann insbesondere anhand der Kategorien betroffener Personen vorgenommen werden, da Artikel 15 Absatz 1 der Richtlinie 2002/58 einer auf objektiven Kriterien beruhenden Regelung nicht entgegensteht, mit der Personen erfasst werden können, deren Verkehrs- und Standortdaten geeignet sind, einen zumindest mittelbaren Zusammenhang mit schweren Straftaten zu offenbaren, auf irgendeine Weise zur Bekämpfung schwerer Kriminalität beizutragen oder eine schwerwiegende Gefahr für die öffentliche Sicherheit oder eine Gefahr für die nationale Sicherheit zu verhüten (vgl. in diesem Sinne Urteil vom 21. Dezember 2016, *Tele2*, C-203/15 und C-698/15, EU:C:2016:970, Rn. 111).

149. Insoweit ist hinzuzufügen, dass zu den erfassten Personen insbesondere diejenigen gehören können, die zuvor im Rahmen der einschlägigen nationalen Verfahren und auf der Grundlage objektiver Kriterien als Bedrohung der öffentlichen Sicherheit oder der nationalen Sicherheit des betreffenden Mitgliedstaats eingestuft wurden.

150. Die Begrenzung einer Maßnahme zur Vorratsspeicherung von Verkehrs- und Standortdaten kann auch auf ein geografisches Kriterium gestützt werden, wenn die zuständigen nationalen Behörden aufgrund objektiver und nicht diskriminierender Anhaltspunkte davon ausgehen, dass in einem oder mehreren geografischen Gebieten eine durch ein erhöhtes Risiko der Vorbereitung oder Begehung schwerer Straftaten gekennzeichnete Situation besteht (vgl. in diesem Sinne Urteil vom 21. Dezember 2016, *Tele2*, C-203/15 und C-698/15, EU:C:2016:970, Rn. 111). Dabei kann es sich insbesondere um Orte handeln, die durch eine erhöhte Zahl schwerer Straftaten gekennzeichnet sind, um Orte, an

denen die Gefahr, dass schwere Straftaten begangen werden, besonders hoch ist, wie Orte oder Infrastrukturen, die regelmäßig von einer sehr hohen Zahl von Personen aufgesucht werden, oder um strategische Orte wie Flughäfen, Bahnhöfe oder Mautstellen.

151. Um sicherzustellen, dass der Eingriff, mit dem die in den Rn. 147 bis 150 des vorliegenden Urteils beschriebenen Maßnahmen gezielter Speicherung verbunden sind, mit dem Grundsatz der Verhältnismäßigkeit im Einklang steht, darf ihre Dauer das im Hinblick auf das verfolgte Ziel sowie die sie rechtfertigenden Umstände absolut Notwendige nicht überschreiten, unbeschadet einer etwaigen Verlängerung wegen des fortbestehenden Erfordernisses einer solchen Speicherung » (EuGH, 6. Oktober 2020, C-511/18, C-512/18 und C-520/18, vorerwähnt).

B.80.2. Aus den Vorarbeiten zu den angefochtenen Bestimmungen geht hervor, dass der Gesetzgeber durch die Artikel 126/1 bis 126/3 des Gesetzes vom 13. Juni 2005 die Möglichkeit umsetzen wollte, eine Maßnahme der Vorratsdatenspeicherung auf der Grundlage eines geografischen Kriteriums einzugrenzen, da diese Möglichkeit durch das vorerwähnte Urteil des Gerichtshofes der Europäischen Union vom 6. Oktober 2020 aufgezeigt wurde (*Parl. Dok.*, Kammer, 2021-2022, Doc 55-2572/001, SS. 45-49).

B.80.3.1. Die Umsetzung des vorerwähnten geografischen Kriteriums muss jedoch sachdienlich und im Hinblick auf die verfolgten Zwecke verhältnismäßig sein.

B.80.3.2. Wie die Gesetzgebungsabteilung des Staatsrates in ihrem Gutachten über den Gesetzesvorentwurf, der zum Gesetz vom 20. Juli 2022 geworden ist, angemerkt hat, sind die Anzahl und Vielfalt der in Artikel 126/3 des Gesetzes vom 13. Juni 2005 erwähnten Gebiete erheblich und zusammengenommen führen sie zur Abdeckung eines beträchtlichen Teils des Staatsgebietes (ebena, S. 283).

B.80.3.3. Aus der Begründung des Entwurfs, der dem Gesetz vom 20. Juli 2022 zugrunde liegt, geht hervor, dass der Gesetzgeber der Auffassung war, dass der Begriff « geografisches Gebiet », der in Randnummer 150 des vorerwähnten Urteils des Gerichtshofes der Europäischen Union vom 6. Oktober 2020 erwähnt wird, « sich nach Abschluss der Prüfung der Statistiken jedes einzelnen Bezirks auf das gesamte nationale Staatsgebiet beziehen kann, wenn es in jedem dieser Bezirke eine hohe Kriminalitätsrate gibt » (ebenda, S. 65).

Bezüglich der ersten Kategorie eines geografischen Gebiets, die in Artikel 126/3 § 1 des Gesetzes vom 13. Juni 2005 definiert ist, der die Vorratsspeicherung der in Artikel 126/2 § 2

des Gesetzes vom 13. Juni 2005 erwähnten Daten auf der Grundlage von Orten vorsieht, die durch eine hohe Anzahl von Taten schwerer Kriminalität gekennzeichnet sind (statistisches Kriterium), räumt der Gesetzgeber ein, dass « nicht zu leugnen ist, dass die Möglichkeit besteht, dass auf der Grundlage statistischer Daten, die naturgemäß dynamisch sind und sich ständig ändern, Daten in allen Gerichtsbezirken und somit für das gesamte Staatsgebiet auf Vorrat gespeichert werden müssen » (ebenda, S. 66).

Der Gesetzgeber stellt auch fest, dass « die Tätergruppen außerdem sehr mobil sind und sich fortbewegen und dass das organisierte Verbrechen seinem Wesen nach polykriminell ist. Sich von vornherein sehr gezielt auf bestimmte Orte auf lokaler Ebene zu beschränken, ist für diese Art von Kriminalität nicht geeignet » (ebenda, SS. 63-64).

Bei der Prüfung des Gesetzentwurfes im zuständigen Ausschuss der Abgeordnetenkammer hat der Minister der Justiz bezüglich der in Artikel 126/3 §§ 3 bis 5 des Gesetzes vom 13. Juni 2005 aufgezählten strategischen Gebiete angemerkt, dass « insgesamt etwa 30 % des Staatsgebiets ein strategisches Gebiet darstellen wird, was vor allem zeigt, dass Belgien ein dicht bevölkertes Land von geringer Größe ist » (*Parl. Dok.*, Kammer, 2021-2022, DOC 55-2572/003, S. 104).

B.80.3.4. Die bloße Feststellung, dass sich die in den Artikeln 126/1 bis 126/3 erwähnte Maßnahme der Vorratsdatenspeicherung unter bestimmten Umständen auf das gesamte Staatsgebiet beziehen kann, bedeutet jedoch nicht, dass diese mit einer allgemeinen Maßnahme der Vorratsdatenspeicherung gleichzusetzen ist, die unterschiedslos sämtliche Nutzer elektronischer Kommunikationsmittel betrifft.

Dies entspricht nämlich nicht dem Ziel des Gesetzgebers, sondern ist nur eine mögliche Folge, die sich aus den statistischen Daten der im Einzelnen in Artikel 126/3 beschriebenen und eingegrenzten geografischen Gebiete ergibt. Die Statistiken über die Anzahl an Straftaten in diesen geografischen Gebieten bestimmen objektiv und sachdienlich die im Bereich der Datenspeicherung und -verarbeitung geltende Regel.

Folglich entspricht das Gesetz der Anforderung, die in Randnummer 150 des vorerwähnten Urteils des Gerichtshofes der Europäischen Union vom 6. Oktober 2020 genannt ist und darin besteht, dass « die zuständigen nationalen Behörden aufgrund objektiver und nicht

diskriminierender Anhaltspunkte davon ausgehen, dass in einem oder mehreren geografischen Gebieten eine durch ein erhöhtes Risiko der Vorbereitung oder Begehung schwerer Straftaten gekennzeichnete Situation besteht ».

B.81. Folglich hat sich der Gesetzgeber mit der in den Artikeln 9 bis 11 des Gesetzes vom 20. Juli 2022 vorgesehenen Maßnahme der Vorratsdatenspeicherung auf das absolut Notwendige beschränkt.

B.82. Der erste, der zweite und der dritte Klagegrund in der Rechtssache Nr. 7930, der einzige Klagegrund in der Rechtssache Nr. 7931 sowie der dritte Teil des ersten Klagegrunds in der Rechtssache Nr. 7932 sind unbegründet, insofern sie aus einem Verstoß gegen Artikel 22 der Verfassung in Verbindung mit Artikel 8 der Europäischen Menschenrechtskonvention, mit den Artikeln 7, 8 und 52 Absatz 1 der Charta und mit Artikel 15 Absatz 1 der Richtlinie 2002/58/EG abgeleitet sind.

8. Die Aufzählung der zuständigen Behörden und der Zwecke im Rahmen des Zugangs zu den Daten (Artikel 13)

B.83. Der erste und der vierte Klagegrund in der Rechtssache Nr. 7930, der einzige Klagegrund in der Rechtssache Nr. 7931, sowie der erste und der zweite Teil des dritten Klagegrunds in der Rechtssache Nr. 7932 beziehen sich auf Artikel 13 des Gesetzes vom 20. Juli 2022.

Diese Bestimmung fügt einen Artikel 127/1 in das Gesetz vom 13. Juni 2005 ein, der bestimmt:

« § 1er. Pour l'application du présent article, la criminalité grave comprend notamment les faits pour lesquels il existe des indices sérieux :

1° qu'ils sont de nature à entraîner la peine minimale d'emprisonnement correctionnel principal visée à l'article 88*bis*, § 1er, alinéa 1er, du Code d'instruction criminelle;

2° qu'ils sont de nature à entraîner une sanction de niveau 5 ou 6 visée à l'article XV.70 du Code de droit économique;

3° qu'ils pourraient constituer une infraction aux articles 14 ou 15 du règlement (UE) n° 596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché (règlement relatif aux abus de marché) et abrogeant la directive 2003/6/CE du Parlement européen et du Conseil et les directives 2003/124/CE, 2003/125/CE et 2004/72/CE de la Commission ou aux dispositions prises sur la base ou en exécution de ces articles.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§ 4. Les données conservées en vertu des articles 126/1 et 126/3 le sont pour les autorités et finalités visées au paragraphe 2, 1° à 3° et 6°.

Seules les autorités visées au paragraphe 2, 1° à 3°, 6° et 9°, peuvent obtenir d'un opérateur, pour les finalités visées dans ce même paragraphe, des données conservées en vertu des articles 126/1 et 126/3, pour autant que prévu par et aux conditions fixées dans une norme législative formelle.

§ 5. La norme législative formelle de droit belge visée aux paragraphes 2 à 4 précise :

- la ou les catégories d'entreprises auxquelles l'autorité peut demander des données;

- les catégories de données qui peuvent être demandées;

- les finalités poursuivies;

- les mécanismes de contrôle de la demande de données, qui est effectué en interne ou, le cas échéant, par une juridiction ou une autorité administrative indépendante.

Le ministre fait publier au *Moniteur belge* une circulaire qui comprend une liste des autorités belges qui sont habilitées à obtenir d'un opérateur des données conservées en vertu des articles 122, 123, 126, 126/1, 126/3 et 127.

À la demande du ministre ou de l'Institut, les autorités belges visées aux paragraphes 2 à 4 fournissent les informations nécessaires pour la rédaction de cette circulaire.

§ 6. Les demandes que les autorités adressent aux opérateurs afin d'obtenir certaines données conservées en vertu des articles 122, 123, 126, 126/1, 126/3 ou 127 comprennent les mentions minimales suivantes :

1° l'identité de l'autorité demanderesse, ou, lorsque la demande est envoyée à l'opérateur par un service central pour le compte de cette autorité, l'identité de ce service;

2° la fonction de la personne de contact auprès de l'autorité demanderesse, ou, lorsque la demande est envoyée à l'opérateur par un service central pour le compte de l'autorité, la fonction de la personne de contact auprès de ce service central;

3° la base juridique sur laquelle se fonde la demande, sauf lorsque la demande est envoyée à l'opérateur par le biais d'un service central pour le compte d'une autre autorité;

4° le délai de réponse souhaité.

§ 7. L'Institut transmet annuellement au ministre et au ministre de la Justice des statistiques sur la fourniture aux autorités de données conservées en vertu des articles 122, 123, 126, 126/1, 126/3 et 127. Ces ministres les transmettent annuellement à la Chambre des représentants.

Ces statistiques comprennent notamment :

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

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

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

Ces statistiques ne peuvent comprendre des données à caractère personnel ou de l'information confidentielle.

Les données qui concernent l'application de l'alinéa 2, 1°, sont également jointes au rapport que le ministre de la Justice fait au Parlement conformément à l'article 90*decies* du Code d'instruction criminelle.

L'Institut demande aux opérateurs et au service désigné par le Roi les informations qui lui permettent de remplir l'obligation visée à l'alinéa 1er ».

B.84.1. Die klagende Partei in der Rechtssache Nr. 7930 leitet einen ersten und einen vierten Klagegrund ab aus einem Verstoß gegen die Artikel 11, 12, 22 und 29 der Verfassung, gegen Artikel 15 Absatz 1 und gegen die Artikel 5, 6 und 9 der Richtlinie 2002/58/EG, gelesen im Lichte der Artikel 7, 8, 11, 47 und 52 Absatz 1 der Charta, der Artikel 6, 8, 10, 11 und 18 der Europäischen Menschenrechtskonvention und der Artikel 13 und 54 der Richtlinie (EU) 2016/680, insofern Artikel 13 des Gesetzes vom 20. Juli 2022 einen sehr umfangreichen Zugang zu den betreffenden Daten erlaube, die ihrerseits Gegenstand einer allgemeinen Vorratsspeicherungspflicht seien. Insbesondere führt sie an, dass die erwähnten Behörden über den Rahmen der von Artikel 15 Absatz 1 der Richtlinie 2002/58/EG aufgezählten Zwecke hinausgingen, dass keine Hierarchie der Zwecke festgelegt sei, dass der herangezogene Begriff der « schweren Kriminalität » nicht im Einklang mit der Rechtsprechung des Gerichtshofes der Europäischen Union stehe und dass es dem zuständigen Minister obliege, die Behörden zu bestimmen, die auf die Daten zugreifen dürften, was nicht mit dem formellen Legalitätsprinzip vereinbar sei.

B.84.2. Die klagende Partei in der Rechtssache Nr. 7931 leitet einen einzigen Klagegrund ab aus einem Verstoß gegen die Artikel 11, 12, 22 und 29 der Verfassung, an sich oder in Verbindung mit den Artikeln 7, 8, 11, 47 und 52 Absatz 1 der Charta, mit Artikel 8 der Europäischen Menschenrechtskonvention, mit den Artikeln 5, 6 und 15 der Richtlinie 2002/58/EG und mit den Artikeln 13 und 54 der Richtlinie (EU) 2016/680. Die klagende Partei behauptet, dass es Artikel 13 des Gesetzes vom 20. Juli 2022 dem zuständigen Minister erlaube, die Behörden aufzulisten, die befugt seien, auf die erwähnten Daten zuzugreifen, was gegen das formelle Legalitätsprinzip verstoße, dass es diese Bestimmung nicht erfordere, dass das Ersuchen auf Zugang im Hinblick auf den verfolgten Zweck begründet werde, und dass die Weise, wie die « schwere Kriminalität » definiert sei, nicht mit der Rechtsprechung des Gerichtshofes der Europäischen Union im Einklang stehe.

