Grondwettelijk Hof

Arrest nr. 97/2024
van 26 september 2024
Rolnummers : 7907, 7929, 7930, 7931 en 7932

In zake : de beroepen tot gehele of gedeeltelijke vernietiging van de wet van 20 juli 2022 « betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten », ingesteld door de « Ordre des barreaux francophones et germanophone », door de vzw « Académie Fiscale » en Jean Pierre Riquet, door de vzw « Liga voor Mensenrechten », door de vzw « Ligue des droits humains » en door Jens Hermans en anderen.

Het Grondwettelijk Hof,

samengesteld uit de voorzitters Pierre Nihoul en Luc Lavrysen, en de rechters Thierry Giet, Joséphine Moerman, Michel Pâques, Yasmine Kherbache, Danny Pieters, Sabine de Bethune, Emmanuelle Bribosia, Willem Verrijdt, Kattrin Jadin en Magali Plovie, bijgestaan door griffier Nicolas Dupont, onder voorzitterschap van voorzitter Pierre Nihoul,

wijst na beraad het volgende arrest :

I. *Onderwerp van de beroepen en rechtspleging*

a. Bij verzoekschrift dat aan het Hof is toegezonden bij op 2 januari 2023 ter post aangetekende brief en ter griffie is ingekomen op 4 januari 2023, heeft de « Ordre des barreaux francophones et germanophone », bijgestaan en vertegenwoordigd door Mr. Alexandre Cassart, advocaat bij de balie te Charleroi, en door Mr. Jean-François Henrotte, Mr. Elisabeth Kiehl en Mr. Eric Lemmens, advocaten bij de balie Luik-Hoei, beroep tot vernietiging ingesteld van de wet van 20 juli 2022 « betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten » (bekendgemaakt in het *Belgisch Staatsblad* van 8 augustus 2022).

b. Bij verzoekschriften die aan het Hof zijn toegezonden bij op 3, 6 en 8 februari 2023 ter post aangetekende brieven en ter griffie zijn ingekomen op 6, 7, 8 en 9 februari 2023, zijn beroepen tot gehele of gedeeltelijke (artikelen 2 tot 17) vernietiging ingesteld van dezelfde wet door de vzw « Académie Fiscale » en Jean Pierre Riquet, door de vzw « Liga voor Mensenrechten », bijgestaan en vertegenwoordigd door Mr. Raf Jespers, advocaat bij de balie van Antwerpen, door de vzw « Ligue des droits humains », bijgestaan en vertegenwoordigd

door Mr. Catherine Forget, advocate bij de balie te Brussel, en door Jens Hermans, de private stichting « Ministry of Privacy » en Matthias Dobbelaere-Welvaert, bijgestaan en vertegenwoordigd door Mr. Jan De Groote, advocaat bij de balie te Dendermonde.

Die zaken, ingeschreven onder de nummers 7907, 7929, 7930, 7931 en 7932 van de rol van het Hof, werden samengevoegd.

De Ministerraad, bijgestaan en vertegenwoordigd door Mr. Evrard de Lophem, Mr. Sébastien Depré en Mr. Germain Haumont, advocaten bij de balie te Brussel, heeft memories ingediend (in alle zaken), de verzoekende partijen in de zaken nrs. 7907, 7930 en 7931 hebben memories van antwoord ingediend en de Ministerraad heeft ook memories van wederantwoord ingediend (in de zaken nrs. 7907, 7930 en 7931).

Bij beschikking van 28 februari 2024 heeft het Hof, na de rechters-verslaggevers Thierry Giet en Sabine de Bethune te hebben gehoord, beslist dat de zaken in staat van wijzen waren, dat geen terechtzitting zou worden gehouden, tenzij een partij binnen zeven dagen na ontvangst van de kennisgeving van die beschikking een verzoek om te worden gehoord, zou hebben ingediend, en dat, behoudens zulk een verzoek, de debatten na die termijn zouden worden gesloten en de zaken in beraad zouden worden genomen.

Ingevolge het verzoek van de verzoekende partij in de zaak nr. 7907 om te worden gehoord, heeft het Hof bij beschikking van 13 maart 2024 :

- de dag van de terechtzitting bepaald op 10 april 2024;

- de partijen uitgenodigd om, in een uiterlijk op 5 april 2024 in te dienen aanvullende memorie, waarvan zij binnen dezelfde termijn een afschrift uitwisselen, hun opmerkingen te kennen te geven over de weerslag van het arrest van het Europees Hof voor de Rechten van de Mens *Podchasov t. Rusland* van 13 februari 2024, op de behandeling van onderhavige beroepen.

Aanvullende memories zijn ingediend door :

- de verzoekende partij in de zaak nr. 7907;

- de verzoekende partij in de zaak nr. 7930;

- de verzoekende partijen in de zaak nr. 7932;

- de Ministerraad.

Op de openbare terechtzitting van 10 april 2024 :

- zijn verschenen :

. Mr. Jean-François Henrotte en Mr. Elisabeth Kiehl, tevens *loco* Mr. Eric Lemmens, voor de verzoekende partij in de zaak nr. 7907;

. Jean Pierre Riquet, in eigen persoon en voor de vzw « Académie Fiscale » (verzoekende partijen in de zaak nr. 7929);

. Mr. Raf Jespers, voor de verzoekende partij in de zaak nr. 7930;

. Mr. Catherine Forget, voor de verzoekende partij in de zaak nr. 7931;

. Mr. Jan De Groote, voor de verzoekende partijen in de zaak nr. 7932;

. Mr. Evrard de Lophem, tevens *loco* Mr. Sébastien Depré, en Mr. Germain Haumont, voor de Ministerraad;

- hebben de rechters-verslaggevers Thierry Giet en Sabine de Bethune verslag uitgebracht;

- zijn de voornoemde partijen gehoord;

- zijn de zaken in beraad genomen.

Bij beschikking van 15 mei 2024 heeft het Hof, na de rechters-verslaggevers Thierry Giet en Sabine de Bethune te hebben behoord, beslist :

- de debatten te heropenen;

- de partijen uit te nodigen om, in een uiterlijk op 30 mei 2024 in te dienen aanvullende memorie, hun opmerkingen te kennen te geven over de weerslag van de arresten van het Hof van Justitie van de Europese Unie *La Quadrature du Net e.a. (Données personnelles et lutte contre la contrefaçon)* (C-470/21) en *Procura della Repubblica presso il Tribunale di Bolzano* (C-178/22) van 30 april 2024 op de behandeling van onderhavige beroepen en binnen dezelfde termijn mee te delen aan de andere partijen, alsook aan de griffie van het Hof via mail op het adres « griffie@const-court.be »;

- de dag van een nieuwe terechtzitting vast te stellen op 5 juni 2024.

Aanvullende memories zijn ingediend door :

- de verzoekende partij in de zaak nr. 7907;

- de Ministerraad.

Op de openbare terechtzitting van 5 juni 2024 :

- zijn verschenen :

. Mr. Alexandre Cassart, tevens *loco* Mr. Jean-François Henrotte, en Mr. Elisabeth Kiehl, tevens *loco* Mr. Eric Lemmens, voor de verzoekende partij in de zaak nr. 7907;

. Mr. Raf Jespers, tevens *loco* Mr. Catherine Forget, voor de verzoekende partijen in de zaken nrs. 7930 en 7931;

. Mr. Jan De Groote, voor de verzoekende partijen in de zaak nr. 7932;

. Mr. Evrard de Lophem, tevens *loco* Mr. Sébastien Depré, voor de Ministerraad;

- hebben de rechters-verslaggevers Thierry Giet en Sabine de Bethune verslag uitgebracht;

- zijn de voornoemde advocaten gehoord;

- zijn de zaken in beraad genomen.

De bepalingen van de bijzondere wet van 6 januari 1989 op het Grondwettelijk Hof met betrekking tot de rechtspleging en het gebruik van de talen werden toegepast.

II. *In rechte*

- A -

Ten aanzien van de ontvankelijkheid

Wat betreft het standpunt van de verzoekende partijen

Zaak nr. 7907

A.1.1. De verzoekende partij, die de « Ordre des barreaux francophones et germanophone » is, voert aan dat zij over het belang beschikt om de vernietiging van de artikelen 5, 4° en 6°, 8 tot 11, 13 tot 15, 19, 21, 22, 24 tot 42 en 44 van de wet van 20 juli 2022 « betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten » (hierna : de wet van 20 juli 2022) te vorderen, ten aanzien van de opdrachten die zij waarneemt krachtens artikel 495 van het Gerechtelijk Wetboek. De bestreden bepalingen doen immers afbreuk aan het beroepsgeheim van de advocaat in zoverre zij het met name mogelijk maken te bepalen of een cliënt een advocaat heeft geraadpleegd en de datum en het tijdstip van die communicatie te bepalen, maar ook de advocaat en zijn cliënten te identificeren. Die informatie is evenwel vertrouwelijk en wordt gedekt door het beroepsgeheim. De verzoekende partij voegt eraan toe dat het Hof, bij het arrest nr. 126/2005 van 13 juli 2005 (ECLI:BE:GHCC:2005:ARR.126), haar belang heeft erkend om in rechte te treden teneinde de vernietiging te vorderen van bepalingen met betrekking tot het beroep van advocaat en, bij het arrest nr. 84/2015 van 11 juni 2015 (ECLI:BE:GHCC:2015:ARR.084), haar belang heeft bevestigd om in rechte te treden met betrekking tot bepalingen met een soortgelijke draagwijdte als die van de bestreden bepalingen.

A.1.2. De verzoekende partij voegt eraan toe dat de bestreden bepalingen een ondeelbaar geheel vormen ten aanzien van de grieven die zij opwerpt, zodat, in tegenstelling tot hetgeen de Ministerraad aanvoert, het belang om in rechte te treden zich niet beperkt tot artikel 27, 2°, van de wet van 20 juli 2022, dat enkel betrekking heeft op de toegang tot beschermde gegevens en niet op de bewaring ervan, die wordt geregeld bij andere bepalingen. Bovendien is het voormelde artikel 27, 2°, niet van toepassing op de communicatie die afkomstig is van de cliënt, noch op de door die cliënt bijgehouden gegevens, terwijl die informatie, in voorkomend geval, wordt gedekt door het beroepsgeheim. De andere bepalingen van de wet van 20 juli 2022 zijn dus noodzakelijkerwijs van toepassing op en doen afbreuk aan het beroepsgeheim, aangezien in die wet geen onderscheid wordt gemaakt op grond van de gegevens die al dan niet worden gedekt door dat beroepsgeheim. Bijgevolg meent de verzoekende partij te beschikken over een belang met betrekking tot het derde en het vierde onderdeel van het enige middel, in tegenstelling tot hetgeen de Ministerraad aanvoert. Het Hof heeft overigens, bij zijn arresten nrs. 57/2021 van 22 april 2021 (ECLI:BE:GHCC:2021:ARR.057) en 96/2018 van 19 juli 2018 (ECLI:BE:GHCC:2018:ARR.096), het belang erkend van de « Ordre des barreaux francophones et germanophone » in het kader van beroepen tot vernietiging die waren gericht tegen wetten met een zeer soortgelijke draagwijdte als die van de wet van 20 juli 2022. Te dezen dient niet te worden afgezien van die rechtspraak.

Zaak nr. 7929

A.2. De eerste verzoekende partij, de vzw « Académie Fiscale », meent te beschikken over een belang om de vernietiging van de artikelen 2 tot 17 van de wet van 20 juli 2022 te vorderen, ten aanzien van haar statutair doel, aangezien die bepalingen de situatie van de boekhouders-fiscalisten, de accountants en de belastingadviseurs alsook die van de belastingplichten die door de voornoemde personen worden verdedigd, rechtstreeks en ongunstig kunnen raken. De wet van 20 juli 2022 doet immers afbreuk aan het beroepsgeheim van de boekhoudkundige en fiscale professionals in zoverre het raadplegen van de bewaarde metagegevens het mogelijk maakt om te bepalen of een boekhoudkundige en fiscale professional werd geraadpleegd, maar ook om die professional en zijn cliënten te identificeren en de datum en het tijdstip van hun communicatie te bepalen. Het beroepsgeheim vormt evenwel een algemeen beginsel dat bijdraagt tot de inachtneming van de grondrechten.