B.84.3.1. Die klagenden Parteien in der Rechtssache Nr. 7932 leiten einen dritten Klagegrund ab aus einem Verstoß gegen die Artikel 10, 11, 15, 22 und 29 der Verfassung, an sich oder in Verbindung mit den Artikeln 5, 6, 8, 9, 10, 11, 14 und 18 der Europäischen Menschenrechtskonvention, mit den Artikeln 7, 8, 11, 47 und 52 der Charta, mit Artikel 5 Absatz 4 des Vertrags über die Europäische Union, mit der Richtlinie 2002/58/EG, mit der Richtlinie (EU) 2016/680 und mit der DSGVO.

In einem ersten Teil führen die klagenden Parteien an, dass Artikel 13 des Gesetzes vom 20. Juli 2022 nicht die Hierarchie der Zwecke, die von der Rechtsprechung des Gerichtshofes der Europäischen Union aufgestellt worden sei, einhalte, dass die herangezogene Definition der « schweren Kriminalität » nicht mit dieser Rechtsprechung im Einklang stehe, dass die erwähnten Behörden zu viele seien und dass diese über den Rahmen der von Artikel 15 Absatz 1 der Richtlinie 2002/58/EG aufgezählten Zwecke hinausgingen.

In einem zweiten Teil führen die klagenden Parteien an, dass die gegen Artikel 13 des Gesetzes vom 20. Juli 2022 gerichteten Beschwerdegründe auch für die spezifischen Modalitäten für den Zugang zu den Daten gälten, die in den Kapiteln 3 bis 10 des Gesetzes vom 20. Juli 2022 vorgesehen seien, die außerdem nicht systematisch die notwendigen Verfahrensgarantien sowie eine unabhängige Kontrolle beim Zugang zu diesen sensiblen Daten vorsähen. Diesbezüglich nennen die klagenden Parteien die Artikel 21, 24, 26, 27, 28, 33, 34, 35, 37, 40, 41, 42 und 44 des Gesetzes vom 20. Juli 2022.

B.85. Die Beschwerdegründe der klagenden Parteien sind hauptsächlich aus einem Verstoß gegen das Recht auf Achtung des Privatlebens und das Recht auf Schutz personenbezogener Daten abgeleitet, die in Artikel 22 der Verfassung, in Artikel 8 der Europäischen Menschenrechtskonvention, in den Artikeln 7, 8 und 52 Absatz 1 der Charta, in der Richtlinie 2002/58/EG, in der Richtlinie (EU) 2016/680 und in der DSGVO gewährleistet sind. Sie führen nicht ausdrücklich einen Beschwerdegrund gegen die anderen in B.84.1 bis B.84.3 genannten Referenznormen an.

B.86. Artikel 127/1 des Gesetzes vom 13. Juni 2005 bezieht sich auf den Zugang zu den aufgrund der Artikel 122, 123, 126, 126/1, 126/3 und 127 dieses Gesetzes auf Vorrat gespeicherten Daten.

B.87.1. Aus dem Wortlaut von Artikel 127/1 des Gesetzes vom 13. Juni 2005 sowie aus seinen Vorarbeiten geht hervor, dass diese Bestimmung nicht den Zugang zu den in den Artikeln 122, 123, 126, 126/1, 126/3 und 127 des Gesetzes vom 13. Juni 2005 erwähnten Daten regelt (*Parl. Dok.*, Kammer, 2021-2022, DOC 55-2572/001, SS. 96-97).

B.87.2. Artikel 127/1 des Gesetzes vom 13. Juni 2005 beschränkt sich nämlich darauf, die Behörden und die Zwecke aufzuzählen, die den Zugang zu den auf der Grundlage der Artikel 122, 123, 126, 126/1, 126/3 und 127 des Gesetzes vom 13. Juni 2005 auf Vorrat gespeicherten Daten ermöglichen können. Zwar steht Artikel 127/1 dem entgegen, dass eine andere Behörde benannt wird oder dass ein anderer Zweck geltend gemacht wird, um auf die vorerwähnten Daten zuzugreifen, aber er selbst erlaubt es auch nicht sämtlichen Behörden und zu den Zwecken, die darin aufgezählt sind, darauf Zugriff zu haben, wie es die Gesetzgebungsabteilung des Staatsrates in ihrem Gutachten zum Vorentwurf des Gesetzes, das dem Gesetz vom 20. Juli 2022 zugrunde liegt, angemerkt hat (ebenda, SS. 309-311).

B.87.3. Die in Artikel 127/1 des Gesetzes vom 13. Juni 2005 vorgesehenen Bedingungen sind nämlich nicht ausreichend, um den Zugang zu den betreffenden Daten zu ermöglichen. Es ist nämlich erforderlich, dass eine spezifische « formelle Gesetzesnorm » angenommen wird (Artikel 127/1 §§ 2 und 3) und dass darin « die Kategorie oder Kategorien von Unternehmen, die die Behörde um Daten ersuchen kann », « die Datenkategorien, die angefragt werden können », « die verfolgten Zwecke » und « die Mechanismen der Kontrolle der Datenanfrage,

die intern oder gegebenenfalls durch ein Gericht oder eine unabhängige Verwaltungsbehörde durchgeführt wird » präzisiert sind (Artikel 127/1 § 5).

Über die verschiedenen « formellen Gesetzesnormen », die in Artikel 127/1 erwähnt sind, muss der Gesetzgeber die Unterscheidungen vornehmen, die zwischen den verschiedenen auf Vorrat gespeicherten Datenarten notwendig sind, um zu gewährleisten, dass sich der Eingriff für jede Datenart auf das absolut Notwendige beschränkt.

B.88. Folglich können die Beschwerdegründe der klagenden Parteien, insofern sie sich auf den Zugang zu den Daten, deren Vorratsspeicherung nach dem Gesetz vom 13. Juni 2005 zulässig ist, beziehen, nicht auf Artikel 127/1 dieses Gesetzes zurückgeführt werden, sondern auf die in dieser Bestimmung erwähnten « formellen Gesetzesnormen », die die erwähnten Daten, die Behörden, die um Zugang dazu ersuchen können, die präzisen verfolgten Zwecke sowie die etwaigen Kontrollmechanismen bestimmen.

In diesem Rahmen kann nicht angenommen werden, dass sich der zweite Teil des dritten Klagegrunds der klagenden Parteien in der Rechtssache Nr. 7932 auf solche formellen Gesetzesnormen bezieht, da diese Parteien sich darauf beschränken, die Artikel 21, 24, 26, 27, 28, 33, 34, 35, 37, 40, 41, 42 und 44 des Gesetzes vom 20. Juli 2022 zu nennen, ohne nachzuweisen, inwiefern diese Anwendungen von Artikel 127/1 des Gesetzes vom 13. Juni 2005 darstellen, und sie auch nicht begründen, inwiefern diese Bestimmungen konkret gegen die in B.85 genannten Referenznormen verstoßen würden.

B.89. Was schließlich die Vereinbarkeit von Artikel 127/1 § 5 Absatz 2 des Gesetzes vom 13. Juni 2005 mit dem formellen Legalitätsprinzip betrifft, insofern diese Bestimmung vorsieht, dass der zuständige Minister im *Belgischen Staatsblatt* ein Rundschreiben veröffentlichen lässt, das die Liste der belgischen Behörden umfasst, die befugt sind, vom Betreiber Zugang zu den aufgrund der Artikel 122, 123, 126, 126/1, 126/3 und 127 des Gesetzes vom 13. Juni 2005 auf Vorrat gespeicherten Daten zu erhalten, so bezweckt diese Bestimmung lediglich, es dem vorerwähnten Minister zu ermöglichen, sämtliche Behörden, die in den « formellen Gesetzesnormen », von denen in Artikel 127/1 des Gesetzes vom 13. Juni 2005 die Rede ist, erwähnt werden, in einem Rundschreiben aufzuzählen.

Artikel 127/1 § 5 Absatz 2 ermächtigt nicht einen Minister, die Behörden zu bestimmen, die zuständig sind, um auf die in den Artikeln 122, 123, 126, 126/1, 126/3 und 127 des Gesetzes vom 13. Juni 2005 erwähnten Daten zuzugreifen.

B.90. Der erste und der vierte Klagegrund in der Rechtssache Nr. 7930, der einzige Klagegrund in der Rechtssache Nr. 7931 sowie der erste und der zweite Teil des dritten Klagegrunds in der Rechtssache Nr. 7932 sind unbegründet, sofern die aus einem Verstoß gegen Artikel 13 des Gesetzes vom 20. Juli 2022 abgeleitet sind.

B.91.1. In ihrem einzigen Klagegrund beanstandet die klagende Partei in der Rechtssache Nr. 7931 auch die fehlende Information der Person, zu deren Daten Zugang gewährt wird, und das Fehlen von Rechtsmitteln im Fall eines unrechtmäßigen Zugangs zu ihnen. In Bezug auf die vorerwähnte fehlende Information beantragt sie hilfsweise, dass dem Gerichtshof der Europäischen Union eine Vorabentscheidungsfrage gestellt wird.

B.91.2. Die klagenden Parteien in der Rechtssache Nr. 7932 leiten einen vierten Klagegrund ab aus einem Verstoß gegen die Artikel 10, 11, 13 und 22 der Verfassung, an sich oder in Verbindung mit den Artikeln 5, 6, 8, 9, 10, 11, 14 und 18 der Europäischen Menschenrechtskonvention, mit den Artikeln 7, 8, 11, 47 und 52 der Charta, mit Artikel 5 Absatz 4 des Vertrags über die Europäische Union, mit der Richtlinie 2002/58/EG, mit der Richtlinie (EU) 2016/680 und mit der DSGVO. In diesem Klagegrund beanstanden die klagenden Parteien allgemein das Fehlen einer Notifizierung an den Nutzer, wenn die zuständigen Behörden auf die Daten zugreifen, was gegen das Recht auf gerichtliches Gehör und das Recht auf eine wirksame Beschwerde verstoße, ohne jedoch eine besondere Bestimmung des Gesetzes vom 20. Juli 2022 zu nennen.

B.91.3. Zwar kann davon ausgegangen werden, dass sich diese Klagegründe auf Artikel 127/1 des Gesetzes vom 13. Juni 2005 beziehen, aber es ist darauf hinzuweisen, dass diese Bestimmung, wie in B.87.1 erwähnt, nicht selbst den Zugang zu den betreffenden Daten erlaubt. Somit ist der Antrag auf eine Vorabentscheidungsfrage der klagenden Partei in der Rechtssache Nr. 7931 im Rahmen von Artikel 127/1 des Gesetzes vom 13. Juni 2005 nicht sachdienlich.

Insofern sich der vierte Klagegrund in der Rechtssache Nr. 7932 auf die spezifischen « formellen Gesetzesnormen », die in Artikel 127/1 des Gesetzes vom 13. Juni 2005 bezöge, nennen die klagenden Parteien außerdem weder eine besondere Gesetzesbestimmung, um ihre Beschwerdegründe zu untermauern, noch erklären sie, inwiefern diese spezifischen formellen Gesetzesnormen gegen die in B.85 genannten Referenznormen verstoßen würden.

B.91.4. Der einzige Klagegrund in der Rechtssache Nr. 7931, insofern er sich auf die in B.91.1 erwähnten Beschwerdegründe bezieht, und der vierte Klagegrund in der Rechtssache Nr. 7932 sind unbegründet.

9. Die Befugnisse der Gerichtspolizeioffiziere des BIPF (Artikel 24)

B.92. Der einzige Klagegrund in der Rechtssache Nr. 7557 bezieht sich auf Artikel 24 des Gesetzes vom 20. Juli 2022. Diese Bestimmung fügt einen Artikel 25/1 in das Gesetz vom 17. Januar 2003 « über das Statut der Regulierungsinstanz des belgischen Post- und Telekommunikationssektors » (nachstehend: Gesetz vom 17. Januar 2003) ein, der bestimmt:

« § 1er. Afin de rechercher, de constater ou de poursuivre une infraction visée à l'article 145, § 3 ou § 3*bis*, de la loi du 13 juin 2005 relative aux communications électroniques ou à l'article 24, § 1er, 2°, un officier de police judiciaire de l'Institut peut, par écrit :

1° exiger d'un opérateur de répondre à une demande de données d'identification qui est nécessaire à ces fins;

2° requérir la collaboration des personnes et institutions visées à l'article 46*quater*, § 1er, du Code d'instruction criminelle et d'associations les représentant, sur la base de la référence de paiement en ligne spécifique à un service de communications électroniques qui a préalablement été communiquée par un opérateur conformément au 1°, afin d'identifier la personne qui a payé le service;

3° requérir la collaboration des centres fermés ou des lieux d'hébergement au sens des articles 74/8 et 74/9 de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers, où la souscription de l'abonné à un service de communications électroniques a été effectué, sur la base des coordonnées du centre ou du lieu d'hébergement qui ont préalablement été communiquées par un opérateur conformément au 1°, afin d'identifier l'abonné;

4° requérir la collaboration de toute autre personne morale qui est l'abonnée d'un opérateur ou qui souscrit à un service de communications électroniques au nom et pour le compte de personnes physiques, sur la base des données qui ont préalablement été

communiquées par un opérateur conformément au 1°, afin d'identifier l'abonné ou l'utilisateur habituel du service.

Une demande visée à l'alinéa 1er ne peut être transmise à un acteur visé à l'alinéa 1er qu'après autorisation écrite d'un officier de police judiciaire visé à l'article 24, § 2. Cette autorisation ne peut être octroyée que sur demande écrite et motivée adressée à cet officier conformément au paragraphe 5.

§ 2. Pour les besoins de l'accomplissement de ses missions, un officier de police judiciaire de l'Institut peut exiger d'un opérateur, par écrit, de répondre à une demande de métadonnées, qui est nécessaire afin de rechercher, de constater ou de poursuivre une infraction visée à l'article 145, § 3, ou § 3*bis*, de la loi du 13 juin 2005 relative aux communications électroniques ou à l'article 24, § 1er, 2°.

Sauf en cas d'urgence dûment justifiée, l'officier de police judiciaire de l'Institut ne peut adresser la demande à l'opérateur qu'après avoir soumis une demande écrite et motivée au juge d'instruction et après autorisation écrite de ce dernier.

En cas d'urgence dûment justifiée visée à l'alinéa 2, l'officier de police judiciaire de l'Institut communique au juge d'instruction, sans délai après l'envoi de la demande à l'opérateur, une copie de cette demande, la motivation de la demande et la justification de l'urgence. Un contrôle ultérieur est effectué par le juge d'instruction.

Lorsqu'à la suite de ce contrôle ultérieur, le juge d'instruction refuse de confirmer la validité de la demande envoyée par l'officier de police judiciaire de l'Institut à l'opérateur, cet officier le notifie sans délai à l'opérateur concerné et supprime les métadonnées reçues.

§ 3. Par dérogation aux paragraphes 1er et 2, afin de contrôler le respect des articles 126, 126/1, 126/2, 126/3 ou 127 de la loi du 13 juin 2005 relative aux communications électroniques et de leurs arrêtés d'exécution et à la demande écrite et motivée d'un officier de police judiciaire de l'Institut, un opérateur fournit, dans le délai fixé dans le réquisitoire, un accès permettant de consulter ses bases de données qui mettent en œuvre un de ces articles ou un de ces arrêtés d'exécution.

Une demande visée à l'alinéa 1er ne peut être transmise à un opérateur qu'après autorisation écrite d'un officier de police judiciaire de l'Institut visé à l'article 24, § 2. Cette autorisation ne peut être octroyée que sur demande écrite et motivée conformément au paragraphe 5.

La demande adressée à l'opérateur précise les noms des officiers de police judiciaire de l'Institut qui peuvent consulter la base de données.

Ces officiers ne peuvent prendre une copie des données et documents consultés dans le cadre de l'alinéa 1er que dans le but de constater des infractions commises par l'opérateur.

§ 4. Pour l'application des paragraphes 1er et 2, les acteurs visés au paragraphe 1er, alinéa 1er, auxquels un officier de police judiciaire de l'Institut a demandé des données, lui communiquent ces données en temps réel ou, le cas échéant, au moment précisé dans le réquisitoire.

Pour l'application des paragraphes 1er à 3, toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

Toute personne qui refuse de communiquer les données ou qui ne les communique pas en temps réel ou, le cas échéant, au moment précisé dans le réquisitoire est punie d'une amende de vingt-six euros à dix mille euros.

Toute personne qui refuse de permettre la consultation de la base de données conformément au paragraphe 3 ou qui ne permet pas cette consultation dans le délai fixé dans le réquisitoire est punie d'une amende de vingt-six euros à dix mille euros.

§ 5. Pour l'application des paragraphes 1er à 3, la motivation de la demande adressée à l'officier de police judiciaire visé à l'article 24, § 2, ou au juge d'instruction doit être développée au regard des circonstances de l'enquête.

Pour l'application des paragraphes 1er et 2, cette motivation indique :

1° le lien entre les données demandées et l'objectif de recherche, de constat ou de poursuite de l'infraction spécifique qui justifie la demande;

2° le caractère strictement nécessaire des données demandées dans le cadre de l'enquête.

§ 6. Les officiers de police judiciaire de l'Institut consignent dans un registre :

1° l'ensemble des demandes visées aux paragraphes 1er, 2 et 3;

2° la motivation de la demande et la justification de l'urgence communiquées au juge d'instruction conformément au paragraphe 2, alinéa 3;

3° les autorisations prévues aux paragraphes 1er, 2 et 3 ».

B.93. Die klagende Partei in der Rechtssache Nr. 7931 leitet einen einzigen Klagegrund ab aus einem Verstoß gegen die Artikel 11, 12, 22 und 29 der Verfassung, an sich oder in Verbindung mit den Artikeln 7, 8, 11, 47 und 52 Absatz 1 der Charta, mit Artikel 8 der Europäischen Menschenrechtskonvention, mit den Artikeln 5, 6 und 15 der Richtlinie 2002/58/EG und mit den Artikeln 13 und 54 der Richtlinie (EU) 2016/680. Sie führt an, dass Artikel 25/1 des Gesetzes vom 17. Januar 2003 gegen die vorerwähnten Referenznormen verstoße, insofern er den Zugang zu den Daten im Rahmen eines Strafverfahrens durch einen Gerichtspolizeioffizier erlaube, der keine unabhängige Behörde sei, und insofern er keine gerichtliche Kontrolle vor diesem Zugang vorschreibe. Außerdem beanstandet sie ebenfalls den Umstand, dass die Person, auf deren Daten zugegriffen wird, davon nicht verständigt wird, sowie das Fehlen von Rechtsmitteln im Fall des unrechtmäßigen Zugangs zu den Daten. In

Bezug auf die vorerwähnte fehlende Information beantragt sie hilfsweise, dass dem Gerichtshof der Europäischen Union eine Vorabentscheidungsfrage gestellt wird.

B.94. Die Beschwerdegründe der klagenden Partei sind ausschließlich aus einem Verstoß gegen das Recht auf Achtung des Privatlebens und das Recht auf Schutz personenbezogener Daten abgeleitet, die in Artikel 22 der Verfassung, in Artikel 8 der Europäischen Menschenrechtskonvention, in den Artikeln 7, 8 und 52 Absatz 1 der Charta, in der Richtlinie 2002/58/EG, in der Richtlinie (EU) 2016/680 und in der DSGVO gewährleistet sind.

B.95. Im Rahmen eines Strafverfahrens erlaubt Artikel 25/1 des Gesetzes vom 17. Januar 2003 einem Gerichtspolizeioffizier des BIPF den Zugang zu den Daten in zwei Fällen. Erstens darf ein Gerichtspolizeioffizier auf Identifizierungsdaten zugreifen, um die in Artikel 145 §§ 3 und 3*bis* des Gesetzes vom 13. Juni 2005 und in Artikel 24 § 1 Nr. 2 des Gesetzes vom 17. Januar 2003 erwähnten Straftaten zu ermitteln, festzustellen oder zu verfolgen (Artikel 25/1 § 1). Zweitens darf ein Gerichtspolizeioffizier für die Zwecke der Erfüllung seiner Aufträge auf die notwendigen Metadaten zugreifen, um die vorwähnten Straftaten zu ermitteln, festzustellen oder zu verfolgen (Artikel 25/1 § 2).

B.96. In Anbetracht des Vorstehenden beschränkt der Gerichtshof seine Prüfung auf Artikel 25/1 §§ 1 und 2 des Gesetzes vom 17. Januar 2003.

B.97. Da in der angefochtenen Bestimmung auf die Bestimmung Bezug genommen wird, zu denen der Gerichtshof dem Gerichtshof der Europäischen Union Vorabentscheidungsfragen gestellt hat, ist die Entscheidung über die Prüfung dieser Klagegründe in Erwartung einer Antwort des Gerichtshofes der Europäischen Union auf diese Vorabentscheidungsfragen auszusetzen.

10. Die Befugnisse des Prokurators des Königs (Artikel 25 und 26)

B.98.1. Der einzige Klagegrund in der Rechtssache Nr. 7931 bezieht sich insbesondere auf die Artikel 25 und 26 des Gesetzes vom 20. Juli 2022.

B.98.2. Artikel 25 des Gesetzes vom 20. Juli 2022 fügt in das Strafprozessgesetzbuch einen Artikel 39*quinquies* ein, der bestimmt:

« § 1. Bei der Ermittlung von Verbrechen und Vergehen kann der Prokurator des Königs, wenn es schwerwiegende Indizien dafür gibt, dass die Straftaten eine Hauptkorrektionalgefängnisstrafe von einem Jahr oder eine schwerere Strafe zur Folge haben können, einem oder mehreren der in Absatz 2 erwähnten Akteure durch eine mit Gründen versehene schriftliche Entscheidung die Anordnung erteilen, die in Artikel 88*bis* § 1 Absatz 1 erwähnten Daten, die er für notwendig erachtet und die bei der Bereitstellung der betreffenden Kommunikationsdienste von ihnen erzeugt oder verarbeitet werden, aufzubewahren.

Die in Absatz 1 erwähnte Anordnung kann unmittelbar oder über einen vom König bestimmten Polizeidienst folgenden Personen erteilt werden:

- dem Betreiber eines elektronischen Kommunikationsnetzes und

- jeglicher Person, die auf belgischem Staatsgebiet auf irgendeine Weise einen Dienst bereitstellt oder anbietet, der in der Übertragung von Signalen über elektronische Kommunikationsnetze besteht oder durch den Nutzer dazu ermächtigt werden, über ein elektronisches Kommunikationsnetz Informationen zu erhalten, zu empfangen oder zu verbreiten. Hierzu zählt auch der Anbieter eines elektronischen Kommunikationsdienstes.

In der mit Gründen versehenen schriftlichen Entscheidung wird Folgendes angegeben:

- der Name des Prokurators des Königs, der die Aufbewahrung anordnet,

- die Straftat, die Gegenstand der Anordnung ist,

- die tatsächlichen Umstände der Sache, die die Aufbewahrung der Daten rechtfertigen,

- die genaue Angabe einer oder mehrerer der folgenden Informationen: die Person(en), die Kommunikationsmittel oder die Orte, die Gegenstand der Aufbewahrung sind,

- gegebenenfalls die Kategorien der Verkehrs- und Standortdaten, die aufbewahrt werden müssen,

- die Dauer der Maßnahme, die zwei Monate ab dem Datum der Anordnung nicht übersteigen darf, unbeschadet einer Erneuerung,

- die Dauer der Aufbewahrung dieser Daten, die sechs Monate nicht übersteigen darf. Diese Frist kann schriftlich verlängert werden.

Im Dringlichkeitsfall kann die Aufbewahrung mündlich angeordnet werden. Die Anordnung muss so schnell wie möglich in der in Absatz 3 vorgesehenen Form bestätigt werden.

§ 2. Die in § 1 Absatz 2 erwähnten Akteure sorgen dafür, dass die Unversehrtheit, die Qualität und Verfügbarkeit der Daten gewährleistet ist und dass die Daten sicher aufbewahrt werden.

§ 3. Jede Person, die aufgrund ihres Amtes Kenntnis von der Maßnahme erlangt oder dabei mitwirkt, unterliegt der Schweigepflicht. Jegliche Verletzung der Schweigepflicht wird gemäß Artikel 458 des Strafgesetzbuches geahndet.

Wer die Mitwirkung verweigert oder die aufbewahrten Daten verschwinden lässt, vernichtet oder ändert, wird mit einer Gefängnisstrafe von sechs Monaten bis zu einem Jahr und mit einer Geldbuße von sechsundzwanzig bis zu zwanzigtausend EUR oder mit nur einer dieser Strafen bestraft.

§ 4. Der Zugang zu den gemäß diesem Artikel aufbewahrten Daten ist nur in Anwendung von Artikel 88*bis* möglich ».

B.98.3. Artikel 26 des Gesetzes vom 20. Juli 2022 ändert Artikel 46*bis* des Strafprozessgesetzbuches ab wie folgt:

« 1. In § 1 wird zwischen Absatz 2 und Absatz 3 ein Absatz mit folgendem Wortlaut eingefügt:

‘ Zur Identifizierung eines Teilnehmers oder eines gewöhnlichen Nutzers eines in Absatz 2 zweiter Gedankenstrich erwähnten Dienstes kann er auch unmittelbar oder über einen vom König bestimmten Polizeidienst die Mitwirkung folgender Personen anfordern:

- der in Artikel 46*quater* § 1 erwähnten Personen und Institutionen, auf der Grundlage der Referenznummer eines elektronischen Bankgeschäfts, die vorher von einem der in Absatz 2 erster und zweiter Gedankenstrich erwähnten Akteure in Anwendung von Absatz 1 mitgeteilt worden ist,

- der geschlossenen Zentren oder Unterbringungsorte im Sinne der Artikel 74/8 und 74/9 des Gesetzes vom 15. Dezember 1980 über die Einreise ins Staatsgebiet, den Aufenthalt, die Niederlassung und das Ausweisen von Ausländern, auf der Grundlage der Kontaktdaten des Zentrums oder Unterbringungsorts - in beziehungsweise an denen das Abonnement des Teilnehmers für einen mobilen elektronischen Kommunikationsdienst abgeschlossen wurde -, die vorher von einem der in Absatz 2 erster und zweiter Gedankenstrich erwähnten Akteure in Anwendung von Absatz 1 mitgeteilt worden sind,

- der anderen juristischen Personen, die Teilnehmer einer der in Absatz 2 erster oder zweiter Gedankenstrich erwähnten Akteure sind, oder die im Namen und für Rechnung natürlicher Personen einen elektronischen Kommunikationsdienst abonnieren auf der Grundlage von Daten, die vorher von einem der in Absatz 2 erster und zweiter Gedankenstrich erwähnten Akteure in Anwendung von Absatz 1 mitgeteilt worden sind. ’

2. In § 2 werden die Absätze 3 und 4 aufgehoben.

3. Der Artikel wird durch die Paragraphen 3 und 4 mit folgendem Wortlaut ergänzt:

‘ § 3. Die in § 1 Absatz 3 erster bis dritter Gedankenstrich erwähnten Akteure, die aufgefordert werden, die Kenndaten des Teilnehmers oder gewöhnlichen Nutzers eines in § 1

Absatz 2 zweiter Gedankenstrich erwähnten Dienstes mitzuteilen, teilen dem Prokurator des Königs oder dem Gerichtspolizeioffizier die Daten in Echtzeit oder gegebenenfalls zu dem in der Anforderung bestimmten Zeitpunkt mit.

§ 4. Jede Person, die aufgrund ihres Amtes Kenntnis von der Maßnahme erlangt oder dabei mitwirkt, unterliegt der Schweigepflicht. Jegliche Verletzung der Schweigepflicht wird gemäß Artikel 458 des Strafgesetzbuches geahndet.

Wer sich weigert, die Daten mitzuteilen, oder wer die Daten nicht in Echtzeit oder gegebenenfalls zu dem in der Anforderung bestimmten Zeitpunkt mitteilt, wird mit einer Geldbuße von sechsundzwanzig bis zu zehntausend EUR bestraft. ' ».

B.99.1. Die klagende Partei in der Rechtssache Nr. 7931 leitet einen einzigen Klagegrund ab aus einem Verstoß gegen die Artikel 11, 12, 22 und 29 der Verfassung, an sich oder in Verbindung mit den Artikeln 7, 8, 11, 47 und 52 Absatz 1 der Charta, mit Artikel 8 der Europäischen Menschenrechtskonvention, mit den Artikeln 5, 6 und 15 der Richtlinie 2002/58/EG und mit den Artikeln 13 und 54 der Richtlinie (EU) 2016/680.

Die klagende Partei in der Rechtssache Nr. 7931 führt an, dass Artikel 39*quinquies* des Strafprozessgesetzbuches auf die Kriminalität « allgemein » abziele, während der Gerichtshof der Europäischen Union sich zum einen auf Fälle « schwerer » Kriminalität beschränke und diese Bestimmung zum anderen eine unverhältnismäßige Speicherdauer vorsehe.

Was die an Artikel 46*bis* des Strafprozessgesetzbuches vorgenommenen Änderungen betrifft, behauptet die klagende Partei zunächst, dass es diese Bestimmung dem Prokurator des Königs oder im Fall äußerster Dringlichkeit einem Gerichtspolizeioffizier erlaube, auf Identifizierungsdaten zuzugreifen, ohne dass dieser Zugriff einer vorherigen und unabhängigen Kontrolle unterliege, wie es der Gerichtshof der Europäischen Union fordere. Hilfsweise beantragt sie, dem Gerichtshof der Europäischen Union eine Vorabentscheidungsfrage zu stellen. Zudem behauptet die klagende Partei, dass es Artikel 46*bis* des Strafprozessgesetzbuches in der geänderten Fassung dem Prokurator des Königs erlaube, in Dringlichkeitsfällen zur Bekämpfung der Kriminalität allgemein auf die Verkehrs- und Standortdaten zuzugreifen, was auch nicht mit den Anforderungen des Gerichtshofes der Europäischen Union vereinbar sei. Hilfsweise beantragt sie, dass diesem Gerichtshof diesbezüglich eine Vorabentscheidungsfrage gestellt wird. Außerdem behauptet die klagende Partei, dass die Mitwirkung der in Artikel 46*bis* des Strafprozessgesetzbuches erwähnten geschlossenen Zentren und Unterbringungsorte im Hinblick auf die Bekämpfung der

Kriminalität nicht gerechtfertigt sei. Schließlich bemängelt sie, dass Artikel 46*bis* des Strafprozessgesetzbuches weder vorsehe, die Person über den Zugriff auf die Daten noch über das Bestehen eines spezifischen Rechtsmittels zu informieren. In Bezug auf die vorerwähnte fehlende Information beantragt sie, dass dem Gerichtshof der Europäischen Union eine Vorabentscheidungsfrage gestellt wird.

B.99.2. Die gegen Artikel 39*quinquies* und 46*bis* des Strafprozessgesetzbuches gerichteten Beschwerdegründe der klagenden Partei sind ausschließlich aus einem Verstoß gegen das Recht auf Achtung des Privatlebens und das Recht auf Schutz personenbezogener Daten abgeleitet, die in Artikel 22 der Verfassung, in Artikel 8 der Europäischen Menschenrechtskonvention, in den Artikeln 7, 8 und 52 Absatz 1 der Charta, in der Richtlinie 2002/58/EG und in der Richtlinie (EU) 2016/680 gewährleistet sind.