Bovendien is de tweede verzoekende partij, die een natuurlijke persoon is, een beroepsbeoefenaar die werkt op het gebied van de fiscaliteit en onderworpen is aan het beroepsgeheim krachtens haar inschrijving in het openbaar register van de gecertificeerde belastingadviseurs van het Instituut van de Belastingadviseurs en de Accountants. In dat opzicht wordt zij rechtstreeks geraakt door de bestreden bepalingen die voorzien in maatregelen tot bewaring van gegevens die aan het beroepsgeheim zijn onderworpen. De verzoekende partij stelt zich eveneens voor als burger en als belastingplichtige, zodat zij, in dat opzicht, meent dat zij rechtstreeks wordt geraakt door de voormelde bewaringsmaatregelen in het kader van haar eventuele private relatie met haar advocaat.

Zaak nr. 7930

A.3. De verzoekende partij, de « Liga voor Mensenrechten », voert aan dat zij over een belang beschikt om de vernietiging van de gehele wet van 20 juli 2022 te vorderen, ten aanzien van haar statutair doel, dat erin bestaat elke onrechtvaardigheid en elke aanslag op de rechten van personen of gemeenschappen te bestrijden, alsook de beginselen van gelijkheid, vrijheid en humanisme te verdedigen waarop de democratische samenlevingen berusten, en zulks met name via rechtsvorderingen. In dat verband beweert zij dat de wet van 20 juli 2022 diverse grondrechten aantast in zoverre zij wijzigingen aanbrengt in de wet van 13 juni 2005 « betreffende de elektronische communicatie » (hierna : de wet van 13 juni 2005). Zij merkt bovendien op dat het Hof haar belang om in rechte te treden reeds herhaalde malen heeft erkend.

Zaak nr. 7931

A.4. De verzoekende partij, de « Ligue des droits humains », meent te beschikken over een belang om de vernietiging van de wet van 20 juli 2022 te vorderen, ten aanzien van haar statutair doel, dat erin bestaat onrechtvaardigheid en elke willekeurige aantasting van de rechten van een individu te bestrijden, alsook elk initiatief te steunen dat strekt tot de totstandkoming en de bevordering van de rechten en vrijheden, aangezien die wet bepaalde grondrechten in het gedrang lijkt te brengen. Zij merkt bovendien op dat het Hof haar belang om in rechte te treden herhaalde malen heeft erkend, met name op het gebied van de bewaring van gegevens uit elektronische communicatie. Daarenboven voert zij aan dat zij ernaar streeft te vermijden dat terrorismebestrijding een excuus wordt om een aantal fundamentele waarden van de rechtsstaat, zoals het beginsel van de wettigheid van de misdrijven en van de straffen, te herzien.

Zaak nr. 7932

A.5.1. De verzoekende partijen voeren aan dat de wet van 20 juli 2022 een algemene draagwijdte heeft in zoverre de bewaring van de erin beoogde gegevens betrekking heeft op elke gebruiker van een elektronische-communicatiedienst. Bovendien is het gebruik van elektronische-communicatiemiddelen onontbeerlijk in de samenleving, zodat elke mogelijke gebruiker van dergelijke middelen over een belang beschikt om die wet te bestrijden. Het Hof heeft immers reeds geoordeeld dat het, in het geval van een norm die een essentieel aspect van de vrijheid van de burger raakt, niet noodzakelijk is te onderzoeken of de persoonlijke situatie van de verzoekers wordt geraakt, aangezien het belang hoe dan ook vaststaat.

A.5.2. De eerste en de derde verzoekende partij stellen zich meer bepaald voor als eindgebruikers van elektronische-communicatiediensten waarop de in de wet van 20 juli 2022 bedoelde maatregelen rechtstreeks

betrekking hebben. Die doen echter afbreuk aan hun privéleven wegens het risico van een ongeoorloofde toegang tot de bewaarde elektronische-communicatiegegevens en het risico van een oneigenlijk gebruik van die gegevens. Bijgevolg hebben de voornoemde verzoekende partijen een belang bij het vorderen van de vernietiging van de wet van 20 juli 2022 om een einde te maken aan de krachtens die wet bedoelde bewaring van hun persoonsgegevens.

A.5.3. De tweede verzoekende partij is een rechtspersoon wiens statutair doel erin bestaat te streven naar het vrijwaren van het privéleven van elke burger en met name tegen te gaan dat een maatschappij wordt opgebouwd waarin de overheid toezicht houdt. In dat kader is zij gemachtigd om elke maatregel te nemen teneinde de in de Grondwet en in het Europees Verdrag voor de rechten van de mens vastgelegde fundamentele rechten en vrijheden te verdedigen. De wet van 20 juli 2022 strekt evenwel ertoe de overheid toe te staan om zich te mengen in het privéleven van de burgers, hetgeen het door artikel 22 van de Grondwet en door artikel 8 van het Europees Verdrag voor de rechten van de mens gewaarborgde recht hoe dan ook aantast. Het belang van de tweede verzoekende partij is dan ook in overeenstemming met de rechtspraak van het Hof en leunt niet aan bij een *actio popularis*.

Wat betreft het standpunt van de Ministerraad

A.6. De Ministerraad voert aan dat het beroep in de zaak nr. 7907 enkel ontvankelijk is ten aanzien van artikel 27, 2°, van de wet van 20 juli 2022. Onder voorbehoud van een aantal uitzonderingen waarop het beroep geen betrekking heeft, wordt bij die bepaling de toegang tot alle metagegevens met betrekking tot de communicatiemiddelen van een advocaat, voor zowel inkomende als uitgaande communicatie, uitgesloten van het toepassingsgebied van de wet van 20 juli 2022. Daarentegen hebben het derde en het vierde onderdeel van het enige middel betrekking op de wet van 20 juli 2022 in haar geheel, zonder enig verband met het beroepsgeheim van de advocaten aan te tonen. Volgens de rechtspraak van het Hof beperkt het belang van de « Ordre des barreaux francophones et germanophone » zich echter tot de bepalingen die een weerslag hebben op het recht op toegang tot een rechter, op de rechtsbedeling en op de bijstand die de advocaten kunnen bieden aan hun cliënten. Enkel de kritiek die die partij met betrekking tot de bescherming van het beroepsgeheim van de advocaat formuleert, is dus ontvankelijk.

Ten gronde

Wat betreft het standpunt van de verzoekende partijen

Zaak nr. 7907

A.7. De verzoekende partij leidt een enig middel af uit de schending van de artikelen 10 en 11 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 6 en 8 van het Europees Verdrag voor de rechten van de mens en met de artikelen 7, 8 en 47 van het Handvest van de grondrechten van de Europese Unie (hierna : het Handvest). Zij voert aan dat de in het middel aangehaalde bepalingen de bescherming van het beroepsgeheim van de advocaat verzekeren, aangezien dat onder het recht op een eerlijk proces valt en een essentieel bestanddeel van het recht op eerbiediging van het privéleven uitmaakt. Zij voegt eraan toe dat, hoewel het beroepsgeheim van de advocaat niet onaantastbaar is, het een van de grondbeginselen vormt waarop de organisatie van het gerecht in een democratische samenleving berust. Dat geheim heeft met name betrekking op het bestaan zelf van de raadpleging van een advocaat. In dat kader zijn de data en tijdstippen waarop de advocaat werd geraadpleegd, gegevens met een vertrouwelijk karakter. Hetzelfde geldt voor de professionele agenda van de advocaat en voor de identiteit van de cliënten.

A.8.1. In het eerste onderdeel van het enige middel voert de verzoekende partij aan dat de bestreden bepalingen geen - of minstens onvoldoende - onderscheid maken tussen de gebruikers die houder zijn van het beroepsgeheim en de andere gebruikers. Bij die bepalingen worden alle gebruikers die elektronische communicatie verzenden immers op dezelfde wijze behandeld, zonder die gebruikers te onderscheiden wier communicatie wordt beschermd door het beroepsgeheim, zoals de cliënten van advocaten. Zij houden dus geen rekening met het bijzondere statuut van de communicatie van de advocaat, met het fundamentele karakter van het beroepsgeheim waaraan de advocaat is onderworpen en met de noodzakelijke vertrouwensrelatie die hem aan zijn cliënten bindt.

De verzoekende partij stelt vast dat het Hof, bij zijn arrest nr. 84/2015, heeft geoordeeld dat artikel 5 van de wet van 30 juli 2013 « houdende wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90*decies* van het Wetboek van strafvordering » onevenredig was ten aanzien van de artikelen 7, 8 en 52, lid 1, van het Handvest in zoverre die wet zonder enige uitzondering van

toepassing was, met name op personen van wie de communicatie onder het beroepsgeheim valt. Bovendien heeft het Hof, bij het arrest nr. 57/2021, artikel 9 van de wet van 29 mei 2016 « betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie » vernietigd, in zoverre die bepaling de communicatie die onder het beroepsgeheim valt en de andere communicatie op dezelfde wijze behandelde.

Volgens de verzoekende partij maakt de wet van 20 juli 2022 het niet mogelijk om de in de voormelde arresten vastgestelde ongrondwettigheid weg te nemen. De wetgever beoogt immers enkel de communicatie die uitgaat van de advocaat en niet die welke afkomstig is van de cliënt, terwijl het communicatie betreft die meer afbreuk doet aan het beroepsgeheim, aangezien zij de overheid te kennen geeft dat de cliënt de advocaat heeft gecontacteerd en zij de locatie en het ogenblik van dat contact aangeeft. De wetgever maakt het dus mogelijk om *in concreto* te bepalen of een advocaat werd geraadpleegd, om die advocaat en zijn gesprekspartner te identificeren, maar ook om de datum en het tijdstip van de communicatie te bepalen. Dat systeem houdt een grote aantasting in van het noodzakelijke vertrouwen van de cliënt jegens zijn advocaat en kan een persoon ervan afbrengen om een beroep op hem te doen via elektronische communicatiemiddelen. De wetgever heeft dus afbreuk gedaan aan het beroepsgeheim en aan de grondrechten die worden gewaarborgd door de in het middel bedoelde bepalingen, en zulks door geen nuttig onderscheid te maken tussen, enerzijds, de personen wier communicatie onder het beroepsgeheim valt en, anderzijds, de andere personen.

A.8.2. In het tweede onderdeel van het enige middel beweert de verzoekende partij dat de wet van 20 juli 2022 de door het beroepsgeheim gedekte gegevens niet - of onvoldoende - onderscheidt van de andere gegevens, terwijl de eerste categorie van gegevens het voorwerp moet uitmaken van een specifiekere behandeling dan de tweede.

A.8.3. In tegenstelling tot hetgeen de Ministerraad aanvoert met betrekking tot het eerste en het tweede onderdeel van het enige middel, beweert de verzoekende partij dat de versterking van de regels met betrekking tot de toegang tot de bewaarde gegevens niet volstaat om de veralgemeende bewaring van die gegevens te verantwoorden. Te dezen leidt het gebrek aan beperkingen en controle inzake de bewaring van de gegevens, in het bijzonder vanuit de invalshoek van de noodzaak om het beroepsgeheim te vrijwaren, ertoe het middel gegrond te achten. Het beroepsgeheim van de advocaat heeft immers niet alleen betrekking op de inhoud van de uitwisselingen maar ook op het bestaan zelf ervan. Bijgevolg schendt het loutere feit dat de metagegevens van de communicatie van de advocaten worden bewaard, de rechten van de verdediging indien de inmenging die de bewaring inhoudt, niet aanvaardbaar is ten aanzien van de grondrechten, hetgeen te dezen net het geval is.

Bovendien is de verzoenende interpretatie van artikel 27, 2°, van de wet van 20 juli 2022, die door de Ministerraad wordt voorgesteld en volgens welke die bepaling ook de communicatie dekt die afkomstig is van de cliënt, niet toelaatbaar aangezien in de bewoordingen van de tekst wordt verwezen naar het elektronische communicatiemiddel van een advocaat. Bovendien, in het geval van de voormelde verzoenende interpretatie, worden de door een derde bijgehouden gegevens bewaard en blijven zij toegankelijk zonder dat er rekening wordt gehouden met de vertrouwelijkheid ervan, hetgeen niet aanvaardbaar is ten aanzien van de grote hoeveelheid en de uitermate ruime aard van de gegevens die worden verzameld en bewaard door derde operatoren.

A.8.4. Wat de ontstentenis van evenredigheid van de maatregel betreft, voegt de verzoekende partij eraan toe dat het door de Ministerraad ter sprake gebrachte feit dat de advocaat niet actief meewerkt, het discriminerende karakter van de wet van 20 juli 2022 en de grote aantasting van het beroepsgeheim lijkt te bevestigen, aangezien een actieve medewerking de advocaat net in staat stelt om te helpen bij het verwezenlijken van de maatregel en om zijn opmerkingen te doen gelden, hetgeen te dezen niet mogelijk is.

De verzoekende partij voegt eraan toe dat het sorteren *a posteriori*, waarop ook de aandacht is gevestigd door de Ministerraad, geen bevredigend antwoord biedt wegens gebrek aan een specifieke procedure of een op straffe van nietigheid voorgeschreven norm, aangezien het Hof van Cassatie erkent dat elk - zelfs illegaal verkregen - bewijs toelaatbaar is in strafzaken en in burgerlijke zaken, behalve in het geval van de schending van een op straffe van nietigheid voorgeschreven regel, van een gebrek dat de betrouwbaarheid van het bewijs aantast of van de schending van het recht op een eerlijk proces. In werkelijkheid zal bij gebrek aan een voorafgaand beroep en een daadwerkelijke medewerking van de advocaat geen controle plaatsvinden. In de feiten, zelfs in het geval waarin een door het beroepsgeheim gedekt bewijselement wordt geweerd, zal de overheid hoe dan ook vooraf kennis hebben genomen van dat element. Het Europees Hof voor de Rechten van de Mens heeft overigens bevestigd dat de inachtneming van het beroepsgeheim uitsluit dat de rechter bij wie een vervolging is ingesteld, zelf onderzoekt en beslist of elementen worden beschermd door dat geheim, aangezien een dergelijke methode het beroepsgeheim stelselmatig in het gedrang zou brengen en volledig zou uithollen. Bovendien bepaalt de wet van

20 juli 2022 niets met betrekking tot de teruggave of het wissen van de gegevens waartoe men zich op onregelmatige wijze toegang zou hebben verschaft, in tegenstelling tot bijvoorbeeld artikel 90*octies*, § 3, van het Wetboek van strafvordering.

A.8.5. De verzoekende partij voegt eraan toe dat een bijzondere behandeling moet worden voorbehouden aan de houders van het beroepsgeheim, maar ook aan de door dat beroepsgeheim gedekte metagegevens, in alle gevallen. Zulks geldt des te meer ten aanzien van de aard van de betrokken metagegevens. Bovendien zijn de bepalingen van het Wetboek van strafvordering die de Ministerraad vergelijkbaar acht met die van de wet van 20 juli 2022, te dezen niet pertinent, aangezien die wet niet in een actieve medewerking van de advocaat voorziet, in tegenstelling tot de voormelde bepalingen van het Wetboek van strafvordering.

A.9.1. In het derde onderdeel van het enige middel merkt de verzoekende partij op dat de wetgever een verplichting heeft ingevoerd tot registratie en bewaring van bepaalde metagegevens die door de overheid kunnen worden geraadpleegd door zich te baseren op een systeem van cijfers inzake strafbare feiten per arrondissement. Een aanzienlijk geheel van gegevens kan dus worden verzameld, hetgeen in werkelijkheid een algemene dekking van het grondgebied en dus van alle burgers uitmaakt. De desbetreffende elektronische-communicatiemiddelen zijn immers zowel de « klassieke » elektronische-communicatiediensten, zoals telefonie, als recentere diensten, zoals onlinediensten voor het sturen van berichten. Bovendien verantwoordt geen enkel element de algemene verplichting tot bewaring van de gegevens, die van toepassing is op zowel de rechtzoekenden die het voorwerp uitmaken van een onderzoek of een vervolging als de rechtzoekenden die niet het voorwerp van dergelijke maatregelen uitmaken. Daarenboven worden in de wet van 20 juli 2022 evenmin de metagegevens gepreciseerd die de doelstellingen van bescherming van de openbare veiligheid en de doelstellingen inzake het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten effectief dienen. In werkelijkheid wijzigt de wet van 20 juli 2022 het vroegere systeem, dat nochtans door het Hof werd vernietigd, niet wezenlijk. Het Hof van Justitie van de Europese Unie (hierna : het Hof van Justitie) is trouwens van oordeel dat een maatregel tot algemene en ongedifferentieerde bewaring van gegevens een zodanige inmenging in de grondrechten van de beoogde personen uitmaakt dat hij in beginsel niet toelaatbaar is.

A.9.2. In het vierde onderdeel van het enige middel is de verzoekende partij van mening dat het bij de wet van 20 juli 2022 ingevoerde systeem niet evenredig is met het door de wetgever nagestreefde doel. Het bijeenbrengen van de gegevens die worden bewaard krachtens een verplichting tot bewaring van een groot geheel van metagegevens die *de facto* het gehele grondgebied dekt, maakt het immers mogelijk om een zeer precieze « digitale kaart » van elke persoon op te maken. Dat systeem vormt een dermate ernstige inmenging in de grondrechten dat het niet evenredig is met het nagestreefde doel en dat het bovendien op vernietigende wijze afbreuk doet aan het beroepsgeheim van de advocaat. De wet van 20 juli 2022 voorziet weliswaar niet in de registratie van de inhoud van het gesprek tussen de advocaat en zijn cliënt, maar het kennisnemen van de metagegevens volstaat om de raadpleging van de advocaat als dusdanig vast te stellen en om een aantal conclusies te trekken naargelang van de omstandigheden, zoals een oproep die enkele minuten na de feiten heeft plaatsgevonden. Het beroepsgeheim van de advocaat heeft evenwel tot doel aan diegenen die dat beroep uitoefenen, de nodige waarborgen inzake geloofwaardigheid te geven opdat de personen die zich tot een advocaat wenden, de zekerheid kunnen hebben dat de aan hun raadsman toevertrouwde geheimen niet aan derden zullen worden bekendgemaakt. De bestreden maatregel is dus geenszins evenredig ten aanzien van het essentiële karakter van het voormelde beroepsgeheim, waarvan het Hof het belang in herinnering heeft gebracht bij zijn arrest nr. 127/2013 van 26 september 2013 (ECLI:BE:GHCC:2013:ARR.127). Het bestreden systeem heeft tot gevolg dat de rechtzoekenden nooit in alle vertrouwen een advocaat zullen kunnen raadplegen en de zekerheid zullen kunnen hebben dat het bestaan en de omstandigheden van die raadpleging niet worden bekendgemaakt aan de overheid. Ten slotte stelt de verzoekende partij vast dat de gelijke behandeling van de personen die houder zijn van het beroepsgeheim en de andere personen niet wordt verantwoord in de parlementaire voorbereiding van de wet van 20 juli 2022. De wetgever heeft de invoering van minder beperkende maatregelen, zoals het sorteren van de gewone metagegevens en die welke zijn verbonden aan een houder van het beroepsgeheim door middel van een filtermechanisme bij binnenkomst, hetgeen nochtans technisch haalbaar is, niet overwogen.

A.9.3. De verzoekende partij voegt, met betrekking tot het derde en het vierde onderdeel van het enige middel, eraan toe dat de rechtspraak van het Hof van Justitie de invoering van een minimale filter bij binnenkomst vereist, los van de bepalingen waarin is voorzien voor de toegang tot de gegevens. In tegenstelling tot hetgeen de Ministerraad aanvoert, brengt de bewaring van de door het beroepsgeheim gedekte gegevens een onderscheiden inmenging met zich mee, los van de beperkingen waarin met betrekking tot de toegang tot de gegevens is voorzien.

De voormelde invoering van een filter bij binnenkomst is maar één voorbeeld waarbij de aandacht wordt gevestigd op het feit dat andere oplossingen mogelijk zijn. Die werden evenwel niet overwogen terwijl de wet van

20 juli 2022 net op discriminerende wijze afbreuk doet aan de grondrechten die worden gewaarborgd door de in het middel aangehaalde bepalingen. Bovendien zijn de technische moeilijkheden die zouden voortvloeien uit de invoering van de voormelde filter, waarop de Ministerraad de nadruk heeft gelegd, niet onoverkomelijk, zodat die maatregel in de praktijk mogelijk is. Hoewel het juist is dat het het Hof niet toekomt zich uit te spreken over de opportuniteit van een wetskrachtige regeling, blijft het desalniettemin bevoegd om te beslissen of een wet ongrondwettig is bij gebrek aan een dergelijke regeling. De voorafgaande filtering blijkt evenwel de enige maatregel te zijn die kan verzekeren dat de bewaring van de metagegevens door de operatoren niet van toepassing is op de door het beroepsgeheim gedekte gegevens. Indien die filtering niet kan worden uitgevoerd, zoals de Ministerraad beweert, betekent dit dat de in de wet van 20 juli 2022 bedoelde inmenging hoe dan ook onevenredig is.

Bovendien zijn de andere door de Ministerraad aangevoerde hinderpalen met betrekking tot het filtermechanisme niet overtuigend volgens de verzoekende partij. Dat systeem zou in het bijzonder niet kunnen worden geacht een voorrecht toe te kennen aan de advocaat. Het beroepsgeheim is immers een fundamentele waarborg voor de rechtzoekende in een democratische Staat. De advocaten zijn ertoe gehouden dat geheim te eerbiedigen op straffe van strafrechtelijke en deontologische sancties. De opheffing van het geheim is trouwens enkel denkbaar krachtens de noodtoestand of een conflict met een hogere waarde. Die afwijking wordt enkel doorgevoerd in de mate die noodzakelijk is voor het verdedigen van de respectieve rechten van de partijen in het geding. Het feit dat bepaalde advocaten zelf misdrijven kunnen plegen, verandert niets aan die vaststellingen, aangezien de advocaat zich niet achter zijn beroep kan verschuilen om straffeloosheid te genieten. Bovendien verwijst het feit dat een kwaadwillig persoon de communicatiemiddelen van een advocaat zou kunnen misbruiken, hetgeen de Ministerraad eveneens opwerpt, naar een uitzonderlijk geval dat de bestreden maatregel geenszins rechtvaardigt.

Zaak nr. 7929

A.10.1. De verzoekende partijen leiden een enig middel af uit de schending van de artikelen 10 en 11 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 6 en 8 van het Europees Verdrag voor de rechten van de mens en met de artikelen 7, 8, 11 en 47 van het Handvest. Volgens hen behandelen de bestreden bepalingen de gebruikers van telecommunicatie- of elektronische-communicatiediensten die aan het beroepsgeheim zijn onderworpen, onder wie de boekhoudkundige en fiscale professionals, en de andere gebruikers van die diensten op identieke wijze, zonder rekening te houden met het bijzondere statuut van de voornoemde professionals, met het fundamentele karakter van het beroepsgeheim waaraan die zijn onderworpen, noch met de noodzakelijke vertrouwensrelatie met hun cliënten. Bovendien behandelen de bestreden bepalingen, enerzijds, de rechtzoekenden die het voorwerp uitmaken van maatregelen van onderzoek en vervolging wegens feiten die onder de omschreven doelstellingen voor de bewaring van de in het geding zijnde elektronische gegevens kunnen vallen en, anderzijds, diegenen die niet het voorwerp van dergelijke maatregelen uitmaken, eveneens op identieke wijze.

A.10.2. De verzoekende partijen merken op dat in de parlementaire voorbereiding van de wet van 20 juli 2022 wordt aangegeven dat die ertoe strekt de richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 « betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische-communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG » (hierna : de richtlijn 2006/24/EG) en artikel 15, lid 1, van de richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 « betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) » (hierna : de richtlijn 2002/58/EG) gedeeltelijk om te zetten. Volgens de verzoekende partijen zijn de in de wet van 20 juli 2022 bedoelde verplichtingen tot bewaring evenwel buitensporig ten opzichte van de door de wetgever nagestreefde doelstellingen, aangezien in geen enkele waarborg wordt voorzien wat betreft de gegevens die betrekking hebben op de accountants en de belastingadviseurs, terwijl die vertrouwelijk zijn en onder het beroepsgeheim vallen. De wet van 20 juli 2022 voldoet immers niet aan de voorwaarden die door het Hof van Justitie zijn aanvaard met betrekking tot de uitzonderingen op het verbod van de algemene bewaring van de gegevens. De verzoekende partijen merken bovendien op dat, hoewel de wet van 20 juli 2022, behoudens uitzondering, niet toestaat dat gegevens worden bewaard die de inhoud van de communicatie onthullen, daarin wel wordt aanvaard dat kennis wordt genomen van metagegevens die aan het licht kunnen brengen dat een boekhoudkundige en fiscale professional werd geraadpleegd en die het mogelijk kunnen maken om bepaalde conclusies te trekken naargelang van de omstandigheden.