B.100. Der Gerichtshof prüft zunächst die gegen Artikel 39*quinquies* des Strafprozessgesetzbuches gerichteten Beschwerdegründe, sodann die zu Artikel 46*bis* desselben Gesetzbuches.

B.101.1. Im Tenor seines vorerwähnten Urteils vom 6. Oktober 2020 hat der Gerichtshof der Europäischen Union für Recht erkannt, dass Artikel 15 Absatz 1 der Richtlinie 2002/58/EG im Licht der Artikel 7, 8, 11 und Artikel 52 Absatz 1 der Charta Maßnahmen nicht entgegensteht, die « es zur Bekämpfung schwerer Kriminalität und, *a fortiori*, zum Schutz der nationalen Sicherheit gestatten, den Betreibern elektronischer Kommunikationsdienste mittels einer Entscheidung der zuständigen Behörde, die einer wirksamen gerichtlichen Kontrolle unterliegt, aufzugeben, während eines festgelegten Zeitraums die ihnen zur Verfügung stehenden Verkehrs- und Standortdaten umgehend zu sichern ».

B.101.2. In seiner Rechtsprechung definiert der Gerichtshof der Europäischen Union den Begriff der « schweren Kriminalität » nicht. Wie aus den Schlussanträgen des Generalstaatsanwalts vor dem vorerwähnten Urteil des Gerichtshofes der Europäischen Union, das die Große Kammer am 2. Oktober 2018 in der Sache *Ministerio Fiscal* erlassen hat, hervorgeht, fällt dieser Begriff grundsätzlich in die Zuständigkeit der Mitgliedstaaten, auch wenn der Gerichtshof der Europäischen Union die Aufgabe hat, über die Einhaltungen aller Anforderungen des Unionsrechts zu wachen und insbesondere eine kohärente Anwendung des durch die Bestimmungen der Charta gewährten Schutzes sicherzustellen. Die rechtliche

Einordnung kann nämlich nicht nur von einem Mitgliedstaat zum anderen je nach seinen Traditionen und Prioritäten variieren, sondern auch im Laufe der Zeit unter dem Einfluss der Strafrechtspolitik in Richtung einer größeren oder geringeren Strenge, um der Entwicklung der Kriminalität Rechnung zu tragen, sowie allgemeiner den gesellschaftlichen Veränderungen und den nationalen Bedürfnissen insbesondere hinsichtlich der Strafverfolgung. Außerdem kann in Bezug auf die Schwere der Strafe von der Tatsache, dass ein Mitgliedstaat eine niedrige Freiheitstrafe oder sogar eine Alternative zur Freiheitsstrafe vorsieht, nicht auf die intrinsische Schwere der betreffenden Straftat geschlossen werden (Schlussanträge des Generalanwalts Henrik Saugmandsgaard Øe, vor EuGH, Große Kammer, 2. Oktober 2018, C-207/16, vorerwähnt, Randnrn. 93-100).

Diesbezüglich hat der Gerichtshof der Europäischen Union betont, dass eine im nationalen Recht vorgenommene Definition « schwerer Straftaten », die einen Zugang zu den von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten Daten, aus denen genaue Schlüsse auf das Privatleben der betroffenen Personen gezogen werden können, ermöglichen können, nicht so weit sein darf, dass der Zugang zu diesen Daten eher zur Regel als zur Ausnahme wird. Sie kann daher nicht den Großteil der Straftaten erfassen, was der Fall wäre, wenn die Schwelle, bei deren Überschreitung die Freiheitsstrafe im Höchstmaß, mit der eine Straftat bedroht ist, es rechtfertigt, diese als schwere Straftat einzustufen, übermäßig niedrig angesetzt wäre (EuGH, Große Kammer, 30 avril 2024, C-178/22, *Procura della Repubblica presso il Tribunale di Bolzano*, ECLI:EU:C:2024:371, Randnr. 55).

B.101.3. Was die Verhältnismäßigkeit der Dauer der Vorratsspeicherung der vorerwähnten Daten betrifft, hat der Gerichtshof der Europäischen Union in seinem vorerwähnten Urteil vom 6. Oktober 2020 geurteilt, dass « die Speicherungsdauer der Daten auf das absolut Notwendige beschränkt bleiben [muss], […] allerdings verlängert werden [kann], wenn die Umstände und das mit der fraglichen Maßnahme verfolgte Ziel es rechtfertigen » (Randnr. 164).

B.102.1. Im vorliegenden Fall weist die klagende Partei nicht nach, inwiefern der Gesetzgeber den nationalen Ermessensspielraum überschritten hätte, indem er in Artikel 39*quinquies* § 1 Absatz 1 des Strafprozessgesetzbuches den Begriff « schwere Kriminalität » unter Bezugnahme auf Straftaten, die « eine Hauptkorrektionalgefängnisstrafe von einem Jahr oder eine schwerere Strafe zur Folge haben » können, definiert hat. Es ist auch

nicht ersichtlich, inwiefern diese Definition gegen die in B.99.2 genannten Referenznormen verstoßen würde. Diesbezüglich hat die Gesetzgebungsabteilung des Staatsrates in ihrem Gutachten zum Vorentwurf des Gesetzes, der dem Gesetz vom 20. Juli 2022 zugrunde liegt, nämlich gerade angemerkt, dass « sich bezüglich der Staatsanwaltschaft zum Beispiel die Einhaltung des Kriteriums ‘ schwere Kriminalität ’ ebenfalls aus dem im Entwurf befindlichen Artikel 39*quinquies* des Strafprozessgesetzbuches ergibt » (*Parl. Dok.*, Kammer, 2021-2022, DOC 55-2572/001, S. 310). Im Übrigen muss die Zuordnung einer Straftat zur schweren Kriminalität unter der Kontrolle des Strafrichters angesichts der Art der begangenen Straftat und sämtlicher Umstände des Falles konkret beurteilt werden.

Der Strafrichter muss insbesondere in der Lage sein, den Zugang zu den betreffenden Daten zu verweigern, wenn dieser im Rahmen der Verfolgung einer Straftat verlangt wird, die offensichtlich nicht schwer ist (EuGH, Große Kammer, 30. April 2024, C-178/22, vorerwähnt, ECLI:EU:C:2024:371, Randnr. 62).

B.102.2. Was die Dauer der Vorratsspeicherung der erwähnten Daten betrifft, sieht Artikel 39*quinquies* des Strafprozessgesetzbuches eine Frist vor, die sechs Monate nicht übersteigen darf, die jedoch schriftlich verlängert werden kann (Artikel 39*quinquies* § 1 Absatz 3). Die präzise Dauer der Vorratsspeicherung muss außer in Dringlichkeitsfällen schriftlich angeordnet und mit Gründen versehen werden, sodass es dem Prokurator des Königs obliegt, unter der Kontrolle des Strafrichters nachzuweisen, dass die Speicherfrist, die er anordnet, auf das absolut Notwendige beschränkt ist, und im Fall einer Verlängerung die Umstände und Ziele, die eine solche Maßnahme rechtfertigen.

B.103.1. Artikel 46*bis* des Strafprozessgesetzbuches in der durch das Gesetz vom 20. Juli 2022 abgeänderten Fassung soll es dem Prokurator des Königs ermöglichen, die Identifizierung des Teilnehmers oder gewöhnlichen Nutzers eines in Absatz 2 dieser Bestimmung erwähnten Dienstes vorzunehmen, das heißt des Dienstes, der vom « Betreiber eines elektronischen Kommunikationsnetzes » und « jeglicher Person, die auf belgischem Staatsgebiet auf irgendeine Weise einen Dienst bereitstellt oder anbietet, der in der Übertragung von Signalen über elektronische Kommunikationsnetze besteht oder durch den Nutzer dazu ermächtigt werden, über ein elektronisches Kommunikationsnetz Informationen zu erhalten, zu empfangen oder zu verbreiten » angeboten wird; hierzu zählen auch « Anbieter elektronischer Kommunikationsdienste ».

B.103.2. Aus den Vorarbeiten zum Gesetz vom 20. Juli 2022 geht hervor, dass Artikel 46*bis* des Strafprozessgesetzbuches in der durch dieses Gesetz abgeänderten Fassung so gedacht ist, dass er sich auf die in Artikel 127 des Gesetzes vom 13. Juni 2005 erwähnten Identifizierungsdaten bezieht (*Parl. Dok.*, Kammer, 2021-2022, DOC 55-2572/002, SS. 148-151).

B.103.3. Da aus den in B.48.1 bis B.48.4 erwähnten Gründen Artikel 126 des Gesetzes vom 13. Juni 2005, eingefügt durch Artikel 8 des Gesetzes vom 20. Juli 2022, nicht gegen die in B.49 genannten Referenznormen verstößt, gilt das Gleiche in Bezug auf Artikel 46*bis* des Strafprozessgesetzbuches in der durch das Gesetz vom 20. Juli 2022 abgeänderten Fassung.

B.103.4. Der Gerichtshof der Europäischen Union und der Europäische Gerichtshof für Menschenrechte verlangen weder die Schaffung einer vorherigen gerichtlichen oder administrativen Kontrolle noch die Information des Betroffenen über einen Zugang zu den Identifizierungsdaten, noch dass ein spezifisches Rechtsmittel vorgesehen wird. Somit kann dem Gesetzgeber nicht vorgeworfen werden, dass er in Artikel 46*bis* des Strafprozessgesetzbuches in der durch das Gesetz vom 20. Juli 2022 abgeänderten Fassung keine solchen Modalitäten vorgesehen hat, da sich diese Bestimmung ausschließlich auf Identifizierungsdaten bezieht. Daher ist es nicht notwendig, die von der klagenden Partei diesbezüglich angeregten Vorabentscheidungsfragen zu stellen.

B.103.5. Insofern die klagende Partei vorbringt, dass es Artikel 46*bis* des Strafprozessgesetzbuches dem Prokurator des Königs in Dringlichkeitsfällen erlaubt, auf Verkehrs- und Standortdaten zur Bekämpfung der Kriminalität allgemein zuzugreifen, entbehrt der einzige Klagegrund der faktischen Grundlage, denn – wie in B.103.2 erwähnt – bezieht sich Artikel 26 des Gesetzes vom 20. Juli 2022, der den vorerwähnten Artikel 46*bis* abändert, nur auf die Identifizierungsdaten und nicht auf die Verkehrs- und Standortdaten. Daher ist die von der klagenden Partei diesbezüglich beantragte Vorabentscheidungsfrage nicht zu stellen.

B.103.6. Schließlich legt die klagende Partei in Bezug auf die Möglichkeit des Prokurators des Königs, die Mitwirkung der geschlossenen Zentren und Unterbringungsorte, die in Artikel 46*bis* § 1 Absatz 2 zweiter Gedankenstrich des Strafprozessgesetzbuches erwähnt sind,

anzufordern, kein konkretes Element dar, das das Fehlen der Notwendigkeit der Maßnahme beweisen würde.

B.103.7. Der einzige Klagegrund in der Rechtssache Nr. 7931 ist unbegründet, insofern er sich auf die Artikel 25 und 26 des Gesetzes vom 20. Juli 2022 bezieht.

11. Die Befugnisse des Untersuchungsrichters (Artikel 27)

B.104. Der fünfte Klagegrund in der Rechtssache Nr. 7930 und der einzige Klagegrund in der Rechtssache Nr. 7931 beziehen sich auf Artikel 27 des Gesetzes vom 20. Juli 2022, der bestimmt:

« Artikel 88*bis* [des Strafprozessgesetzbuches], eingefügt durch das Gesetz vom 11. Februar 1991, ersetzt durch das Gesetz vom 10. Juni 1998 und zuletzt abgeändert durch das Gesetz vom 5. Mai 2019, wird wie folgt abgeändert:

1. Paragraph 2, ersetzt durch Artikel 9 des Gesetzes vom 29. Mai 2016, selbst für nichtig erklärt durch den Entscheid Nr. 57/2021 des Verfassungsgerichtshofs, wird wie folgt ersetzt:

‘ § 2 - In Bezug auf die Anwendung der in § 1 Absatz 1 erwähnten Maßnahme auf die Verkehrs- oder Standortdaten, die aufgrund der Artikel 126/1 und 126/3 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation gespeichert werden, gelten folgende Bestimmungen:

- Für eine in Buch 2 Titel 1*ter* des Strafgesetzbuches erwähnte Straftat kann der Untersuchungsrichter in seinem Beschluss die Daten für einen Zeitraum von zwölf Monaten vor dem Beschluss anfordern.

- Für eine andere in Artikel 90*ter* §§ 2 bis 4 erwähnte Straftat, die nicht im ersten Gedankenstrich erwähnt ist, oder für eine Straftat, die im Rahmen einer in Artikel 324*bis* des Strafgesetzbuches erwähnten kriminellen Organisation begangen worden ist, oder für eine Straftat, die eine Hauptkorrektionalgefängnisstrafe von fünf Jahren oder eine schwerere Strafe zur Folge haben kann, kann der Untersuchungsrichter in seinem Beschluss die Daten für einen Zeitraum von neun Monaten vor dem Beschluss anfordern.

- Für andere Straftaten kann der Untersuchungsrichter die Daten nur für einen Zeitraum von sechs Monaten vor dem Beschluss anfordern. ’

2. Anstelle von § 3, eingefügt durch Artikel 9 des Gesetzes vom 29. Mai 2016, selbst für nichtig erklärt durch den Entscheid Nr. 57/2021 des Verfassungsgerichtshofs, wird ein § 3 mit folgendem Wortlaut eingefügt:

‘ § 3 - Die Maßnahme darf sich nur dann auf elektronische Kommunikationsmittel eines Rechtsanwalts oder Arztes beziehen, wenn dieser selbst verdächtigt wird, eine in § 1 erwähnte Straftat begangen zu haben oder daran beteiligt gewesen zu sein, oder wenn genaue Tatsachen vermuten lassen, dass Dritte, die verdächtigt werden, eine in § 1 erwähnte Straftat begangen zu haben, seine elektronischen Kommunikationsmittel benutzen.

Die Maßnahme darf nicht durchgeführt werden, ohne dass - je nach Fall - der Präsident der Rechtsanwaltskammer oder der Vertreter der provinzialen Ärztekammer davon in Kenntnis gesetzt worden ist. Dieselben Personen werden vom Untersuchungsrichter darüber in Kenntnis gesetzt, welche Elemente seiner Meinung nach unter das Berufsgeheimnis fallen. Diese Elemente werden nicht im Protokoll festgehalten. Diese Personen unterliegen der Schweigepflicht. Jegliche Verletzung der Schweigepflicht wird gemäß Artikel 458 des Strafgesetzbuches geahndet. ’ ».

B.105.1. Die klagende Partei in der Rechtssache Nr. 7930 leitet einen fünften Klagegrund ab aus einem Verstoß gegen die Artikel 11, 12, 22 und 29 der Verfassung, an sich oder in Verbindung mit Artikel 15 Absatz 1, mit den Artikeln 5, 6 und 9 der Richtlinie 2002/58/EG, mit den Artikeln 6, 8, 10, 11 und 18 der Europäischen Menschenrechtskonvention und mit den Artikeln 13 und 54 der Richtlinie (EU) 2016/680. Sie führt an, dass Artikel 88*bis* § 3 des Strafprozessgesetzbuches in der durch das Gesetz vom 20. Juli 2022 abgeänderten Fassung eine spezifische Maßnahme in Bezug auf den Zugang zu den Daten von Rechtsanwälten und Ärzten vorsehe, die es nicht ermögliche, der Verfassungswidrigkeit der allgemeinen Vorratsdatenspeicherung als solche abzuhelfen, und dass diese Maßnahme nur den Untersuchungsrichter und nicht die anderen Behörden betreffe, die ebenfalls den Zugang zu den Daten von Rechtsanwälten, Ärzten und Journalisten verlangen könnten.