Volgens de verzoekende partijen is de bestaansreden van het beroepsgeheim van boekhoudkundige professionals van algemeen belang en beoogt het aan diegenen die dat beroep uitoefenen, de nodige waarborgen inzake geloofwaardigheid te bieden opdat diegenen die zich tot hen wenden, de zekerheid hebben dat de toevertrouwde geheimen niet aan derden worden bekendgemaakt. De wet van 20 juli 2022 doet evenwel afbreuk aan die waarborg, terwijl niets het mogelijk maakt om de identieke behandeling van alle gebruikers van telecommunicatiediensten, onder wie diegenen die aan het beroepsgeheim zijn onderworpen, te verantwoorden. De verzoekende partijen merken op dat door de bevoegde autoriteiten een strafvervolging zou kunnen worden ingesteld op grond van de vertrouwelijke gegevens die krachtens de wet van 20 juli 2022 zijn verzameld, zonder dat in de diverse stadia van de procedure in een jurisdictionele controle wordt voorzien, hetgeen niet in overeenstemming is met artikel 6 van het Europees Verdrag voor de rechten van de mens, noch met artikel 47 van het Handvest. Wat de voormelde identieke behandeling van de rechtzoekenden betreft, voeren de verzoekende partijen bovendien aan dat er een niet te verwaarlozen risico bestaat dat de gegevensbanken lichtzinnig worden beheerd door de operatoren die terughoudend zijn ten opzichte van de kosten die worden veroorzaakt door de verplichtingen die voortvloeien uit de wet van 20 juli 2022.

A.10.3. De verzoekende partijen merken op dat artikel 13 van de wet van 20 juli 2022 in algemene bewoordingen is geformuleerd die het niet mogelijk maken om alle in die bepaling bedoelde autoriteiten te identificeren. Die zullen waarschijnlijk worden geïdentificeerd in een ministeriële omzendbrief. De wet van 20 juli 2022 voorziet overigens niet in een waarborg met betrekking tot de vertrouwelijke gegevens die worden gedekt door het beroepsgeheim van de accountants en fiscalisten, maar beperkt zij zich ertoe het aan de Koning over te laten om de technische en administratieve maatregelen vast te stellen die de betrokken operatoren zullen moeten nemen om de bescherming van de bewaarde gegevens te waarborgen. Bovendien is het, vanuit technisch oogpunt, mogelijk om de gewone metagegevens en die welke zijn verbonden aan een houder van het beroepsgeheim te sorteren door middel van een filtermechanisme bij binnenkomst.

Volgens de verzoekende partijen is het Hof van Justitie van oordeel dat artikel 15 van de richtlijn 2002/58/EG zich verzet tegen een nationale regeling die, ten behoeve van de bestrijding van de criminaliteit, voorziet in een algemene en ongedifferentieerde bewaring van alle verkeers- en locatiegegevens van alle abonnees en gebruikers, met betrekking tot alle elektronische-communicatiemiddelen. Bij die bepaling wordt bovendien een voorafgaande toetsing door een rechterlijke instantie of door een onafhankelijke bestuurlijke autoriteit opgelegd, alsook een bewaring van de gegevens op het grondgebied van de Unie. De verzoekende partijen stellen overigens vast dat het Hof van Justitie heeft geoordeeld dat de richtlijn 2006/24/EG onbestaanbaar was met het evenredigheidsbeginsel, zodat een nationale regeling niet dezelfde inhoud als die richtlijn kan hebben, hetgeen het discriminerende karakter van de wet van 20 juli 2022 aantoont.

A.10.4. De verzoekende partijen voegen eraan toe dat de in de wet van 20 juli 2022 bedoelde verplichting tot bewaring van de gegevens valt onder het toepassingsgebied van het recht op eerbiediging van het privéleven en van de vrijheid van meningsuiting, die worden gewaarborgd door de artikelen 7, 8 en 11 van het Handvest. In dat verband is het Hof van Justitie van oordeel dat artikel 15 van de richtlijn 2002/58/EG, gelezen in het licht van de voormelde bepalingen van het Handvest, aldus moet worden uitgelegd dat het zich verzet tegen een nationale regeling op grond waarvan een overheidsorgaan ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronische-communicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten kan opleggen. De wet van 20 juli 2022 voorziet weliswaar in een bewaring voor een duur die is beperkt tot twaalf maanden, maar niets verantwoordt te dezen dat alle personen worden beoogd zonder een onderscheid te maken wanneer de gegevens onder het beroepsgeheim vallen. De omstandigheid dat de bewaarde gegevens, in voorkomend geval, later mogelijkerwijs niet worden gebruikt, is eveneens irrelevant, aangezien de toegang tot de gegevens een onderscheiden inmenging in de grondrechten uitmaakt. Bovendien kunnen de verkeers- en locatiegegevens informatie prijsgeven over een groot aantal aspecten van het privéleven van de betrokken personen, zoals de seksuele geaardheid, de politieke opvattingen, de religieuze overtuigingen of nog de gezondheidstoestand. In hun geheel genomen geven die gegevens zeer precieze aanwijzingen over de personen wier gegevens werden bewaard en maken zij het dan ook mogelijk om het profiel van die personen te bepalen.

A.10.5. De verzoekende partijen merken op dat de bewaring van verkeers- en locatiegegevens voor politiële doeleinden op zichzelf afbreuk kan doen aan het recht dat wordt gewaarborgd door artikel 7 van het Handvest en de gebruikers kan ontmoedigen met betrekking tot het gebruik van hun elektronische-communicatiemiddelen, hetgeen een inmenging in de door artikel 11 van het Handvest gewaarborgde vrijheid van meningsuiting vormt. Die ontmoedigende effecten raken in het bijzonder de personen wier communicatie onder het beroepsgeheim valt en de klokkenluiders. Bovendien houdt de aanzienlijke hoeveelheid verkeers- en locatiegegevens, die gevoelige informatie aan het licht kunnen brengen, verzameld krachtens een algemene en ongedifferentieerde

bewaringsmaatregel, risico's van misbruik en onrechtmatige toegang in. Het Hof van Justitie legt in dat kader de verplichting op dat de bewaring van gegevens met betrekking tot elektronische communicatie de uitzondering moet zijn en niet de regel. Die bewaring moet bovendien aan duidelijke en nauwkeurige regels zijn onderworpen en daarnaast voldoen aan een minimum aan vereisten. De inmenging moet tot het strikt noodzakelijke worden beperkt en een evenredigheidsbeginsel in acht nemen. Het doel van de bestrijding van zware criminaliteit kan een algemene en ongedifferentieerde bewaring van alle verkeers- en locatiegegevens zoals bedoeld in de wet van 20 juli 2022 hoe dan ook niet verantwoorden. Hoewel die wet voorziet in het creëren van zones op grond van de criminaliteitscijfers, wordt daarin immers niet gepreciseerd hoe de strafbare feiten worden geteld. Bovendien beperkt die wet zich niet tot het beogen van precieze situaties die te maken hebben met een ernstige en daadwerkelijke bedreiging van de nationale veiligheid. Zij voorziet evenmin in een specifieke regeling voor de aan het beroepsgeheim onderworpen personen, noch voor die welke het voorwerp van een onderzoek uitmaken.

Zaak nr. 7930

A.11.1. De verzoekende partij leidt een eerste middel af uit de schending van de artikelen 11, 12, 22 en 29 van de Grondwet, en de artikelen 5, 6, 9 en 15, lid 1, van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8, 11, 47 en 52, lid 1, van het Handvest, uit de schending van de artikelen 6, 8, 10, 11 en 18 van het Europees Verdrag voor de rechten van de mens en de artikelen 13 en 54 van de richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 « betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad » (hierna : de richtlijn (EU) 2016/680). Zij voert aan dat de artikelen 5, 6, 8, 9, 10, 11, 12 en 13 van de wet van 20 juli 2022 maatregelen zijn die *de jure* en *de facto* een algemene verplichting tot bewaring van de communicatiegegevens invoeren, alsook een zeer brede toegang tot de bewaarde gegevens instellen.

Volgens de verzoekende partij zijn de voormelde bepalingen van de wet van 20 juli 2022 niet in overeenstemming met de ter zake toepasselijke rechtspraak van het Hof van Justitie. Die bepalingen beogen immers een vijftigtal verschillende soorten van gegevens die het merendeel van de verkeers- en locatiegegevens vormen. Artikel 11 van die wet bepaalt vijf geografische zones waarbinnen de gegevens onder bepaalde voorwaarden door de operatoren moeten worden bewaard, hetgeen *de facto* ertoe leidt dat het volledige Belgische grondgebied onder de bewaarplicht kan vallen, gedurende lange of onbepaalde periodes. Artikel 13 van die wet stelt tien autoriteiten vast die onder bepaalde voorwaarden toegang kunnen krijgen tot de door de operatoren bewaarde gegevens. Het gaat om een zeer groot aantal autoriteiten waarvan de meeste buiten het kader van de doelstellingen van artikel 15, lid 1, van de richtlijn 2002/58/EG vallen. Onder die autoriteiten bevinden zich autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing of de vervolging van feiten die gewone strafrechtelijke inbreuken vormen, zonder dat ze onder zware criminaliteit vallen.

A.11.2. De verzoekende partij voegt eraan toe dat de wet van 20 juli 2022 in haar geheel moet worden onderzocht, aangezien het de volledige wet is die de door de rechtspraak van het Hof van Justitie omlijnde beginselen schendt, zowel vanuit het oogpunt van de gegevensbewaring als van de toegang tot die gegevens. De algemene aard van de maatregelen druist immers in tegen het evenredigheidsbeginsel, aangezien alle verkeers- en locatiegegevens worden bewaard, zowat het volledige grondgebied onder de bewaarplicht valt en een ruime groep van autoriteiten toegang kan krijgen tot de gegevens, wat ingaat tegen de doelstellingen die met artikel 15, lid 1, van de richtlijn 2002/58/EG worden nagestreefd. In werkelijkheid voert de wet van 20 juli 2022 een algemene en ongedifferentieerde gegevensbewaring in.

Volgens de verzoekende partij worden de uitzonderlijke voorwaarden waaronder het Hof van Justitie een algemene en ongedifferentieerde gegevensbewaring toestaat, niet vervuld door de wet van 20 juli 2022. Het feit dat de gegevens in het kader van de nationale veiligheid worden bewaard op basis van het door het Coördinatieorgaan voor de dreigingsanalyse (hierna : het OCAD) vastgestelde dreigingsniveau, voorziet immers niet in een toetsing door een rechterlijke instantie of een onafhankelijke bestuurlijke instantie, en bepaalt te dezen geen termijn van strikte noodzakelijkheid. Bovendien zijn de bepalingen met betrekking tot de gegevensbewaring in het kader van zware criminaliteit gericht op strafbare feiten die niet onder dat soort criminaliteit vallen. Het begrip « zware criminaliteit » zelf wordt, wat betreft de toegang tot de gegevens door de autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing of de vervolging, te ruim bepaald ten opzichte van de definitie van zware criminaliteit voor de bewaring van de gegevens. Terwijl voor de gegevensbewaring artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering van toepassing wordt gesteld, verwijst de toegang tot de gegevens

immers naar artikel 88*bis*, § 1, van het Wetboek van strafvordering, alsook naar de inbreuken inzake marktmisbruik, die een veel lagere strafdrempel hebben dan artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering.

A.11.3. Wat betreft de evenredigheid van de gegevensbewaring voegt de verzoekende partij eraan toe dat, in tegenstelling tot wat de Ministerraad aanvoert, de bewaring van een groot aantal gegevens niet enkel wordt bepaald in artikel 8 van de wet van 20 juli 2022, maar eveneens in de artikelen 5 en 12 van die wet. Uit die bepalingen blijkt dat het mogelijk is identificatiegegevens te bewaren, zonder dat zulks noodzakelijk of strikt beperkt is. Daarnaast is artikel 8 van de wet van 20 juli 2022 niet bestaanbaar met de rechtspraak van het Hof van Justitie, in zoverre het betrekking heeft op andere gegevens dan het IP-adres en de burgerlijke gegevens van de gebruiker, zoals de afdeling wetgeving van de Raad van State heeft beklemtoond. Bovendien houden de betrokken gegevens geen verband met de doeleinden inzake de vrijwaring van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid. Daarenboven wijst de verzoekende partij erop dat het grote aantal beoogde gegevens niet kan worden verantwoord door een technische noodzaak. Zij vestigt daarnaast de aandacht erop dat de bewaring van de gegevens, enerzijds, en de toegang ertoe, anderzijds, onderscheiden inmengingen vormen, zodat een algemene gegevensbewaring niet kan worden verantwoord door waarborgen betreffende de toegang tot die gegevens. Tot slot moet de inmenging in het recht op eerbiediging van het privéleven worden onderzocht in het licht van de concrete identificatie van de betrokken personen en niet vanuit het algemene en abstracte oogpunt van de beschikbare technologieën.

A.12.1. Een tweede middel is afgeleid uit de schending van de artikelen 11, 12, 22 en 29 van de Grondwet, van artikel 15, lid 1, en van de artikelen 5, 6 en 9 van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8, 11, 47 en 52, lid 1, van het Handvest, uit de schending van de artikelen 6, 8, 10, 11 en 18 van het Europees Verdrag voor de rechten van de mens en van de artikelen 13 en 54 van de richtlijn (EU) 2016/680. De verzoekende partij betoogt dat de artikelen 5, 6, 8, 9, 10 en 12 van de wet van 20 juli 2022, die betrekking hebben op de gegevens die de operatoren verplicht moeten bewaren, wat betreft het aantal en de beoogde categorieën van gegevens, de beginselen van evenredigheid en noodzakelijkheid schenden. De verzoekende partij preciseert dat uit de voormelde bepalingen van de wet van 20 juli 2022 zeer precieze conclusies kunnen worden getrokken over het privéleven van de beoogde personen, met name hun dagelijkse gewoontes, hun woonplaats of nog hun sociale relaties, waardoor een profiel van die personen kan worden opgesteld. De wet van 20 juli 2022 brengt de bewaring van een groot aantal en diverse categorieën van gegevens teweeg, hetgeen op zich de schending van artikel 22 van de Grondwet en van de artikelen 7 en 8 van het Handvest met zich meebrengt, daar het privéleven van de burgers niet meer wordt beschermd.

De artikelen 5, 6, 8, 9, 10 en 12 van de wet van 20 juli 2022 zijn overigens op een te ruim geheel van gegevens gericht ten opzichte van de rechtspraak van het Hof van Justitie en zij voorzien in te lange bewaringstermijnen. Bovendien is geen enkel beroep vrijgesteld van de gegevensbewaring, ook niet de artsen, advocaten of journalisten. Daarnaast heeft de bewaarplicht voor de operatoren betrekking op vrijwel alle gegevens en maakt die plicht het mogelijk de betrokken communicatie nauwkeurig te identificeren. De bewaring van die gegevens heeft betrekking op nagenoeg de hele bevolking zonder dat die zich noodzakelijkerwijs in een situatie bevindt die aanleiding geeft tot strafrechtelijke vervolging. Anders gezegd, de wet van 20 juli 2022 legt zonder grondslag de algemene en, vanuit persoonlijk, temporeel en geografisch oogpunt, ongedifferentieerde bewaring van het merendeel van de verkeers- en locatiegegevens op.

In dat verband verplicht artikel 8 van de wet van 20 juli 2022 niet ertoe de grondslag van de bewaring te vermelden, in tegenstelling tot de artikelen 5 en 6 van die wet. De verzoekende partij voegt eraan toe dat de beoogde gegevens kunnen worden opgevraagd door de autoriteiten zonder dat die toegang noodzakelijkerwijs iets te maken heeft met de vermelde doelstelling. Wat betreft de gegevensbewaring in de geografische zones vermeldt artikel 9 van de wet van 20 juli 2022 als doelstellingen de vrijwaring van de nationale veiligheid, de strijd tegen zware criminaliteit, de preventie van ernstige bedreigingen van de openbare veiligheid en de bescherming van de vitale belangen van een natuurlijke persoon. Hetzelfde artikel 9 preciseert evenwel ook dat de geografische zones enkel kunnen worden opgenomen ter vrijwaring van de nationale veiligheid of bij een hoog risico van zware criminaliteit, hetgeen tegenstrijdig is. Artikel 11 voorziet dan weer in een bewaarplicht die het volledige grondgebied kan dekken.

A.12.2. De verzoekende partij herinnert eraan dat de Gegevensbeschermingsautoriteit heeft onderstreept dat de wet van 20 juli 2022 in de feiten leidt tot een algemene en ongedifferentieerde bewaarplicht voor de gegevens met het oog op de bestrijding van criminaliteit. Bovendien vroeg die Autoriteit zich af of een verplichting tot een preventieve en systematische gegevensbewaring, waarin artikel 5 van die wet voorziet, noodzakelijk is. Volgens de verzoekende partij zijn de opmerkingen van de Gegevensbeschermingsautoriteit eveneens relevant wat betreft

de verplichting om systematisch de verkeersgegevens te bewaren van alle gebruikers van elektronische-communicatiemiddelen en wat betreft de mogelijkheid om andere locatiegegevens dan verkeersgegevens te verwerken teneinde de veiligheid en de correcte werking van het netwerk of de dienst te waarborgen, of teneinde fraude of kwaadwillig gebruik van het netwerk op te sporen of te analyseren. In de artikelen 6, 8 en 9 van de wet van 20 juli 2022 wordt verduidelijkt dat zij gelden onverminderd de verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 « betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) » (hierna : de AVG) en de wet van 30 juli 2018 « betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens » (hierna : de wet van 30 juli 2018). Volgens de verzoekende partij volstaat die stelling niet om de naleving van de AVG te waarborgen.

A.12.3. Hoewel de bewaarplicht de inhoud van de communicatie uitdrukkelijk uitsluit, merkt de verzoekende partij op dat het Hof van Justitie heeft geoordeeld dat de bewaring van categorieën van zeer precieze gegevens op basis waarvan het profiel van de beoogde personen kan worden opgesteld, zoals dat het geval is voor die welke worden bedoeld in de wet van 20 juli 2022, niet toelaatbaar was. In het bijzonder wat betreft de algemene en ongedifferentieerde bewaring van de gegevens met betrekking tot de burgerlijke identiteit van de gebruikers en de IP-adressen stelt de verzoekende partij dat een dergelijke bewaring is toegestaan met het oog op de vrijwaring van de nationale veiligheid, en enkel ter bestrijding van zware criminaliteit en ter voorkoming van ernstige bedreigingen van de openbare veiligheid, voor zover die mogelijkheid afhankelijk wordt gesteld van de strikte naleving van materiële en procedurele voorwaarden, dat de bewaring niet langer duurt dan strikt noodzakelijk is in het licht van de nagestreefde doelstelling en dat de maatregel voorziet in strikte voorwaarden en waarborgen met betrekking tot het gebruik van de gegevens.

In dat kader merkt de verzoekende partij op dat artikel 8 van de wet van 20 juli 2022 in het algemeen voorziet in de verplichting om het rijksregisternummer, de gegevens van de *identifier* en het IP-adres dat heeft gediend voor de inschrijving of voor de activering van de elektronische-communicatiediensten te bewaren. Het verduidelijkt niet binnen welk kader die gegevens moeten worden bewaard, in tegenstelling tot hetgeen is bepaald in artikel 5 van die wet. Die gegevens worden tot twaalf maanden na het einde van de dienst bewaard. Artikel 9 van de wet van 20 juli 2022 bepaalt dat voor de geografische zones de in artikel 10 bedoelde gegevens, met name de identificatiegegevens en het IP-adres, worden bewaard. Enkel in artikel 9 wordt gepreciseerd dat de doeleinden bestaan in de vrijwaring van de nationale veiligheid, de bestrijding van zware criminaliteit, de preventie van ernstige bedreigingen van de openbare veiligheid en de bescherming van de vitale belangen van een natuurlijke persoon. Tot slot legt artikel 12 de bewaring van een lange reeks identificatiegegevens op. De verzoekende partij voert aan dat dat systeem niet strookt met de eisen van het Hof van Justitie, aangezien het doeleinde van de bewaring veel ruimer is dan enkel de nationale veiligheid, de bestrijding van zware criminaliteit en de preventie van ernstige bedreigingen van de openbare veiligheid. De voormelde bepalingen van de wet van 20 juli 2022 leggen immers geen enkele grondslag vast voor de bewaring of voorzien in een grondslag die bestaat in de veiligheid van het netwerk of de bescherming van de vitale belangen van een natuurlijke persoon. Alleen in artikel 9 van de wet is een zeker kader bepaald. Bovendien voorziet geen enkele bepaling in materiële en procedurele voorwaarden die het gebruik van de beoogde gegevens regelen.

A.12.4. De verzoekende partij maakt aanvullende opmerkingen met betrekking tot het doeleinde dat is gericht op de bestrijding van fraude en het kwaadwillige gebruik van netwerken, enerzijds, en met betrekking tot het doeleinde inzake vrijwaring van de veiligheid en de correcte werking van het netwerk, anderzijds. Zij betoogt dat artikel 5 van de wet van 20 juli 2022 duidelijk een onderscheid maakt tussen die doeleinden en dat die bepaling een algemene bewaring van de verkeersgegevens van de gebruikers invoert. Bovendien wordt niet getoetst of de gegevensbewaring noodzakelijk is.

Wat meer bepaald de verantwoordelijkheid betreft die aan de operatoren wordt gedelegeerd opdat zij de nodige verkeersgegevens bewaren teneinde de veiligheid en de goede werking van de netwerken en de diensten te waarborgen, voert de verzoekende partij aan dat dat doeleinde niet is vermeld in artikel 23 van de AVG, zodat de maatregel niet toelaatbaar is. In dat verband kan artikel 6, lid 1, *f)*, van de AVG niet worden aangevoerd. In de veronderstelling dat die maatregel zou kunnen worden verantwoord door artikel 15, lid 1, van de richtlijn 2002/58/EG, zou artikel 5 van de wet van 20 juli 2022 tot slot leiden tot een algemene gegevensbewaring die niet bestaanbaar is met artikel 6, leden 1 en 2, van het Verdrag betreffende de Europese Unie.

A.13.1. De verzoekende partij leidt een derde middel af uit de schending van de artikelen 11, 12, 22 en 29 van de Grondwet, van artikel 15, lid 1, en van de artikelen 5, 6 en 9 van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8, 11, 47 en 52, lid 1, van het Handvest, uit de schending van de artikelen 6, 8, 10, 11 en

18 van het Europees Verdrag voor de rechten van de mens en van de artikelen 13 en 54 van de richtlijn (EU) 2016/680. Zij betoogt dat de artikelen 10 en 11 van de wet van 20 juli 2022 de operatoren ertoe verplichten bepaalde gegevens te bewaren in vijf welbepaalde zones, hetgeen in de feiten leidt tot een algemene en ongedifferentieerde bewaring van het merendeel van de verkeers- en locatiegegevens voor een periode die niet systematisch bij wet is vastgesteld, maar die met name bij koninklijk besluit moet worden verduidelijkt. Artikel 10 van de wet van 20 juli 2022 leidt, in het bijzonder, tot de bewaring van de locatiegegevens van personen die zich niet in de geografische zone bevinden waarvoor de gegevens moeten worden bewaard.