B.105.2. Die klagende Partei in der Rechtssache Nr. 7931 leitet einen einzigen Klagegrund ab aus einem Verstoß gegen die Artikel 11, 12, 22 und 29 der Verfassung, an sich oder in Verbindung mit den Artikeln 7, 8, 11, 47 und 52 Absatz 1 der Charta, mit Artikel 8 der Europäischen Menschenrechtskonvention, mit den Artikeln 5, 6 und 15 der Richtlinie 2002/58/EG und mit den Artikeln 13 und 54 der Richtlinie (EU) 2016/680. Sie führt an, dass Artikel 88*bis* § 2 des Strafprozessgesetzbuches in der durch das Gesetz vom 20. Juli 2022 abgeänderten Fassung den Zugang zu den Daten erlaube, wenn es schwerwiegende Indizien für die Begehung von Straftaten gibt, die eine Hauptkorrektionalgefängnisstrafe von einem Jahr oder eine schwerere Strafe zur Folge haben können, was in Wirklichkeit die überwiegende Mehrheit der Straftaten betreffe und sich nicht auf den Fall der schweren Kriminalität beschränke. Hilfsweise beantragt die klagende Partei, dass dem Gerichtshof der Europäischen Union zu diesem Punkt eine Vorabentscheidungsfrage gestellt wird. Außerdem beanstandet die

klagende Partei ebenfalls die fehlende Information der Person, zu deren Daten Zugang gewährt wird, und das Fehlen von Rechtsmitteln im Fall des unrechtmäßigen Zugangs zu den Daten. In Bezug auf die vorerwähnte fehlende Information beantragt sie hilfsweise, dass dem Gerichtshof der Europäischen Union eine Vorabentscheidungsfrage gestellt wird.

B.106.1. Die gegen Artikel 88*bis* des Strafprozessgesetzbuches gerichteten Beschwerdegründe der klagenden Parteien sind ausschließlich aus einem Verstoß gegen das Recht auf Achtung des Privatlebens und das Recht auf Schutz personenbezogener Daten abgeleitet, die in Artikel 22 der Verfassung, in Artikel 8 der Europäischen Menschenrechtskonvention, in den Artikeln 7, 8 und 52 Absatz 1 der Charta, in der Richtlinie 2002/58/EG und in der Richtlinie (EU) 2016/680 gewährleistet sind.

B.106.2. Der Gerichtshof prüft zunächst die gegen Absatz 2 von Artikel 88*bis* des Strafprozessgesetzbuches gerichteten Beschwerdegründe, sodann die zu Absatz 3 dieser Bestimmung.

B.107.1. Artikel 88*bis* § 2 des Strafprozessgesetzbuches bezieht sich auf den Zugang des Untersuchungsrichters zu den aufgrund der Artikel 126/1 und 126/3 des Gesetzes vom 13. Juni 2005 gespeicherten Daten, das heißt zu den Verkehrs- und Standortdaten (siehe *Parl. Dok.*, Kammer, 2021-2022, DOC 55-2572/001, S. 145).

B.107.2. Was die Zwecke betrifft, erlaubt Artikel 88*bis* § 2 des Strafprozessgesetzbuches, abgeändert durch Artikel 27 des Gesetzes vom 20. Juli 2022, einen Zugang des Untersuchungsrichters zu den gespeicherten Daten, wenn es schwerwiegende Indizien für die Begehung von Straftaten gibt, die eine Hauptkorrektionalgefängnisstrafe von einem Jahr oder eine schwerere Strafe zur Folge haben können.

Wie in B.102.1 erwähnt, weist die klagende Partei nicht nach, inwiefern der Gesetzgeber seinen Ermessensspielraum überschritten hätte, indem er in Artikel 88*bis* § 2 des Strafprozessgesetzbuches den Begriff « schwere Kriminalität » unter Bezugnahme auf Straftaten, die « eine Hauptkorrektionalgefängnisstrafe von einem Jahr oder eine schwerere Strafe zur Folge haben » können, definiert hat. Diese Definition verstößt nicht gegen die in B.105.2 genannten Referenznormen. Im Übrigen muss die Zuordnung einer Straftat zur

schweren Kriminalität unter der Kontrolle des Strafrichters angesichts der Art der begangenen Straftat und sämtlicher Umstände des Falles konkret beurteilt werden.

B.107.3. Die klagenden Parteien beanstanden ebenfalls die fehlende Information der Person, zu deren Daten Zugang gewährt wird, und das Fehlen von Rechtsmitteln im Fall des unrechtmäßigen Zugangs zu den Daten.

Es ist zwar zutreffend, dass Artikel 88*bis* § 2 des Strafprozessgesetzbuches keine spezifische gerichtliche Kontrolle des Zugangs des Untersuchungsrichters zu den aufgrund der Artikel 126/1 und 126/3 gespeicherten Daten vorsieht, aber es ist wichtig festzustellen, dass der Untersuchungsrichter ein unabhängiger und unparteiischer Magistrat ist, dessen Eingreifen eine wesentliche Garantie für die Einhaltung der Bedingungen ist, denen eine Beeinträchtigung des Rechts auf Achtung des Privatlebens unterworfen ist. Auch wenn die Entscheidungen, die er trifft, keine materielle Rechtskraft haben, gehören sie zur Ausübung der Rechtsprechungsfunktion und sind Bestandteil eines Gerichtsverfahrens.

Außerdem sind die gemeinrechtlichen Rechtsmittel gegen einen Beschluss des Untersuchungsrichters auf diesem Gebiet ausreichend. Es ist insbesondere festzustellen, dass ein Angeklagter im Rahmen des Strafverfahrens diesbezüglich das Recht besitzt, bei den Untersuchungsgerichten oder beim erkennenden Gericht die Nichtigkeit einer Untersuchungshandlung, die gegen sein Recht auf Achtung des Privatlebens oder sein Recht auf ein faires Verfahren verstößt, geltend zu machen. Außerdem kann ein Interessehabender aufgrund von Artikel 58 des Gesetzes vom 3. Dezember 2017 « zur Schaffung der Datenschutzbehörde » im Fall einer unrechtmäßigen Verarbeitung seiner personenbezogenen Daten kostenlos eine Beschwerde bei der Datenschutzbehörde einreichen.

Was die Information der betroffenen Person betrifft, so erfolgt sie gemäß den auf gerichtliche Untersuchungen anwendbaren Regeln des Strafprozessgesetzbuches.

B.107.4. Der einzige Klagegrund in der Rechtssache Nr. 7931 ist unbegründet, insofern er sich auf Artikel 88*bis* § 2 des Strafprozessgesetzbuches bezieht.

B.108.1. Was Artikel 88*bis* § 3 des Strafprozessgesetzbuches betrifft, beziehen sich die Beschwerdegründe der klagenden Partei in der Rechtssache Nr. 7930 in Wirklichkeit nicht auf

diese Bestimmung. « Die Maßnahme der allgemeinen Vorratsdatenspeicherung als solche », auf die sich die klagende Partei bezieht, ist nämlich nicht durch Artikel 88*bis* § 3 geregelt und außerdem kann der Umstand, dass das von dieser Bestimmung vorgesehene System nicht auf die « anderen Behörden », die den Zugang zu den Daten von Rechtsanwälten, Ärzten und Journalisten verlangen können, ausgedehnt wird, nicht auf Artikel 88*bis* zurückgeführt werden, denn dieser grenzt nur die Befugnisse des Untersuchungsrichters und in Fällen der Entdeckung auf frischer Tat des Prokurator des Königs ein (Paragraph 1 Absatz 1).

B.108.2. Der fünfte Klagegrund in der Rechtssache Nr. 7930 ist unbegründet, insofern er aus einem Verstoß gegen Artikel 20 Nr. 2 des Gesetzes vom 20. Juli 2022 abgeleitet ist.

12. Die Befugnisse der Nachrichten- und Sicherheitsdienste (Artikel 33, 34 und 37)

B.109.1. Der erste Klagegrund in der Rechtssache Nr. 7932 bezieht sich insbesondere auf die Artikel 33, 34 und 37 des Gesetzes vom 20. Juli 2022.

B.109.2. Artikel 33 des Gesetzes vom 20. Juli 2022 ändert das Gesetz vom 30. November 1998 ab, indem er einen Artikel 13/6 einfügt, der bestimmt:

« § 1er. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, requérir le concours d'un opérateur de réseaux de communications électroniques ou d'un fournisseur de services de communications électroniques pour procéder à :

1° la conservation des données de trafic et de localisation de moyens de communications électroniques qui sont à sa disposition au moment de la réquisition;

2° la conservation des données de trafic et de localisation qu'il génère et traite à partir de la réquisition.

La réquisition visée à l'alinéa 1er repose sur une décision écrite et motivée du dirigeant du service ou de son délégué.

§ 2. La réquisition visée au paragraphe 1er, alinéa 1er, mentionne :

1° la nature des données de trafic et de localisation à conserver;

2° les personnes, les groupements, les zones géographiques, les moyens de communication et/ou le mode d'utilisation dont les données de trafic et de localisation doivent être conservées;

3° pour la mesure visée au paragraphe 1er, alinéa 1er, 1°, le délai de conservation des données, qui ne peut excéder six mois à compter de la date de la réquisition, sans préjudice de la possibilité de prolongation en suivant la même procédure;

4° pour la mesure visée au paragraphe 1er, alinéa 1er, 2° :

- la durée de la mesure, qui ne peut excéder six mois à compter de la date de la réquisition, sans préjudice de la possibilité de prolongation en suivant la même procédure;

- le délai de conservation des données, qui ne peut excéder six mois à compter de la date de la communication, sans préjudice de la possibilité de prolongation en suivant la même procédure;

5° la date de la réquisition;

6° la signature du dirigeant du service ou de son délégué.

§ 3. En cas d'extrême urgence, le dirigeant du service ou son délégué peut requérir la conservation verbalement. Cette réquisition verbale est confirmée par écrit au plus tard le premier jour ouvrable qui suit.

§ 4. Les services de renseignement et de sécurité tiennent un registre de toutes les réquisitions de conservation.

Chaque décision de réquisition est notifiée avec sa motivation au Comité permanent R. Lorsqu'il constate une illégalité, le Comité permanent R met fin à la réquisition.

Lorsqu'il est mis fin prématurément à la réquisition, l'opérateur d'un réseau de communications électroniques ou le fournisseur d'un service de communications électroniques requis en est averti le plus rapidement possible.

§ 5. Pour l'exécution de la réquisition, le dirigeant du service ou son délégué peut requérir le concours de l'Institut visé à l'article 2, 1°, de la loi du 13 juin 2005 relative aux communications électroniques, ainsi que des personnes dont il présume qu'elles ont une expertise technique utile. Cette réquisition est écrite et mentionne la base légale.

§ 6. Toute personne qui refuse de prêter son concours aux réquisitions visées aux paragraphes 1er et 5 est punie d'une amende de vingt-six euros à vingt mille euros.

§ 7. Le Roi peut déterminer, sur proposition du ministre de la Justice, du ministre de la Défense et du ministre qui a les Communications électroniques dans ses attributions, les modalités de collaboration des opérateurs d'un réseau de communications électroniques ou des fournisseurs d'un service de communications électroniques ».

Artikel 34 des Gesetzes vom 20. Juli 2022 ändert das Gesetz vom 30. November 1998 ab, indem er einen Artikel 13/7 einfügt, der bestimmt:

« § 1er. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions et lorsqu'il existe une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, requérir le concours des opérateurs d'un réseau de communications électroniques et des fournisseurs d'un service de communications électroniques afin de procéder à la conservation généralisée et indifférenciée des données de trafic et de localisation de moyens de communications électroniques générées et traitées par eux.

§ 2. La réquisition visée au paragraphe 1er ne peut avoir lieu qu'avec l'accord écrit préalable de la commission. La commission donne son accord dans les quatre jours suivant la réception de la demande écrite et motivée du dirigeant du service.

§ 3. La demande du dirigeant du service de requérir la conservation mentionne, sous peine d'illégalité :

1° la menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible;

2° les circonstances de fait qui justifient la conservation généralisée et indifférenciée des données de trafic et de localisation;

3° la nature des données de trafic et de localisation à conserver;

4° la durée de la mesure de conservation, qui ne peut excéder six mois à compter de la date de la réquisition. Elle peut être prolongée en suivant la même procédure;

5° le délai de conservation des données, qui ne peut excéder six mois à compter de la date de la communication. Il peut être prolongé en suivant la même procédure;

6° le cas échéant, les motifs qui justifient l'extrême urgence visée au paragraphe 5;

7° la date de la demande;

8° la signature du dirigeant du service.

§ 4. La réquisition visée au paragraphe 1er mentionne :

1° la date de l'accord de la commission;

2° la nature des données de trafic et de localisation à conserver;

3° la durée de la mesure et le délai de conservation des données;

4° la date de la réquisition;

5° la signature du dirigeant du service ou de son délégué.

§ 5. En cas d'extrême urgence, le dirigeant du service demande l'accord verbal préalable du président de la commission ou, en cas d'indisponibilité, d'un autre membre de la commission. L'auteur de l'accord en informe immédiatement les autres membres de la commission. Le dirigeant du service confirme sa demande par écrit dans les vingt-quatre heures

suivant l'accord. Le président ou le membre contacté confirme également son accord par écrit le plus rapidement possible. Cet accord est valable cinq jours.

§ 6. La réquisition de conservation généralisée et indifférenciée est confirmée par arrêté royal.

L'arrêté royal ne mentionne que :

1° la date de l'accord de la commission;

2° la date de la réquisition;

3° la nature des données de trafic et de localisation à conserver;

4° la durée de la mesure et le délai de conservation des données.

En l'absence de confirmation par arrêté royal dans le mois de la réquisition, cette réquisition prend fin.

Les opérateurs d'un réseau de communications électroniques et les fournisseurs d'un service de communications électroniques requis en sont avertis le plus rapidement possible.

§ 7. Pour l'exécution de la réquisition, le dirigeant du service peut requérir le concours de l'Institut visé à l'article 2, 1°, de la loi du 13 juin 2005 relative aux communications électroniques, ainsi que des personnes dont il présume qu'elles ont une expertise technique utile. Cette réquisition est écrite et mentionne la base légale et l'accord de la commission.

§ 8. Toute personne qui refuse de prêter son concours aux réquisitions visées aux paragraphes 1er et 7 est punie d'une amende de vingt-six euros à vingt mille euros.

§ 9. La commission transmet sans délai la demande du dirigeant du service et son accord au Comité permanent R.

§ 10. Le service de renseignement et de sécurité fait rapport à la commission toutes les deux semaines sur l'évolution de la menace. Ce rapport met en évidence les éléments qui justifient soit le maintien de la conservation généralisée et indifférenciée, soit la fin de celle-ci.

§ 11. Le dirigeant du service met fin à la réquisition, nonobstant la confirmation par arrêté royal, lorsque la conservation n'est plus utile pour lutter contre la menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, lorsque cette menace a disparu ou lorsqu'il constate une illégalité.

Lorsque la commission ou le Comité permanent R constate une illégalité, il est mis fin à la réquisition nonobstant la confirmation par arrêté royal.

Lorsqu'il est mis fin prématurément à la réquisition, les opérateurs d'un réseau de communications électroniques ou les fournisseurs d'un service de communications électroniques requis en sont avertis le plus rapidement possible.

§ 12. Le Roi détermine, sur proposition du ministre de la Justice, du ministre de la Défense et du ministre qui a les Communications électroniques dans ses attributions, les modalités de collaboration des opérateurs d'un réseau de communications électroniques ou des fournisseurs d'un service de communications électroniques ».