A.13.2. De verzoekende partij preciseert dat artikel 11 van de wet van 20 juli 2022 bepaalt dat de beoogde gegevens hetzij gedurende zes tot twaalf maanden worden bewaard, hetzij voor een periode die niet bij de wet is bepaald, hetzij voor een bij koninklijk besluit vast te leggen periode. Volgens haar voldoet artikel 11 dan ook niet aan de door het Hof van Justitie opgelegde voorwaarde dat de periode niet langer is dan strikt noodzakelijk. Allereerst zijn de bewaringstermijnen van zes tot twaalf maanden dermate lang dat zij toelaten precieze informatie over het privéleven van de gebruiker van het elektronische-communicatiemiddel te verschaffen. Wat betreft de door het OCAD bepaalde zones, geldt vervolgens de verplichting tot algemene bewaring op het hele grondgebied zodra dat orgaan inschat dat de dreiging op niveau 3 staat voor het volledige grondgebied. In die hypothese moet de bewaarplicht bij koninklijk besluit worden bevestigd, met dien verstande dat, wanneer die bevestiging er niet komt, een einde wordt gemaakt aan de gegevensbewaring. De bewaringstermijn is dus niet erg duidelijk. Tot slot is niet in enige termijn voorzien voor de zones bedoeld in artikel 126/3, §§ 3 tot 5, van de wet van 13 juni 2005, ingevoegd bij artikel 11 van de wet van 20 juli 2022. Voor die laatste heeft de wetgever enkel bepaald dat de bewaringstermijn bij koninklijk besluit wordt vastgesteld, zonder dat daarbij minimum- of maximumtermijnen worden vastgelegd. Bijgevolg voldoet artikel 11 van de wet van 20 juli 2022 niet aan de door het Hof van Justitie gestelde voorwaarde volgens welke de gegevens slechts worden bewaard indien is voldaan aan materiële en procedurele voorwaarden die door middel van duidelijke en nauwkeurige regels zijn geformuleerd.

A.13.3. Wat betreft de geografische zones die rond de in artikel 11 van de wet van 20 juli 2022 bepaalde criminaliteitscijfers zijn ingericht, betoogt de verzoekende partij dat de noodzaak van de maatregel niet is aangetoond. Uit de parlementaire voorbereiding van die wet blijkt immers dat er geen precieze gegevens bestaan wat betreft de gevolgen die de bewaring van de gegevens heeft voor de bestrijding van zware criminaliteit. Bovendien is de maatregel waarin artikel 11 van de wet van 20 juli 2022 voorziet, niet gekoppeld aan strategische plaatsen of plaatsen die door een groot aantal personen worden bezocht, maar enkel aan criminaliteitscijfers. Er wordt een permanente situatie geschapen, aangezien de lijst met zones jaarlijks wordt opgesteld. Daarnaast is de criminaliteitsgraad die verband houdt met de strafbare feiten in de zone laag, waardoor het gekozen criterium te ruim is. De maatregel treft op zich de grote meerderheid van de burgers die niets met strafbare feiten te maken hebben. Volgens de verzoekende partij kan uit de in artikel 11 van de wet van 20 juli 2022 gekozen lage criminaliteitscijfers niet worden afgeleid dat er een hoog risico op strafbare feiten is, zelfs niet rekening houdend met de aard van de beoogde strafbare feiten. De maatregel is dan ook niet evenredig en niet bestaanbaar met de grondrechten van de burgers, zoals bovendien blijkt uit de parlementaire voorbereiding van de wet van 20 juli 2022, die daarenboven aantoont dat de wetgever niet in de mogelijkheid is om precies aan te geven welk percentage van het grondgebied of welk percentage van de bevolking daadwerkelijk wordt beoogd.

De verzoekende partij wijst erop dat het door de wetgever gekozen criterium dat is van de strafbare feiten bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering. Door het grote aantal in die bepaling bedoelde strafbare feiten is het voormelde criterium te ruim voor het bepalen van de strafbare feiten die in het kader van de gegevensbewaring in aanmerking moeten worden genomen. Volgens de verzoekende partij kan de bevoegdheid van de onderzoeksrechter in het kader van artikel 90*ter* van het Wetboek van stafvordering niet als verantwoording dienen voor de bestreden maatregel inzake gegevensbewaring, die een algemene bewaringsmaatregel blijkt te zijn die niet bestaanbaar is met het uitzonderlijke en subsidiaire karakter van een methode waarbij een inmenging plaatsvindt in de bij de artikelen 7 en 8 van het Handvest en bij artikel 22 van de Grondwet gewaarborgde grondrechten in het kader van de strijd tegen zware criminaliteit. De verzoekende partij preciseert dat niet alle strafbare feiten bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering onder het begrip « zware criminaliteit » vallen, daar sommige ervan worden bestraft met een gevangenisstraf van drie maanden tot twee jaar. Bovendien is de lijst van artikel 90*ter* van het Wetboek van strafvordering opgesteld om de specifieke bevoegdheid van de onderzoeksrechter af te bakenen en niet om zware criminaliteit te definiëren in het kader van de gegevensbescherming, hetgeen niet bestaanbaar is met de rechtspraak van het Hof van Justitie. Daarnaast kent het begrip « zware criminaliteit » op zich geen exacte definitie in het strafrecht. Het gekozen criterium maakt overigens geen onderscheid tussen vervolging, veroordeling, niet-vervolging en seponering. Voor het overige dient te worden opgemerkt dat het begrip « zwaar strafbaar feit » niet overdreven ruim mag worden geïnterpreteerd door de lidstaten van de Europese Unie.

A.13.4. De verzoekende partij betwist de bewering dat de bedoelde vaststellingen van het aantal strafbare feiten op een wetenschappelijke en objectieve wijze kunnen worden verricht op basis van de in de wet van 20 juli 2022 bepaalde statistische gegevens, aangezien de door de wetgever daartoe aangewezen gegevensbank niet met dat doel is ontworpen. Die gegevensbank bevat een groot aantal gegevens die gewoonweg verband houden met strafbare feiten, met name de gegevens van slachtoffers, de terechte of onterechte meldingen van strafbare feiten, alsook de feiten die hebben geleid tot een schuldigverklaring. Anders gezegd, de wetgever beoogt niet alleen de feiten die voor de rechter zijn gebracht en tot een veroordeling hebben geleid, terwijl het nochtans het aantal effectief gepleegde strafbare feiten is dat bepaalt of er aan gegevensbewaring kan worden gedaan in een bepaald arrondissement. Bovendien had de Gegevensbeschermingsautoriteit in het kader van haar advies over de wet van 20 juli 2022 twijfels bij de relevantie van het gebruik van die gegevensbank.

In tegenstelling tot wat de Ministerraad aanvoert, stelt de verzoekende partij dat het niet nodig is een oplossing naar voren te schuiven ter vervanging van de door de wetgever gekozen gegevensbank teneinde de irrelevantie van die laatste aan te tonen. Hoe dan ook zou het wenselijk zijn dat de wet van 20 juli 2022 betrekking heeft op een specifieke gegevensbank, rekening houdend met de aanzienlijke impact ervan op het recht op eerbiediging van het privéleven, en dat die gegevensbank op zaken berust die daadwerkelijk aanhangig zijn gemaakt bij het parket of de rechtbanken met het oog op vervolging.

A.13.5. Wat betreft de gegevensbewaring in het kader van een dreiging van niveau 3, waarin artikel 11 van de wet van 20 juli 2022 eveneens voorziet, voert de verzoekende partij aan dat de door het Hof van Justitie geformuleerde eisen worden geschonden. Er wordt immers in geen effectieve rechterlijke controle voorzien om na te gaan of een dergelijk niveau is vastgesteld. Hoewel het dreigingsniveau 4 overeenstemt met een dreiging die ernstig en zeer nabij is, moet overigens worden vastgesteld dat het niveau 3 niet die graad van ernst bereikt, zodat dat dat laatste niveau niet beantwoordt aan het begrip « werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid » dat is verankerd in de rechtspraak van het Hof van Justitie. Bovendien beantwoordt artikel 11 van de wet van 20 juli 2022 niet aan de voorwaarde volgens welke de gegevensbewaringsmaatregel niet langer dan strikt noodzakelijk kan worden opgelegd. In artikel 11 wordt overigens niet verduidelijkt hoe een einde wordt gemaakt aan die maatregel, met uitzondering wat betreft de automatische beëindiging van een maatregel die het volledige grondgebied dekt bij ontstentenis van een koninklijk besluit tot bekrachtiging ervan.

A.13.6. Artikel 11 van de wet van 20 juli 2022 heeft bovendien betrekking op drie bij artikel 126/3, §§ 3 tot 5, van de wet van 13 juni 2005 ingevoegde zones die worden onderscheiden op basis van de aard van de bedreiging waaraan zij kunnen worden blootgesteld. Volgens de verzoekende partij is het aantal plaatsen en infrastructuren waarvoor gegevens moeten worden bewaard in het kader van die zones, dermate groot dat vrijwel het volledige Belgische grondgebied wordt beoogd, hetgeen leidt tot een algemene en ongedifferentieerde bewaring van de gegevens van de hele bevolking. Bovendien is de perimeter van de zones niet bij wet bepaald, maar bij een koninklijk besluit, zonder dat de wetgever in een minimum- of maximumperimeter voorziet. Voor het overige heeft de Gegevensbeschermingsautoriteit erop gewezen dat artikel 11 van de wet van 20 juli 2022 plaatsen beoogt die niet enkel worden gekenmerkt door een hoog risico op het voorbereiden of plegen van daden van zware criminaliteit, zoals de rechtspraak van het Hof van Justitie vereist.

Wat betreft de in artikel 11 van de wet van 20 juli 2022 bedoelde *de facto* algemene gegevensbewaring, preciseert de verzoekende partij dat die bepaling voorziet in de bewaring van gegevens in de gemeenten waar zich kritieke infrastructuren bevinden. In de feiten is die maatregel gericht op de gegevens van iedere persoon die verbinding maakt met de internetservers van die infrastructuren, met name de servers van een ziekenhuis, maar ook de verhuurde servers in een commercieel datacenter of bij *cloudproviders*. De impact van een dergelijke gegevensbewaring is enorm en komt in werkelijkheid neer op een algemene bewaarplicht. Evenzo worden de personen die een vaste internetverbinding hebben en in de buurt wonen van bepaalde gebouwen of zones, bijvoorbeeld in de buurt van een station, eveneens geraakt door de gegevensbewaring. Artikel 10 van de wet van 20 juli 2022 heeft immers niet alleen betrekking op de mobiele netwerken, maar ook op bepaalde vaste internetverbindingen. Die maatregel is geenszins pertinent wat betreft zware criminaliteit of nationale veiligheid.

A.13.7. Artikel 11 van de wet van 20 juli 2022 bepaalt dat de omvang van de perimeter van bepaalde zones bij koninklijk besluit wordt vastgesteld, zonder dat de wetgever zelf de na te leven minimum- en maximumperimeters vastlegt. Een dergelijke maatregel is strijdig met het verbod op een algemene en ongedifferentieerde gegevensbewaring, daar hij niet beantwoordt aan de vereiste van duidelijkheid en nauwkeurigheid. Bovendien komt het de wetgever toe om zelf de lijst van de zones en de perimeter daarvan vast te stellen. Het in artikel 22 van de Grondwet vervatte beginsel van de formele wettigheid is geschonden.

A.13.8. De verzoekende partij merkt op dat artikel 45 van de wet van 20 juli 2022 bepaalt dat de gerichte gegevensbewaring op basis van de in artikel 126/3, §§ 3 tot 5, van de wet van 13 juni 2005 bedoelde criteria in werking treedt op een bij koninklijk besluit vastgestelde datum, uiterlijk op 1 januari 2027. Die uiterste datum bevestigt dat de gegevensbewaringsmaatregel niet haalbaar is, omdat er veel tijd nodig is om het systeem in de beoogde zones in werking te stellen. Bovendien is het niet coherent dat die overgangsmaatregel betrekking heeft op bepaalde zones en niet op andere, terwijl de legitieme belangen en technische moeilijkheden dezelfde zijn voor de verschillende zones.

A.13.9. Wat betreft het gebruik door artikel 11 van de wet van 20 juli 2022 van variabelen, teneinde een soepel systeem op te zetten dat overeenstemt met de realiteit op het terrein, betoogt de verzoekende partij dat de wetgever louter willekeurige kwantitatieve criteria in het leven heeft geroepen die kunnen worden betwist ten aanzien van de beginselen van noodzakelijkheid, evenredigheid en subsidiariteit. De drempels die in de wet van 20 juli 2022 in aanmerking worden genomen, verwijzen naar lage criminaliteitscijfers die niet ernstig zijn. In tegenstelling tot wat de Ministerraad aanvoert, staat het wel degelijk aan het Hof om die drempels te onderzoeken in het kader van zijn evenredigheidstoets. Wat betreft de variabelen met betrekking tot de bewaringstermijn, wijst de verzoekende partij erop dat dat mechanisme flagrant in tegenspraak is met, enerzijds, de bepaling van de wet van 20 juli 2022 waarin de zwaarte van de strafbare feiten wordt vastgesteld op basis van de statistieken met betrekking tot het aantal strafbare feiten over een gemiddelde van drie jaar en, anderzijds, de bepaling waarin elk jaar de lijst van de arrondissementen en politiezones wordt vastgesteld. Artikel 11 van de wet van 20 juli 2022 is niet bestaanbaar met de noodzaak om het hoge risico op daden van zware criminaliteit te bestrijden, aangezien de zones in de feiten elk jaar *a posteriori* worden vastgesteld voor een variabele bewaringstermijn, daar zij ontstaan zijn uit vroegere criminaliteitsstatistieken. In werkelijkheid houdt de lijst die jaarlijks wordt opgesteld gewoonweg geen rekening met de actuele realiteit op het terrein. Voor het overige is de verzoekende partij van mening dat kan worden betwist of het mechanisme van periodieke herziening toepasbaar is, en dat dat mechanisme niet aantoont dat de in artikel 11 van de wet van 20 juli 2022 bedoelde maatregel noodzakelijk is.