Artikel 37 des Gesetzes vom 20. Juli 2022 ersetzt Artikel 18/8 des Gesetzes vom 30. November 1998, der nunmehr bestimmt:

« § 1er. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, au besoin en requérant à cette fin le concours technique de l'opérateur d'un réseau de communications électroniques ou du fournisseur d'un service de communications électroniques, procéder ou faire procéder :

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

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

Dans les cas visés à l'alinéa 1er et pour chaque moyen de communication électronique dont les données de trafic sont repérées ou dont l'origine ou la destination de la communication électronique est localisée, le jour, l'heure et la durée ainsi que, si nécessaire, le lieu de la communication électronique sont indiqués et consignés dans un rapport.

La nature de la décision est communiquée à l'opérateur requis du réseau de communications électroniques ou au fournisseur du service de communications électroniques qui est requis.

§ 2. [...]

§ 3. Tout opérateur d'un réseau de communications électroniques et tout fournisseur d'un service de communications électroniques qui est requis de communiquer les données visées au paragraphe 1er donne au dirigeant du service les données qui ont été demandées dans un délai et selon les modalités à fixer par un arrêté royal pris sur la proposition du ministre de la Justice, du ministre de la Défense et du ministre qui a les Communications électroniques dans ses attributions.

Toute personne visée à l'alinéa 1er qui refuse de prêter son concours technique aux réquisitions visées au présent article est punie d'une amende de vingt-six euros à vingt mille euros.

§ 4. [...] ».

B.109.3. Der erste Klagegrund in der Rechtssache Nr. 7932 ist abgeleitet aus einem Verstoß gegen die Artikel 10, 11, 13, 15, 22, 23 und 29 der Verfassung, an sich oder in Verbindung mit den Artikeln 5, 6, 8, 9, 10, 11, 14 und 18 der Europäischen

Menschenrechtskonvention, mit den Artikeln 7, 8, 11, 47 und 52 der Charta, mit Artikel 5 Absatz 4 des Vertrags über die Europäische Union und mit Artikel 6 der Richtlinie 2002/58/EG, mit der Richtlinie (EU) 2016/680 und mit der DSGVO.

Im einem vierten Teil führen die klagenden Parteien an, dass Artikel 13/6 des Gesetzes vom 30. November 1998 gegen den Grundsatz der Vorhersehbarkeit, der in Artikel 22 der Verfassung gewährleistet ist, verstoße, insofern er die Verkehrs- und Standortdaten, auf die er sich bezieht, nicht genau beschreibe. Außerdem führen sie an sie, dass Artikel 13/6 nicht mit der Rechtsprechung des Gerichtshofes der Europäischen Union im Einklang stehe, insofern er einerseits eine Vorratsspeicherungspflicht vorsehe, die über das hinausgehe, was absolut notwendig sei, und in Wirklichkeit einer allgemeinen und unterschiedslosen Vorratsdatenspeicherung gleichkomme, und insofern er andererseits weder ein Rechtsmittel noch die Notifizierung der Vorratsdatenspeicherung noch das Eingreifen eines Richters noch die Löschung der gesammelten Daten, wenn die Anforderung durch den Ständigen Ausschuss N wegen einer Rechtswidrigkeit vorzeitig beendet werde, festlege.

Im einem fünften Teil führen die klagenden Parteien an, dass Artikel 13/7 des Gesetzes vom 30. November 1998 das Kriterium der Vorhersehbarkeit, das sich aus Artikel 22 der Verfassung und der Rechtsprechung des Gerichtshofes der Europäischen Union ergebe, nicht erfülle, insofern er den darin genannten Begriff der « Verkehrs- und Standortdaten » nicht definiere. Außerdem behaupten sie, dass keine Notifizierung der Betroffenen vorgesehen sei, was die Möglichkeit erschwere, die Einmischung in das Recht auf Achtung des Privatlebens anzufechten. Schließlich führen sie an, dass Artikel 13/7 im Gegensatz zu dem, was der Gerichtshof der Europäischen Union verlange, keine Löschung der auf Vorrat gespeicherten Daten im Fall der Rechtswidrigkeit der Maßnahme vorsehe.

Im einem sechsten Teil führen die klagenden Parteien an, dass Artikel 13/8 des Gesetzes vom 30. November 1998 weder den darin genannten Begriff « Verkehrs- und Standortdaten » definiere noch die Dauer der Speicherungsmaßnahme festlege, was gegen den Grundsatz der Vorhersehbarkeit, der in Artikel 22 der Verfassung und durch die Rechtsprechung des Gerichtshofes der Europäischen Union gewährleistet sei, verstoße. Außerdem behaupten die klagenden Parteien, dass Artikel 18/8 im Gegensatz zu dem, was der Gerichtshof der Europäischen Union verlange, keine Kontrolle in Bezug auf die Notwendigkeit der Maßnahme vorsehe.

B.109.4. In Anbetracht ihres Zusammenhangs werden diese Teile zusammen geprüft.

B.110. Aus dem in B.109.2 Erwähnten geht hervor, dass sich die gegen die Artikel 13/6, 13/7 und 18/8 des Gesetzes vom 30. November 1998 gerichteten Beschwerdegründe der klagenden Parteien im Wesentlichen auf die Vereinbarkeit dieser Bestimmungen mit dem Recht auf Achtung des Privatlebens und dem Recht auf Schutz personenbezogener Daten beziehen.

B.111.1. Aufgrund von Artikel 1 Absatz 3 der Richtlinie 2002/58/EG « gilt [diese Richtlinie] nicht für Tätigkeiten, die nicht in den Anwendungsbereich des Vertrags zur Gründung der Europäischen Gemeinschaft fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des Vertrags über die Europäische Union, und auf keinen Fall für Tätigkeiten betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Tätigkeit die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich ».

Aufgrund von Artikel 2 Absatz 2 Buchstabe a des DSGVO findet « [diese Verordnung] keine Anwendung auf die Verarbeitung personenbezogener Daten im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt ». Aufgrund von Artikel 2 Absatz 2 Buchstabe d der DSGVO findet sie auch keine Anwendung auf die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke des Schutzes vor und der Abwehr von Gefahren für die öffentlichen Sicherheit.

Aufgrund von Artikel 2 Absatz 3 Buchstabe a der Richtlinie (EU) 2016/680 findet diese Richtlinie keine Anwendung auf die Verarbeitung personenbezogener Daten « im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrecht fällt ».

Im vorerwähnten Urteil vom 6. Oktober 2020 hat der Gerichtshof der Europäischen Union entschieden:

« Insoweit ist zunächst festzustellen, dass nach Artikel 4 Absatz 2 EUV die nationale Sicherheit weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten fällt. Diese Verantwortung entspricht dem zentralen Anliegen, die wesentlichen Funktionen des Staates und die grundlegenden Interessen der Gesellschaft zu schützen, und umfasst die Verhütung und Repression von Tätigkeiten, die geeignet sind, die tragenden Strukturen eines Landes im

Bereich der Verfassung, Politik oder Wirtschaft oder im sozialen Bereich in schwerwiegender Weise zu destabilisieren und insbesondere die Gesellschaft, die Bevölkerung oder den Staat als solchen unmittelbar zu bedrohen, wie insbesondere terroristische Aktivitäten » (Randnr. 135).

B.111.2. Aufgrund der Artikel 13/6, 13/7 und 18/8 des Gesetzes vom 30. November 1998 können die Nachrichten- und Sicherheitsdienste im Interesse der Erfüllung ihrer Aufträge die Mitwirkung eines Betreibers eines elektronischen Kommunikationsnetzes oder eines Anbieters eines elektronischen Kommunikationsdienstes anfordern, damit er die Aufbewahrung und Übermittlung von Verkehrs- und Standortdaten vornimmt.

B.111.3. Da die Artikel 13/6, 13/7 und 18/8 des Gesetzes vom 30. November 1998 nur im Rahmen der Aufträge der Nachrichten- und Sicherheitsdienste Anwendung finden, fallen sie nicht unter den Anwendungsbereich des Rechts der Europäischen Union. Der Klagegrund ist daher unzulässig, insoweit er aus einem Verstoß gegen die geltend gemachten Bestimmungen des Vertrags über die Europäische Union, der Charta, der DSGVO, der Richtlinie (EU) 2016/680 oder der Richtlinie 2002/58/EG, wie sie durch die Rechtsprechung des Gerichtshofes der Europäischen Union ausgelegt werden, abgeleitet ist.

B.112.1. Die anderen Beschwerdegründe der klagenden Parteien zu den Artikeln 13/6, 13/7 und 18/8 des Gesetzes vom 30. November 1998 sind aus einem Verstoß gegen Artikel 22 der Verfassung abgeleitet.

B.112.2. Wie in B.11.3 erwähnt, hat der Verfassunggeber eine möglichst weitgehende Übereinstimmung zwischen Artikel 22 der Verfassung und Artikel 8 der Europäischen Menschenrechtskonvention angestrebt (*Parl. Dok.*, Kammer, 1992-1993, Nr. 997/5, S. 2).

Die Tragweite dieses Artikels 8 ist analog zu derjenigen der vorerwähnten Verfassungsbestimmung, weshalb die Garantien, die durch diese beiden Bestimmungen geboten werden, ein untrennbares Ganzes bilden.

B.112.3. Außerdem behält Artikel 22 der Verfassung, wie in B.24.1 und B.24.2 dargelegt, dem zuständigen Gesetzgeber die Befugnis vor, festzulegen, in welchen Fällen und unter welchen Bedingungen das Recht auf Achtung des Privatlebens beeinträchtigt werden darf. Er garantiert es so jedem Bürger, dass eine Einmischung in die Ausübung dieses Rechts nur aufgrund von Regeln erfolgen darf, die durch eine demokratisch gewählte beratende

Versammlung angenommen wurden. In diesem Zusammenhang müssen die wesentlichen Elemente der Verarbeitung personenbezogener Daten im Gesetz, im Dekret oder in der Ordonnanz selbst festgelegt sein. Diesbezüglich sind die wesentlichen Elemente unabhängig von dem betroffenen Bereich grundsätzlich die folgenden Elemente: (1) die Kategorie der verarbeiteten Daten, (2) die betroffene Personenkategorie, (3) der mit der Verarbeitung verfolgte Zweck, (4) die Kategorie der Personen, die Zugriff auf die verarbeiteten Daten haben, und (5) die maximale Dauer der Aufbewahrung der Daten.

Neben dem formellen Legalitätserfordernis wird durch Artikel 22 der Verfassung in Verbindung mit Artikel 8 der Europäischen Menschenrechtskonvention die Verpflichtung auferlegt, dass die Einmischung in das Recht auf Achtung des Privatlebens und das Recht auf Schutz personenbezogener Daten deutlich und ausreichend präzise formuliert wird, damit es möglich ist, die Fälle vorherzusehen, in denen der Gesetzgeber eine solche Einmischung erlaubt. Auf dem Gebiet des Datenschutzes bedeutet dieses Erfordernis der Vorhersehbarkeit, dass ausreichend präzise vorgesehen werden muss, unter welchen Umständen Verarbeitungen von personenbezogenen Daten erlaubt sind. Deshalb muss es jeder Person möglich sein, sich ein ausreichend klares Bild von den verarbeiteten Daten, den von einer bestimmten Datenverarbeitung betroffenen Personen sowie den Bedingungen und den Zwecken der Verarbeitung zu machen.

B.113.1. Die Artikel 13/6, 13/7 und 18/8 des Gesetzes vom 30. November 1998 sehen vor, dass die Nachrichtendienste im Interesse der Erfüllung ihrer Aufträge die Mitwirkung eines Betreibers eines elektronischen Kommunikationsnetzes oder eines Anbieters eines elektronischen Kommunikationsdienstes anfordern können, damit er die Aufbewahrung und Übermittlung der « Verkehrs- und Standortdaten » vornimmt. Dadurch hat der Gesetzgeber das formelle Legalitätsprinzip, das in Artikel 22 der Verfassung gewährleistet ist, eingehalten, da er die verarbeiteten Datenkategorien präzisiert hat.

B.113.2. Überdies sind in den Artikeln 13/6, 13/7 und 18/8 des Gesetzes vom 30. November 1998 die Verkehrs- und Standortdaten, die die Nachrichtendienste speichern und verarbeiten dürfen, sowie die Bedingungen und Modalitäten dieser Aktivitäten klar und detailliert dargelegt, was es den betroffenen Personen ermöglicht, die Fälle ausreichend vorherzusehen, in denen der Gesetzgeber eine Einmischung in das Recht auf Achtung des Privatlebens und in das Recht auf Schutz personenbezogener Daten erlaubt.

B.114. Schließlich betrifft die in Artikel 18/8 des Gesetzes vom 30. November 1998 vorgesehene Maßnahme die Erfassung oder die Lokalisierung von Daten und nicht ihre Speicherung.

Im Kommentar zu den Artikeln heißt es nämlich zu diesem Punkt:

« Cet article 18/8 porte sur l'accès aux données de communications électroniques par les services de renseignement et de sécurité et non sur la conservation de ces données.

[…].

[...] [I]l convient de préciser qu'aucune modification n'est apportée à l'accès par les services de renseignement et de sécurité aux données de communications électroniques, ni à ses modalités.

La seule modification de l'article 18/8 consiste en la suppression du paragraphe 2 annulé par la Cour constitutionnelle.

L'accès aux données par les services de renseignement et de sécurité visé à l'article 18/8 porte bien entendu sur toutes les données conservées par les opérateurs, peu importe pour quelle finalité.

[...]

En réponse à un commentaire du Comité permanent R (points 16-18), les auteurs du projet souhaitent souligner qu'il n'y a plus de raison de moduler l'accès aux données, puisque l'accès dépendra de la durée de conservation effective et modulée. En outre, l'accès devra toujours être motivé de sorte que la Commission et le Comité permanent R puissent vérifier la proportionnalité, la subsidiarité et la légalité de l'historique demandé. Cette obligation de motivation a en effet été réintroduite, à la demande du Comité, à l'article 18/3, 2, 12 » (*Parl. Dok.*, Kammer, 2021-2022, DOC 55-2572/001, SS. 163-164).

Daraus folgt, dass der sechste Teil des ersten Klagegrunds in der Rechtssache Nr. 7932, der sich auf die Vorratsdatenspeicherung bezieht, unbegründet ist.

B.115. Der vierte, der fünfte und der sechste Teil des ersten Klagegrunds in der Rechtssache Nr. 7932 sind unbegründet.

13. Das Inkrafttreten (Artikel 45)

B.116.1. Der dritte Klagegrund in der Rechtssache Nr. 7930 bezieht sich auf Artikel 45 des Gesetzes vom 20. Juli 2022, der bestimmt:

« La conservation ciblée des données sur la base des critères visés à l'article 126/3, §§ 3 à 5, de la loi du 13 juin 2005 relative aux communications électroniques, entre en vigueur à la date fixée par le Roi par arrêté délibéré en Conseil des ministres, et au plus tard le 1er janvier 2027.

Pour la première application de l'article 126/3, §§ 3 à 5, de la loi du 13 juin 2005 relative aux communications électroniques, les autorités compétentes visées à l'article 126/3, § 6, alinéa 2, de la même loi, transmettent les informations nécessaires au service désigné par le Roi à une date fixée par l'arrêté royal visé à l'alinéa 1er et au plus tard le 1er janvier 2026 ».

B.116.2. Der dritte Klagegrund in der Rechtssache Nr. 7930 ist abgeleitet aus einem Verstoß gegen die Artikel 11, 12, 22 und 29 der Verfassung, gegen Artikel 15 Absatz 1 und gegen die Artikel 5, 6 und 9 der Richtlinie 2002/58/EG, gelesen im Lichte der Artikel 7, 8, 11, 47 und 52 Absatz 1 der Charta, der Artikel 6, 8, 10, 11 und 18 der Europäischen Menschenrechtskonvention und der Artikel 13 und 54 der Richtlinie (EU) 2016/680. Die klagende Partei führt an, dass das von Artikel 45 geregelte Inkrafttreten gegen das Legalitätsprinzip, das in Artikel 22 der Verfassung gewährleistet ist, verstoße.