A.13.10. De verzoekende partij beklemtoont dat artikel 11 van de wet van 20 juli 2022 gelijkstaat met een algemene en ongedifferentieerde bewaarplicht van de gegevens. In haar advies over het voorontwerp van wet dat aan de oorsprong ligt van die wet had de afdeling wetgeving van de Raad van State trouwens vragen bij de keuze voor de geografische zones en bij de noodzaak om de verschillende types van zones vast te stellen. De maatregel lijkt dus onevenredig en niet bestaanbaar met de rechtspraak van het Hof van Justitie. De verzoekende partij voert bovendien aan dat het argument van de Ministerraad volgens hetwelk de kenmerken die eigen zijn aan de Belgische Staat, die laatste zouden onderscheiden van andere Staten, en de noodzaak en de evenredigheid van de maatregel zouden verantwoorden, niet verdedigbaar is. In de feiten zou dat argument verantwoorden dat elke lidstaat met een kleinere oppervlakte zich kan onttrekken aan de werkingssfeer van artikel 15, lid 1, van de richtlijn 2002/58/EG. Bijgevolg kan niet staande worden gehouden dat objectieve factoren een algemene gegevensbewaring verantwoorden op het hele grondgebied.

A.14.1. Een vierde middel is afgeleid uit de schending van de artikelen 11, 12, 22 en 29 van de Grondwet, van artikel 15, lid 1, en van de artikelen 5, 6 en 9 van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8, 11, 47 en 52, lid 1, van het Handvest, van de artikelen 6, 8, 10, 11 en 18 van het Europees Verdrag voor de rechten van de mens en van de artikelen 13 en 54 van de richtlijn (EU) 2016/680. De verzoekende partij betoogt dat artikel 13 van de wet van 20 juli 2022, dat betrekking heeft op de autoriteiten die toegang mogen krijgen tot de door de operatoren krachtens de artikelen 5 en 6 van die wet bewaarde gegevens, niet bestaanbaar is met de rechtspraak van het Hof van Justitie. Volgens haar dient de toegang tot de gegevens te worden verantwoord vanuit het oogpunt van de vrijwaring van de nationale veiligheid of de bestrijding van zware criminaliteit, met dien verstande dat, wanneer de gegevens werden bewaard op de grondslag van de nationale veiligheid, de grondslag van de zware criminaliteit niet kan worden aangevoerd. Artikel 13 van de wet van 20 juli 2022 heeft echter een te ruime draagwijdte, aangezien de bedoelde autoriteiten niet bevoegd zijn om de nationale veiligheid te vrijwaren of zware criminaliteit te bestrijden. Bijgevolg is de maatregel niet in overeenstemming met artikel 15, lid 1, van de richtlijn 2002/58/EG.

Artikel 13 van de wet van 20 juli 2022 maakt tien onderscheiden autoriteiten bevoegd om toegang tot de beoogde gegevens te krijgen. Van die autoriteiten zijn de meeste nieuw ten opzichte van de vroegere regelingen die reeds door het Hof waren afgekeurd. De omstandigheid dat de toegang tot de gegevens in zekere mate beperkt is, is niet van dien aard dat zij aantoont dat de inmenging in de grondrechten verantwoord is, aangezien de beoogde gegevens zeer ruim zijn. Bovendien is het in dat artikel 13 bepaalde begrip « zware criminaliteit » niet hetzelfde als datgene dat wordt bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van stafvordering, waarvan sprake is in artikel 11 van de wet van 20 juli 2022. Dat artikel 13 heeft in dat opzicht een veel ruimere draagwijdte, hetgeen leidt tot tegenspraak wat betreft het begrip « zware criminaliteit » in het kader van de gegevensbewaring, enerzijds,

en in het kader van de toegang tot de gegevens, anderzijds. Om die reden wordt artikel 15, lid 1, van de richtlijn 2002/58/EG geschonden. De verzoekende partij voert bovendien aan dat de in artikel 13 van de wet van 20 juli 2022 beoogde administratieve autoriteiten geen toegang mogen krijgen tot de gegevens in het kader van zware criminaliteit en dat de verschillende in die bepaling vermelde doeleinden geen grondslagen vormen op basis waarvan gegevensverwerking is toegestaan in het licht van de rechtspraak van het Hof van Justitie, van de richtlijn 2002/58/EG en van de AVG.

A.14.2. De verzoekende partij betoogt dat, in zoverre artikel 13 van de wet van 20 juli 2022 de « administratieve of gerechtelijke autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing of de vervolging van een online gepleegde inbreuk of een inbreuk gepleegd via een elektronische-communicatienetwerk of -dienst » betreft, dat artikel problematisch is aangezien het niet beperkt is tot de strafbare feiten die onder zware criminaliteit vallen, maar betrekking heeft op alle strafbare feiten. Bovendien vermeldt artikel 13 dat de erin beoogde autoriteiten enkel toegang mogen hebben krachtens een formele wetskrachtige norm, zonder dat die norm wordt geïdentificeerd. De wetgever heeft trouwens bepaald dat de lijst van de autoriteiten die ertoe gemachtigd zijn van de operator de bewaarde gegevens te ontvangen, bij een ministeriële omzendbrief wordt vastgesteld. De verzoekende partij merkt in dat verband op dat niet wordt gepreciseerd wie daarvoor de bevoegde minister is en dat het in elk geval niet een omzendbrief is waarbij de inhoud van de wet kan worden gewijzigd. Die maatregel lijkt eveneens in tegenspraak te zijn met het feit dat artikel 13 van de wet van 20 juli 2022 ook bepaalt dat enkel de in de wet bedoelde autoriteiten van de operatoren toegang mogen krijgen tot de gegevens.

A.14.3. De verzoekende partij leidt een vijfde middel af uit de schending van de artikelen 10, 11, 22 en 29 van de Grondwet, al dan niet in samenhang gelezen met artikel 15, lid 1, en de artikelen 5, 6 en 9 van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8, 11, 47 en 52, lid 1, van het Handvest, van de artikelen 6, 8, 10, 11 en 18 van het Europees Verdrag voor de rechten van de mens en van de artikelen 13 en 54 van de richtlijn (EU) 2016/680. De verzoekende partij merkt op dat de wet van 20 juli 2022 met name betrekking heeft op de bewaring van communicatiegegevens van aan het beroepsgeheim onderworpen personen, namelijk artsen, advocaten en journalisten, en zulks op dezelfde wijze als de bewaring van de communicatiegegevens van de andere personen, die niet aan het beroepsgeheim zijn onderworpen. De wetgever heeft echter in geen enkel pertinent controlemechanisme voorzien dat het de aan het beroepsgeheim onderworpen personen mogelijk maakt zich te verzetten tegen de verzameling, de bewaring of de kennisname van hun gegevens, terwijl zij zich in een situatie bevinden die objectief verschilt van die van andere personen.

Bovendien wijst de verzoekende partij erop dat artikel 88*bis* van het Wetboek van strafvordering, gewijzigd bij artikel 27 van de wet van 20 juli 2022, een onderzoeksrechter machtigt om een advocaat of een arts te viseren die zelf wordt verdacht van een strafbaar feit. Er is weliswaar bepaald dat de stafhouder of de provinciale vertegenwoordiger van de Orde der artsen op de hoogte wordt gebracht bij de tenuitvoerlegging van de maatregel en dat wat onder het beroepsgeheim valt, niet wordt opgenomen in het proces-verbaal. Die waarborgen zijn evenwel onvoldoende om te verzekeren dat het procedé grondwettig is. Bovendien is niet in enige waarborg voorzien ten aanzien van de andere autoriteiten dan de onderzoeksrechter, terwijl ook de eerstgenoemde de toegang kunnen vragen tot de gegevens van advocaten, artsen of journalisten.

Zaak nr. 7931

A.15. De verzoekende partij leidt een enig middel af uit de schending van de artikelen 11, 12, 22 en 29 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 7, 8, 11, 47 en 52, lid 1, van het Handvest, met artikel 8 van het Europees Verdrag voor de rechten van de mens, met de artikelen 5, 6 en 15 van de richtlijn 2002/58/EG en met de artikelen 13 en 54 van de richtlijn (EU) 2016/680.

A.16.1. Allereerst, wat betreft de systematische en ongedifferentieerde verzameling van bepaalde gegevens, merkt de verzoekende partij op dat de wet van 20 juli 2022 aan de operatoren de bewaring oplegt van bepaalde identificatiegegevens, bovenop de gegevens die reeds moeten worden verzameld om de abonnees te identificeren, waaronder het rijksregisternummer. De gegevens dienen te worden bewaard gedurende het gebruik van de dienst en tot twaalf maanden na de datum van de laatste communicatie met behulp van de dienst, zonder dat de wetgever evenwel aangeeft waarom die bewaringstermijn noodzakelijk blijkt ten aanzien van de nagestreefde doelstelling. Bovendien, hoewel het Hof van Justitie in principe toelaat dat de verzamelde gegevens met betrekking tot de burgerlijke identiteit van de gebruikers worden bewaard zonder specifieke termijn, dient te worden vastgesteld dat te dezen de wet van 20 juli 2022 betrekking heeft op andere gegevens, met name de *identifier* gecreëerd voor elke communicatie, de datum van het begin van het abonnement of de gegevens met betrekking tot de betaling. In elk geval laat die informatie toe personen te lokaliseren. De wetgever geeft echter niet aan waarom de verzameling

van die gegevens noodzakelijk is ten aanzien van de nagestreefde doelstelling, zodat artikel 8 van de wet van 20 juli 2022 onevenredig is en de in het middel aangehaalde bepalingen schendt.

In geval van twijfel over artikel 8 van de wet van 20 juli 2022 dient volgens de verzoekende partij in de zaak nr. 7931 een prejudiciële vraag te worden gesteld aan het Hof van Justitie om te bepalen of artikel 15, lid 1, van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8, 11 en 52, lid 1, van het Handvest, in de weg staat aan een wetgevende maatregel waarbij, zonder specifieke termijn, de bewaring van verschillende identificatiegegevens van alle gebruikers van elektronische-communicatiemiddelen wordt opgelegd om te strijden tegen strafbare feiten en om de openbare veiligheid te vrijwaren, dan wel of die bepaling moet worden beperkt tot het verzamelen van gegevens met betrekking tot de burgerlijke identiteit van de gebruiker.

A.16.2. De verzoekende partij merkt op dat het Hof van Justitie de systematische en ongedifferentieerde verzameling van IP-adressen toelaat in het kader van de strijd tegen zware criminaliteit en de preventie van ernstige bedreigingen van de openbare veiligheid. Desalniettemin laat de wet van 20 juli 2022 de toegang tot IP-adressen toe in veel ruimere hypotheses. Bovendien laat artikel 13 van die wet toe dat autoriteiten die niet belast zijn met de strijd tegen zware criminaliteit toegang hebben tot IP-adressen, hetgeen niet toelaatbaar is. Bovendien legt het Hof van Justitie op dat de bewaringstermijn wordt beperkt tot het strikt noodzakelijke ten aanzien van de nagestreefde doelstelling, hetgeen de wetgever niet uitlegt, en dat strikte voorwaarden en waarborgen worden opgesteld wat betreft de verwerking van de gegevens, waarin de wet van 20 juli 2022 niet voorziet.