B.116.3. Aus der Darlegung des Klagegrunds ist nicht ersichtlich, inwiefern gegen das vorerwähnte Legalitätsprinzip verstoßen würde. Der Klagegrund ist unbegründet.

14. Der Schutz des Berufsgeheimnisses

B.117.1. Der einzige Klagegrund in der Rechtssache Nr. 7907, der einzige Klagegrund in der Rechtssache Nr. 7929, der zweite und der fünfte Klagegrund in der Rechtssache Nr. 7930 sowie der siebte Teil des dritten Klagegrunds und der dritte Teil des dritten Klagegrunds in der Rechtssache Nr. 7932 beziehen sich auf den fehlenden Schutz von Informationen, die dem Berufsgeheimnis unterliegen.

B.117.2.1. Der einzige Klagegrund in der Rechtssache Nr. 7907, der aus einem Verstoß gegen Artikel 10 und 11 der Verfassung, an sich oder in Verbindung mit den Artikeln 6 und 8

der Europäischen Menschenrechtskonvention und mit den Artikeln 7, 8 und 47 der Charta, abgeleitet ist, bezieht sich auf die Artikel 5 Nrn. 4 und 6, 8 bis 11, 13 bis 15, 19, 21, 22, 24 bis 42 und 44 des Gesetzes vom 20. Juli 2022.

Insbesondere führt die klagende Partei an, dass in den angefochtenen Bestimmungen einerseits die Nutzer, die Träger des Berufsgeheimnisses seien, und andererseits die Daten, die dem Berufsgeheimnis unterlägen, nicht oder zumindest nicht ausreichend von den anderen Nutzern bzw. von den anderen Daten unterschieden würden. Was insbesondere Artikel 27 des Gesetzes vom 20. Juli 2022 betrifft, behauptet die klagende Partei, dass sich diese Bestimmung nur auf die Kommunikation beziehe, die von einem Rechtsanwalt oder einem Arzt ausgehe, aber nicht auf diejenige, die vom Klienten oder Patienten stamme, wodurch es nicht möglich sei, den Trägern des Berufsgeheimnisses eine angemessene spezifische Behandlung vorzubehalten (erster und zweiter Teil). Außerdem führt die klagende Partei an, dass die angefochtenen Bestimmungen zu einer allgemeinen Überwachung sämtlicher Bürger führten (dritter Teil) und dass sie nicht im Verhältnis zum verfolgten Ziel stünden (vierter Teil).

B.117.2.2. Der einzige Klagegrund in der Rechtssache Nr. 7929 ist abgeleitet aus einem Verstoß gegen die Artikel 10 und 11 der Verfassung, an sich oder in Verbindung mit den Artikeln 6 und 8 der Europäischen Menschenrechtskonvention und mit den Artikeln 7, 8, 11 und 47 der Charta. Dieser Klagegrund bezieht sich auf die Artikel 2 bis 17 des Gesetzes vom 20. Juli 2022.

Im Wesentlichen führen die klagenden Parteien an, dass die angefochtenen Bestimmungen die Nutzer von Telekommunikationsdiensten oder elektronischen Kommunikationsdiensten, die dem Berufsgeheimnis unterliegen, insbesondere die Wirtschafts- und Steuerprüfer, einerseits und die anderen Nutzer dieser Dienste andererseits gleich behandelten, ohne dass die grundlegende Bedeutung des Berufsgeheimnisses berücksichtigt werde.

B.117.2.3. Der zweite Klagegrund in der Rechtssache Nr. 7930, der aus einem Verstoß gegen die Artikel 10, 11, 22 und 29 der Verfassung, an sich oder in Verbindung mit den Artikeln 15 Absatz 1, 5, 6 und 9 der Richtlinie 2002/58/EG, gelesen im Lichte der Artikel 7, 8, 11, 47 und 52 Absatz 1 der Charta, mit den Artikeln 6, 8, 10, 11 und 18 der Europäischen Menschenrechtskonvention und mit den Artikeln 13 und 54 der Richtlinie (EU) 2016/680 abgeleitet ist, bezieht sich auf die Artikel 5, 6, 8, 9, 10 und 12 des Gesetzes vom 20. Juli 2022,

insofern diese Bestimmungen keine Ausnahme in Bezug auf die Vorratsspeicherung von Daten und den Zugang zu ihnen für Ärzte, Rechtsanwälte oder Journalisten vorsähen.

Der fünfte Klagegrund in der Rechtssache Nr. 7930, der aus einem Verstoß gegen die Artikel 10, 11, 22 und 29 der Verfassung, an sich oder in Verbindung mit den Artikeln 15 Absatz 1, 5, 6 und 9 der Richtlinie 2002/58/EG, gelesen im Lichte der Artikel 7, 8, 11, 47 und 52 Absatz 1 der Charta, mit den Artikeln 6, 8, 10, 11 und 18 der Europäischen Menschenrechtskonvention und mit den Artikeln 13 und 54 der Richtlinie (EU) 2016/680 abgeleitet ist, bezieht sich auf das Gesetz vom 20. Juli 2022 insgesamt, insofern es keinen sachdienlichen Kontrollmechanismus vorsehe, der es den Begünstigten des Berufsgeheimnisses ermögliche, dem Sammeln, der Vorratsspeicherung oder der Kenntnisnahme ihrer Daten zu widersprechen.

B.117.2.4. Der siebte Teil des ersten Klagegrunds in der Rechtssache Nr. 7932, der aus einem Verstoß gegen die Artikel 10, 11, 13, 15, 22, 23 und 29 der Verfassung, an sich oder in Verbindung mit den Artikeln 5, 6, 8, 9, 10, 11, 14 und 18 der Europäischen Menschenrechtskonvention, mit den Artikeln 7, 8, 11, 47 und 52 der Charta, mit Artikel 5 Absatz 4 des Vertrags über die Europäische Union sowie mit der Artikel 6 der Richtlinie 2002/58/EG, mit der Richtlinie (EU) 2016/680 und mit der DSGVO abgeleitet ist, bezieht sich auf das Gesetz vom 20. Juli 2022, insofern es keine besondere Behandlung für die Vorratsspeicherung der Verkehrs- und Standortdaten von Rechtsanwälten, Ärzten und Journalisten vorsehe, obgleich es sich um sensible Daten handele, die unter das Berufsgeheimnis fielen.

Der dritte Teil des dritten Klagegrunds in dieser Rechtssache, der aus einem Verstoß gegen die Artikel 10, 11, 13, 15, 22, 23 und 29 der Verfassung, an sich oder in Verbindung mit den Artikeln 5, 6, 8, 9, 10, 11, 14 und 18 der Europäischen Menschenrechtskonvention, mit den Artikeln 7, 8, 11, 47 und 52 der Charta, mit Artikel 5 Absatz 4 des Vertrags über die Europäische Union sowie mit der Artikel 6 der Richtlinie 2002/58/EG, mit der Richtlinie (EU) 2016/680 und mit der DSGVO abgeleitet ist, bezieht sich auf das Gesetz vom 20. Juli 2022, insofern es keinen besonderen Schutz für den Zugang zu den Daten von Rechtsanwälten, Ärzten und Journalisten vorsehe. Die klagenden Parteien führen außerdem an, dass die vorerwähnten Daten unterschiedlich behandelt würden, je nachdem, ob der Zugang zu den Daten auf der Grundlage von Artikel 27 des Gesetzes vom 20. Juli 2022 erfolge oder nicht.

B.117.3. Wegen ihres Zusammenhangs prüft der Gerichtshof die vorerwähnten Klagegründe und Teile zusammen.

B.118. Artikel 88*bis* des Strafprozessgesetzbuches, abgeändert durch das angefochtene Gesetz, bestimmt:

« § 1. Wenn es schwerwiegende Indizien dafür gibt, dass die Straftaten eine Hauptkorrektionalgefängnisstrafe von einem Jahr oder eine schwerere Strafe zur Folge haben können, und wenn der Untersuchungsrichter der Meinung ist, dass es Umstände gibt, die die Erfassung von elektronischen Nachrichten oder die Lokalisierung der Herkunft oder der Bestimmung von elektronischen Nachrichten notwendig machen, um die Wahrheit herauszufinden, kann er Folgendes vornehmen lassen:

1. die Erfassung der Verkehrsdaten von elektronischen Kommunikationsmitteln, von denen elektronische Nachrichten ausgehen oder ausgingen beziehungsweise an die elektronische Nachrichten gerichtet sind oder waren,

2. die Lokalisierung der Herkunft oder der Bestimmung von elektronischen Nachrichten.

Hierfür kann er erforderlichenfalls unmittelbar oder über einen vom König bestimmten Polizeidienst die Mitwirkung folgender Personen anfordern:

- des Betreibers eines elektronischen Kommunikationsnetzes und

- jeglicher Person, die auf belgischem Staatsgebiet auf irgendeine Weise einen Dienst bereitstellt oder anbietet, der in der Übertragung von Signalen über elektronische Kommunikationsnetze besteht oder durch den Nutzer dazu ermächtigt werden, über ein elektronisches Kommunikationsnetz Informationen zu erhalten, zu empfangen oder zu verbreiten. Hierzu zählt auch der Anbieter eines elektronischen Kommunikationsdienstes.

In den in Absatz 1 erwähnten Fällen werden für jedes elektronische Kommunikationsmittel, für das die Verkehrsdaten erfasst werden oder die Herkunft oder Bestimmung der elektronischen Nachricht lokalisiert wird, Tag, Uhrzeit, Dauer und, wenn nötig, Ort der elektronischen Nachricht in einem Protokoll angegeben und festgehalten.

Der Untersuchungsrichter gibt die tatsächlichen Umstände der Sache, die die Maßnahme rechtfertigen, deren Verhältnismäßigkeit unter Berücksichtigung des Privatlebens und deren Subsidiarität gegenüber jeder anderen Ermittlungsaufgabe in einem mit Gründen versehenen Beschluss an.

Er gibt auch die Dauer der Maßnahme für die Zukunft an, die nicht länger als zwei Monate ab dem Beschluss betragen darf, unbeschadet einer Erneuerung, und gegebenenfalls den Zeitraum in der Vergangenheit, über den der Beschluss sich gemäß § 2 erstreckt.

Bei Entdeckung auf frischer Tat kann der Prokurator des Königs die Maßnahme für die in Artikel 90*ter* §§ 2, 3 und 4 erwähnten Straftaten anordnen. In diesem Fall muss die Maßnahme binnen vierundzwanzig Stunden vom Untersuchungsrichter bestätigt werden.

Wenn es jedoch die in Artikel 137, 347*bis*, 434 oder 470 des Strafgesetzbuches erwähnte Straftat betrifft, mit Ausnahme der in Artikel 137 § 3 Nr. 6 desselben Gesetzbuches erwähnten Straftat, kann der Prokurator des Königs die Maßnahme anordnen, solange die Situation der Entdeckung auf frischer Tat andauert, ohne dass eine Bestätigung durch den Untersuchungsrichter nötig ist.

Wenn es die in Artikel 137 des Strafgesetzbuches erwähnte Straftat betrifft, mit Ausnahme der in Artikel 137 § 3 Nr. 6 desselben Gesetzbuches erwähnten Straftat, kann der Prokurator des Königs die Maßnahme außerdem binnen zweiundsiebzig Stunden nach Entdeckung dieser Straftat anordnen, ohne dass eine Bestätigung durch den Untersuchungsrichter nötig ist.

Der Prokurator des Königs kann die Maßnahme jedoch auf Ersuchen des Klägers hin anordnen, wenn diese Maßnahme sich als unbedingt notwendig erweist, um eine in Artikel 145 § 3 und § 3*bis* des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation erwähnte Straftat festzustellen.

Im Dringlichkeitsfall kann die Maßnahme mündlich angeordnet werden. Sie muss so schnell wie möglich in der in den Absätzen 4 und 5 vorgesehenen Form bestätigt werden.

§ 2. In Bezug auf die Anwendung der in § 1 Absatz 1 erwähnten Maßnahme auf die Verkehrs- oder Standortdaten, die aufgrund der Artikel 126/1 und 126/3 des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation gespeichert werden, gelten folgende Bestimmungen:

- Für eine in Buch 2 Titel 1*ter* des Strafgesetzbuches erwähnte Straftat kann der Untersuchungsrichter in seinem Beschluss die Daten für einen Zeitraum von zwölf Monaten vor dem Beschluss anfordern.

- Für eine andere in Artikel 90*ter* §§ 2 bis 4 erwähnte Straftat, die nicht im ersten Gedankenstrich erwähnt ist, oder für eine Straftat, die im Rahmen einer in Artikel 324*bis* des Strafgesetzbuches erwähnten kriminellen Organisation begangen worden ist, oder für eine Straftat, die eine Hauptkorrektionalgefängnisstrafe von fünf Jahren oder eine schwerere Strafe zur Folge haben kann, kann der Untersuchungsrichter in seinem Beschluss die Daten für einen Zeitraum von neun Monaten vor dem Beschluss anfordern.

- Für andere Straftaten kann der Untersuchungsrichter die Daten nur für einen Zeitraum von sechs Monaten vor dem Beschluss anfordern.

§ 3. Die Maßnahme darf sich nur dann auf elektronische Kommunikationsmittel eines Rechtsanwalts oder Arztes beziehen, wenn dieser selbst verdächtigt wird, eine in § 1 erwähnte Straftat begangen zu haben oder daran beteiligt gewesen zu sein, oder wenn genaue Tatsachen vermuten lassen, dass Dritte, die verdächtigt werden, eine in § 1 erwähnte Straftat begangen zu haben, seine elektronischen Kommunikationsmittel benutzen.

Die Maßnahme darf nicht durchgeführt werden, ohne dass - je nach Fall - der Präsident der Rechtsanwaltskammer oder der Vertreter der provinzialen Ärztekammer davon in Kenntnis

gesetzt worden ist. Dieselben Personen werden vom Untersuchungsrichter darüber in Kenntnis gesetzt, welche Elemente seiner Meinung nach unter das Berufsgeheimnis fallen. Diese Elemente werden nicht im Protokoll festgehalten. Diese Personen unterliegen der Schweigepflicht. Jegliche Verletzung der Schweigepflicht wird gemäß Artikel 458 des Strafgesetzbuches geahndet.

§ 4. Die in § 1 Absatz 2 erwähnten Akteure teilen die angeforderten Informationen in Echtzeit oder gegebenenfalls zu dem in der Anforderung bestimmten Zeitpunkt gemäß den vom König auf Vorschlag des Ministers der Justiz und des für das Fernmeldewesen zuständigen Ministers festgelegten Modalitäten mit.

Jede Person, die aufgrund ihres Amtes Kenntnis von der Maßnahme erlangt oder dabei ihre Mitwirkung gewährt, unterliegt der Schweigepflicht. Jegliche Verletzung der Schweigepflicht wird gemäß Artikel 458 des Strafgesetzbuches geahndet.

Wer seine technische Mitwirkung bei den im vorliegenden Artikel erwähnten Anforderungen verweigert oder nicht in Echtzeit oder gegebenenfalls zu dem in der Anforderung bestimmten Zeitpunkt gewährt, wird mit einer Geldbuße von sechsundzwanzig bis zu zehntausend EUR bestraft; die Modalitäten dieser Mitwirkung werden vom König auf Vorschlag des Ministers der Justiz und des für das Fernmeldewesen zuständigen Ministers festgelegt ».

B.119. Abgesehen von dem in Artikel 88*bis* § 3 des Strafprozessgesetzbuches erwähnten Fall sieht das Gesetz vom 20. Juli 2022 einen besonderen Schutz für die vom Berufsgeheimnis geschützten Daten nicht ausdrücklich vor.

Der Wortlaut von Artikel 88*bis* § 3 des Strafprozessgesetzbuches, ersetzt durch Artikel 27 des Gesetzes vom 20. Juli 2022, selbst sieht einen besonderen Schutz für die elektronischen Kommunikationsmittel von Rechtsanwälten oder Ärzten vor, das heißt sowohl für die Kommunikation, die von einem Rechtsanwalt oder Arzt stammt, als auch für die Kommunikation, die von Klienten und Patienten ausgeht (*Parl. Dok.*, Kammer, 2021-2022, DOC 55-2572/003, S. 48).

B.120. Das Berufsgeheimnis, an das die in Artikel 458 des Strafgesetzbuches erwähnten Personen, insbesondere Rechtsanwälte und Ärzte, gebunden sind, dient nicht dazu, ihnen irgendein Vorrecht zu gewähren, sondern bezweckt hauptsächlich, das Grundrecht auf Achtung des Privatlebens derjenigen, die sie in bisweilen sehr persönlichen Dingen ins Vertrauen ziehen, zu schützen. Zudem genießen die vertraulichen Informationen, die einem Rechtsanwalt bei der Ausübung seines Berufes und wegen dieser Eigenschaft anvertraut werden, in bestimmten Fällen auch den Schutz, der sich für den Rechtsuchenden aus den Garantien ergibt, die in Artikel 6 der Europäischen Menschenrechtskonvention festgelegt sind, da die dem

Rechtsanwalt auferlegte Regel des Berufsgeheimnisses ein fundamentales Element der Rechte der Verteidigung des Rechtsuchenden, der ihn ins Vertrauen zieht, ist.

Die Wirksamkeit der Verteidigungsrechte eines Rechtsuchenden setzt es notwendigerweise voraus, dass ein Vertrauensverhältnis zwischen ihm und dem Rechtsanwalt, der ihn berät und ihn verteidigt, entstehen kann. Dieses notwendige Vertrauensverhältnis kann nur entstehen und aufrechterhalten werden, wenn der Rechtsuchende die Garantie hat, dass das, was er seinem Rechtsanwalt anvertraut, von diesem nicht weitergegeben wird. Daraus ergibt sich, dass die Rechtsanwälten auferlegte Regel des Berufsgeheimnisses ein fundamentales Element der Rechte der Verteidigung ist.

Wie der Kassationshof bemerkt, « beruht das Berufsgeheimnis, dem die Mitglieder der Rechtsanwaltschaft unterliegen, auf der Notwendigkeit, denjenigen, die sich ihnen anvertrauen, absolute Sicherheit zu bieten » (Kass., 13. Juli 2010, ECLI:BE:CASS:2010:ARR.20100713.1; siehe auch Kass., 9. Juni 2004, ECLI:BE:CASS:2004:ARR.20040609.10).

Auch wenn es « nicht unantastbar » ist, stellt das Berufsgeheimnis des Rechtsanwalts daher « eines der Grundprinzipien, auf denen die Organisation des Gerichtswesens in einer demokratischen Gesellschaft beruht » dar (EuGHMR, 6. Dezember 2012, *Michaud gegen Frankreich*, ECLI:CE:ECHR:2012:1206JUD001232311, § 123).

B.121.1. In diesem Kontext ist das Gesetz vom 20. Juli 2022 im Einklang mit der Verfassung auszulegen, unter Berücksichtigung des Umstands, dass das Berufsgeheimnis des Rechtsanwalts einen allgemeinen Grundsatz darstellt, der mit der Beachtung der Grundrechte im Zusammenhang steht. Folglich können die Regeln, die davon abweichen, ausschließlich eng ausgelegt werden unter Berücksichtigung der Weise, wie der anwaltliche Beruf durch das innerstaatliche Recht geregelt ist.

In den Vorarbeiten zu dieser Bestimmung heißt es:

« Le point 2° de l'article 21 [devenu 27] réintègre l'ancien § 3 qui protège les données de communications des médecins et des avocats. La mesure ne peut porter sur leurs moyens de communications électronique que dans le cadre de certaines situations très spécifiques. Ce paragraphe est une reprise des articles 39*bis*, § 9, 56*bis*, 88*bis*, § 3 et 90*octies* CIC » (*Parl. Dok.*, Kammer, 2021-2022, DOC 55-2572/001, S. 145).

Zu diesem Artikel 39*bis* § 9 des Strafprozessgesetzbuches hat der Gerichtshof in seinem Entscheid Nr. 66/2021 vom 29. April 2021 (ECLI:BE:GHCC:2021:ARR.066) geurteilt:

« B.11.1. Artikel 39*bis* § 9 Absatz 2 des Strafprozessgesetzbuches sieht vor, dass die Maßnahme nicht durchgeführt werden darf, ohne dass - je nach Fall - der Präsident der Rechtsanwaltskammer oder der Vertreter des Provinzialrats der Ärztekammer davon in Kenntnis gesetzt worden ist, und dass diese Personen vom Prokurator des Königs über die Elemente informiert werden, die seiner Meinung nach unter das Berufsgeheimnis fallen.

B.11.2. In dieser Bestimmung ist nicht festgelegt, in welcher Weise die Beteiligung des Vertreters der betreffenden Kammer konkret erfolgen muss. Diesbezüglich ist Artikel 39*bis* § 9 des Strafprozessgesetzbuches in einer Weise auszulegen, dass er im Lichte seiner *ratio legis*, die der Schutz des Berufsgeheimnisses des Rechtsanwalts und des Arztes ist, eine sachdienliche Wirkung hat. Deshalb ist Artikel 39*bis* § 9 Absatz 2 des Strafprozessgesetzbuches so auszulegen, dass er den Prokurator des Königs verpflichtet, den Präsidenten der Rechtsanwaltskammer oder den Vertreter des Provinzialrats der Ärztekammer vor der Durchführung der Maßnahme in Kenntnis zu setzen, sodass dieser daran teilnehmen kann und imstande ist, vorher die Dokumente, Dateien oder Elemente, die der Prokurator des Königs einsehen möchte, zu prüfen und diesen darüber zu informieren, was seiner Meinung nach unter das Berufsgeheimnis fällt. Der Vertreter der betreffenden Kammer kann außerdem geeignete Maßnahmen empfehlen, die es ermöglichen, bestimmte dem Berufsgeheimnis unterliegende Schriftstücke einzusehen, ohne dieses Geheimnis zu gefährden.

Es obliegt dem Prokurator des Königs, darüber zu befinden, ob die Elemente, die er einsehen möchte, vertraulich sind oder nicht, nachdem er - je nach Fall - die Stellungnahme des Präsidenten der Rechtsanwaltskammer oder des Vertreters des Provinzialrats der Ärztekammer eingeholt hat. Im Fall unterschiedlicher Meinungen kann der Vertreter der betreffenden Kammer seine Vorbehalte in dem Protokoll festhalten lassen.

B.11.3. Da dieses Vorrecht des Prokurators des Königs die logische Folge seiner Befugnis ist, nicht geheime Suchen in einem Datenverarbeitungssystem anzuordnen, wie in B.9.3 dargelegt, entbehrt es nicht einer vernünftigen Rechtfertigung, dass der Prokurator des Königs selber über den vertraulichen oder nicht vertraulichen Charakter der Elemente, die er einsehen möchte, nach der Stellungnahme des Vertreters der betreffenden Kammer und unbeschadet der Kontrolle der Anklagekammer und der erkennenden Gerichte entscheidet. Der Prokurator des Königs trägt nämlich gesetzlich die Verantwortung für den ordnungsgemäßen Ablauf der Ermittlung, die darin besteht, Straftaten, deren Urheber und Beweise zu ermitteln und die der Ausübung der Strafverfolgung dienlichen Informationen zu sammeln (Artikel 28*bis* § 1 Absätze 1 und 3 des Strafprozessgesetzbuches).

B.11.4. Aufgrund von Artikel 39*bis* § 9 Absatz 2 des Strafprozessgesetzbuches werden die Elemente, die nach Meinung des Prokurators des Königs unter das Berufsgeheimnis fallen, nicht im Protokoll festgehalten und der Vertreter der betreffenden Kammer unterliegt der Schweigepflicht.

[...]

B.14. Vorbehaltlich der in B.11.2 erwähnten Auslegung sind die zwei Klagegründe nicht begründet ».

Derselbe Vorbehalt der Auslegung gilt für den angefochtenen Artikel 88*bis* § 3 des Strafprozessgesetzbuches.

B.121.2. Dieselbe Auslegung muss *mutatis mutandis* allgemein für alle Daten, die unter den Anwendungsbereich von Artikel 458 des Strafgesetzbuches fallen, und folglich für andere Kategorien von Berufsangehörigen gemäß den Modalitäten und unter den Bedingungen, die vom Gesetzgeber vorgesehen sind, angewandt werden. Somit ist nur von der Regel des Berufsgeheimnisses abzuweichen, wenn dies in jedem konkreten Einzelfall, in dem ein Untersuchungsrichter oder eine andere Behörde Zugang zu den gespeicherten Daten hat, durch einen zwingenden Grund des Allgemeininteresses zu rechtfertigen ist und wenn die Aufhebung des Geheimnisses strikt im Verhältnis zu diesem Ziel steht.

B.122. Unter Berücksichtigung der in B.121 erwähnten Auslegung verstößt das Gesetz vom 20. Juli 2022 nicht in diskriminierender Weise gegen das Berufsgeheimnis.

B.123. Der einzige Klagegrund in der Rechtssache Nr. 7907, de einzige Klagegrund in der Rechtssache Nr. 7929, der zweite und der fünfte Klagegrund in der Rechtssache Nr. 7930 sowie der siebte Teil des ersten Klagegrunds und der dritte Teil des dritten Klagegrunds in der Rechtssache Nr. 7932 sind unbegründet.

Aus diesen Gründen:

Der Gerichtshof

- stellt vor der Urteilsfällung über die Beschwerdegründe in Bezug auf die Artikel 5, 6 und 24 des Gesetzes vom 20. Juli 2022 « über die Sammlung und Speicherung von Identifizierungsdaten und Metadaten im Bereich der elektronischen Kommunikation und die Übermittlung dieser Daten an die Behörden » dem Gerichtshof der Europäischen Union folgende Vorabentscheidungsfragen:

1. Ist Artikel 15 Absatz 1 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 « über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) » in Verbindung mit den Artikeln 7, 8 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union dahin auszulegen,

a) dass er nationalen Rechtsvorschriften entgegensteht, die eine Verpflichtung für Betreiber von elektronischen Kommunikationsdiensten vorsehen, die in diesen Rechtsvorschriften erwähnten Verkehrsdaten im Rahmen der Bereitstellung dieses Netzes oder dieses Dienstes je nach Fall für vier oder zwölf Monate auf Vorrat zu speichern und zu verarbeiten, damit sie angemessene und verhältnismäßige Vorsorge- und Abhilfemaßnahmen treffen, mit denen Betrug und böswillige Nutzungen in ihren Netzen vermieden und es verhindert werden kann, dass Endnutzern ein Schaden entsteht oder sie belästigt werden, sowie mit denen Betrugsfälle oder böswillige Nutzungen des Netzes oder des Dienstes festgestellt oder deren Urheber und Ursprung identifiziert werden können;

b) dass er nationalen Rechtsvorschriften entgegensteht, die es diesen Betreibern erlauben, die betreffenden Verkehrsdaten im Fall eines identifizierten spezifischen Betrugsfalls oder einer identifizierten spezifischen böswilligen Nutzung des Netzes über die vorerwähnten Fristen hinaus die für deren Analyse und Lösung notwendige Zeit oder die für die Bearbeitung dieser böswilligen Nutzung notwendige Zeit auf Vorrat zu speichern und zu verarbeiten;

c) dass er nationalen Rechtsvorschriften entgegensteht, die es diesen Betreibern erlauben, ohne eine Verpflichtung vorzusehen, eine vorherige Stellungnahme anzufordern oder eine

Notifizierung an eine unabhängige Behörde vorzunehmen, andere als die in dem Gesetz erwähnten Daten auf Vorrat zu speichern und zu verarbeiten, um einen Betrug oder eine böswillige Nutzung des Netzes oder des Dienstes feststellen oder deren Urheber und Ursprung identifizieren zu können;

d) dass er nationalen Rechtsvorschriften entgegensteht, die es diesen Betreibern erlauben, ohne eine Verpflichtung vorzusehen, eine vorherige Stellungnahme anzufordern oder eine Notifizierung an eine unabhängige Behörde vorzunehmen, die Verkehrsdaten, die sie für notwendig halten, um die Sicherheit und das ordnungsgemäße Funktionieren ihrer Netze und elektronischen Kommunikationsdienste sicherzustellen und insbesondere um eine potenzielle oder tatsächliche Beeinträchtigung dieser Sicherheit zu erkennen und zu analysieren und auch den Ursprung dieser Beeinträchtigung zu identifizieren, für eine Dauer von zwölf Monaten und im Fall einer spezifischen Beeinträchtigung der Sicherheit des Netzes für die für deren Bearbeitung notwendige Dauer auf Vorrat zu speichern und zu verarbeiten?

2. Ist Artikel 15 Absatz 1 der Richtlinie 2002/58/EG in Verbindung mit den Artikeln 7, 8 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union dahin auszulegen,

a) dass er nationalen Rechtsvorschriften entgegensteht, die es Mobilfunknetzbetreibern erlauben, Standortdaten im Rahmen der Bereitstellung dieses Netzes oder dieses Dienstes für einen Zeitraum von je nach Fall vier oder zwölf Monaten auf Vorrat zu speichern und zu verarbeiten, ohne dass in den Rechtsvorschriften präzise beschrieben wird, um welche Daten es geht, wenn dies für das ordnungsgemäße Funktionieren und die Sicherheit des Netzes oder des Dienstes oder dafür notwendig ist, um Betrugsfälle oder eine böswillige Nutzung des Netzes zu erkennen oder zu analysieren;

b) dass er nationalen Rechtsvorschriften entgegensteht, die es diesen Betreibern erlauben, die Standortdaten im Fall einer spezifischen Beeinträchtigung, eines spezifischen Betrugs oder einer spezifischen böswilligen Nutzung über die vorerwähnten Fristen hinaus auf Vorrat zu speichern und zu verarbeiten?

3. Falls der Verfassungsgerichtshof auf der Grundlage der Antworten auf die erste oder zweite Vorabentscheidungsfrage zu dem Schluss gelangen sollte, dass bestimmte Bestimmungen des Gesetzes vom 20. Juli 2022 « über die Sammlung und Vorratsspeicherung

von Identifizierungsdaten und Metadaten im Bereich der elektronischen Kommunikation und über die Übermittlung dieser Daten an die Behörden » gegen eine oder mehrere der Verpflichtungen verstoßen, die sich aus den in diesen Fragen genannten Bestimmungen ergeben, könnte er die Folgen der vorerwähnten Bestimmungen des Gesetzes vom 20. Juli 2022 vorläufig aufrechterhalten, um eine Rechtsunsicherheit zu vermeiden und zu ermöglichen, dass die zuvor gesammelten und auf Vorrat gespeicherten Daten noch für die durch das Gesetz angestrebten Ziele benutzt werden können?

- weist die anderen Beschwerdegründe vorbehaltlich der in B.121 erwähnten Auslegung zurück.

Erlassen in französischer, niederländischer und deutscher Sprache, gemäß Artikel 65 des Sondergesetzes vom 6. Januar 1989 über den Verfassungsgerichtshof, am 26. September 2024.

Der Kanzler, Der Präsident,

Nicolas Dupont Pierre Nihoul