A.16.3. De verzoekende partij merkt overigens op dat artikel 5 van de wet van 20 juli 2022 de operatoren ertoe verplicht de locatiegegevens en de andere verkeersgegevens te bewaren, en in voorkomend geval te verwerken, die nodig zijn om vermeende fraude of vermeend kwaadwillig gebruik van het elektronische-communicatienetwerk op te sporen en te analyseren. De begrippen « fraude » en « kwaadwillig gebruik van het netwerk » zijn bij de wet en in de parlementaire voorbereiding ervan gedefinieerd, waarbij in die laatste meerdere concrete voorbeelden worden gegeven. Op die manier voert de wetgever in werkelijkheid een verplichting tot systematische en ongedifferentieerde verzameling en bewaring van bepaalde gegevens in omwille van de strijd tegen criminaliteit in het algemeen. Het Hof van Justitie preciseert evenwel dat enkel de strijd tegen zware criminaliteit een inmenging in de bij de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten kan verantwoorden, hetgeen niet het geval is voor vermeende fraude of vermeend kwaadwillig gebruik van het netwerk. In dat kader is de omstandigheid dat de verzameling beperkt is tot bepaalde categorieën van gegevens niet pertinent. Volgens de wetgever is het niet mogelijk om in een minder ingrijpend systeem te voorzien. De Gegevensbeschermingsautoriteit heeft niettemin benadrukt dat maatregelen mogelijk waren die minder afbreuk doen, bijvoorbeeld door te voorzien in een verplichting tot bewaring van gegevens wanneer aanwijzingen bestaan van fraude of van kwaadwillig gebruik van het netwerk. Bovendien lijkt de bewaringstermijn van de gegevens kennelijk onevenredig te zijn. In elk geval probeert de Ministerraad het noodzakelijke karakter van de maatregel aan te tonen, terwijl het de evenredigheid ervan is die in het geding is gebracht.

Voor het overige moet, volgens de verzoekende partij, in geval van twijfel wat betreft artikel 5 van de wet van 20 juli 2022, een prejudiciële vraag worden gesteld aan het Hof van Justitie om te bepalen of artikel 15, lid 1, van de richtlijn 2002/58/EG, in samenhang gelezen met de artikelen 7, 8 en 52, lid 1, van het Handvest, in de weg staat aan een algemene verplichting, voor de operatoren en de aanbieders van elektronische-communicatiediensten, van toepassing op andere feiten dan handelingen van zware criminaliteit, omwille van de opsporing en de analyse van vermeende fraude of vermeend kwaadwillig gebruik van een elektronische-communicatienetwerk, om de verkeers- en locatiegegevens in de zin van die richtlijn, gegenereerd of verwerkt in het kader van de levering van die diensten, te bewaren.

A.16.4. Artikel 5 van de wet van 20 juli 2022 laat de mogelijkheid aan de operatoren om de verkeersgegevens te bewaren en te verwerken die nodig zijn om de veiligheid en de correcte werking van de elektronische-communicatienetwerken en -diensten te waarborgen, in het bijzonder om een mogelijke of werkelijke aanslag op die veiligheid op te sporen en te analyseren, inclusief om de oorsprong van die aanslag te identificeren. De verzoekende partij stelt vast dat de operatoren bovendien reeds gebonden zijn door een verplichting om de technische en organisatorische maatregelen te nemen teneinde de risico's inzake de veiligheid van de netwerken en van de diensten op gepaste wijze te beheren, in voorkomend geval gezamenlijk om de veiligheid van het netwerk te waarborgen. Zij mogen ook de betrokken personen identificeren door informatie door te geven en kennis te nemen van gegevens inzake elektronische communicatie indien de goede werking van het netwerk en de goede uitvoering van een elektronische-communicatiedienst dat vereisen. Bijgevolg ziet de verzoekende partij niet in hoe artikel 5 van de wet van 20 juli 2022 noodzakelijk blijkt bovenop de reeds bestaande verplichtingen. Bovendien laat die bepaling de verwerkingsverantwoordelijke toe om geen afweging meer te

maken van de aanwezige belangen om zich ervan te vergewissen dat er geen andere manieren zijn om de beoogde doelstelling te bereiken die minder ingrijpend zijn voor de betrokken persoon. De maatregel is dus onevenredig.

A.17.1. Wat betreft de bij de wet van 20 juli 2022 bepaalde gerichte bewaring van gegevens, geeft de verzoekende partij aan dat de wetgever heeft voorzien in een statistisch criterium en bepaalde zones heeft beoogd waar een hoge graad van zware criminaliteit heerst. De gegevens die dienen te worden bewaard, zijn opgesomd in artikel 10 van de wet van 20 juli 2022. Zij worden krachtens artikel 9 van die wet systematisch en ongedifferentieerd bewaard, op basis van een geografisch criterium dat bij artikel 11 nauwkeurig wordt bepaald. Volgens dat systeem legt de wetgever de verzameling van verkeers- en locatiegegevens op voor bepaalde zones met een hoge graad van zware criminaliteit, berekend op basis van het jaarlijkse gemiddelde aantal strafbare feiten bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering die zijn vastgesteld per politiezone of per gerechtelijk arrondissement, per duizend inwoners, over een gemiddelde van drie jaar. De bewaartermijn van de gegevens, tussen zes en twaalf maanden, varieert op basis van het aantal vastgestelde strafbare feiten. Volgens de verzoekende partij verantwoordt de wetgever echter niet de redenen waarom de gegevens gedurende die termijn moeten worden bewaard, noch waarom die bewaring noodzakelijk is. Bovendien, hoewel het Hof van Justitie de systematische en ongedifferentieerde verzameling van de gegevens omwille van de strijd tegen ernstige criminaliteit toelaat, dient te worden vastgesteld dat de wet van 20 juli 2022 de criminaliteit in het algemeen beoogt, aangezien de in artikel 90*ter* van het Wetboek van strafvordering beoogde strafbare feiten met name gemeenrechtelijke misdrijven zijn zoals valsheid in informatica, informaticabedrog of diefstal met geweld. In werkelijkheid had de wetgever zich kunnen richten op bepaalde strafbare feiten op basis van de straf die eraan is verbonden. De voormelde bepalingen van de wet van 20 juli 2022 dienen dus te worden vernietigd.

In tegenstelling tot hetgeen de Ministerraad aanvoert, kan het begrip « zwaar strafbaar feit » niet volledig aan de beoordeling van de lidstaten worden overgelaten, om geen uiteenlopende interpretaties van de in artikel 15, lid 1, van de richtlijn 2002/58/EG bedoelde doelstellingen te veroorzaken. In geval van twijfel daaromtrent dient een prejudiciële vraag te worden gesteld aan het Hof van Justitie om te bepalen of artikel 15, lid 1, van de richtlijn 2002/58/EG, in samenhang gelezen met de artikelen 7, 8 en 52, lid 1, van het Handvest, in de weg staat aan een gerichte bewaring van gegevens met betrekking tot het verkeer en de locatie, beperkt aan de hand van een geografisch criterium tot andere doeleinden dan zware criminaliteit, namelijk de strijd tegen valsheid in informatica, informaticabedrog of diefstel met geweld, los van de strafmaat. In haar memorie van antwoord stelt de verzoekende partij voor om aan het Hof van Justitie ook een vraag te stellen om te bepalen of de begrippen « zwaar strafbaar feit » en « zware criminaliteit » in de zin van de rechtspraak van het Hof van Justitie autonome begrippen zijn van het Unierecht, dan wel of het aan de bevoegde autoriteiten van de lidstaten staat om de inhoud ervan zelf te preciseren en, in de hypothese waarin het autonome begrippen van het Unierecht zouden zijn, om de nadere regels te bepalen volgens welke moet worden bepaald of er sprake is van zware strafbare feiten of zware criminaliteit.

A.17.2. De verzoekende partij voegt eraan toe dat de voormelde bepalingen van de wet van 20 juli 2022 geen indicator vaststellen met betrekking tot het aantal gepleegde feiten, in tegenstelling tot hetgeen in de parlementaire voorbereiding is vermeld, aangezien zij voorzien in een criterium gebaseerd op gegevens met betrekking tot de kwalificatie van de feiten bij het begin van het onderzoek, zodat er onjuistheden bestaan, met name wanneer de kwalificatie van de feiten in de loop van het onderzoek wordt gewijzigd of wanneer de feiten worden geseponeerd. Er had een meer nauwkeurig criterium in aanmerking kunnen worden genomen, zoals het aantal strafbare feiten die tot een veroordeling door de hoven en rechtbanken hebben geleid. In tegenstelling tot hetgeen de Ministerraad aanvoert, in de hypothese waarin de verplichting tot bewaring van de metagegevens voor het volledige grondgebied zou gelden, zou dat niet zijn wegens een hoge criminaliteitsgraad in de verschillende zones, maar wegens een bijzonder ruim geografisch criterium dat de criminaliteit in het algemeen omvat en dat is gebaseerd op onjuiste gegevens, aangezien de door de wet van 20 juli 2022 in aanmerking genomen statistische gegevens niet betrouwbaar zijn. Bovendien veroorzaakt de toepassing van het geografische criterium bepaalde moeilijkheden voor diensten zoals WhatsApp, Skype of Facebook, die onderworpen zijn aan dezelfde verplichtingen als de andere operatoren, terwijl die diensten niet altijd in staat zijn om de locatie van de gebruiker te bepalen. In die hypothese blijkt uit de wet van 20 juli 2022, met name uit artikel 9 ervan, dat alle gegevens *a minima* dienen te worden bewaard om de betrokken zone te dekken, hetgeen dus een verzameling veronderstelt van de gegevens die over het volledige Belgische grondgebied zijn verwerkt, hetgeen niet is toegelaten door het Hof van Justitie.

Bovendien, wanneer de operator niet in staat is om de bewaring van gegevens te beperken tot de in de wet van 20 juli 2022 beoogde zones, is hij ertoe gebonden die gegevens te bewaren maar de bewaring ervan buiten die zone tot het strikt noodzakelijke te beperken, in het licht van de technische mogelijkheden. Door dat te doen, heeft de wetgever beslist om het beginsel van de minimale gegevensverwerking op soepele wijze toe te passen, teneinde

discriminatie tussen de slachtoffers van feiten van zware criminaliteit op basis van de middelen van de operatoren te vermijden. In werkelijkheid doet hij zo afbreuk aan een grondbeginsel van het recht op bescherming van de persoonsgegevens dat niet mag worden geschonden. Om de inmenging tot het strikt noodzakelijke te beperken, had de wetgever erin moeten voorzien dat de operator in geval van twijfel enkel de gegevens met betrekking tot de betrokken zone mag bewaren.

A.17.3. Artikel 11 van de wet van 20 juli 2022 voorziet erin dat de grenzen van de zones met een hoge graad van zware criminaliteit door de Koning worden bepaald, terwijl het in artikel 22 van de Grondwet en in de artikelen 7, 8 en 52, lid 1, van het Handvest vervatte wettigheidsbeginsel oplegt dat dat element in een formele wet wordt vastgesteld. Voor het overige legt de wetgever de bewaring van gegevens op voor een zeer groot aantal zones die volgens hem een hoge graad van zware criminaliteit kennen, zonder concreet te verantwoorden hoe die zones effectief door een dergelijke hoge graad worden gekenmerkt, en dus ook zonder de redenen te verantwoorden waarom het verzamelen van gegevens noodzakelijk is ten aanzien van de nagestreefde doelstelling.

A.17.4. Bij artikel 11 wordt bovendien de gerichte bewaring van metagegevens omwille van de nationale veiligheid vastgelegd, hetgeen niet toelaatbaar is om dezelfde redenen als die welke de bewaring van gegevens voor strafrechtelijke doeleinden betreffen. Bovendien zijn de opdrachten van het OCAD, dat aan de hand van het dreigingsniveau de betrokken geografische zones in dat kader bepaalt, ruimer dan die met betrekking tot de nationale veiligheid. Het Hof van Justitie preciseert echter dat criminaliteit, zelfs zware criminaliteit, niet kan worden gelijkgesteld met een bedreiging van de nationale veiligheid. Bovendien zijn de zones waarop de bewaring van gegevens omwille van de nationale veiligheid betrekking heeft, die waarvan het dreigingsniveau ten minste 3 bedraagt, en dat zolang dat niveau aanhoudt. Dat criterium lijkt ook niet in overeenstemming te zijn met de rechtspraak van het Hof van Justitie, dat de toevlucht tot het, hogere, niveau 4, alsook een periode waarin het dreigingsniveau opnieuw dient te worden geëvalueerd, lijkt op te leggen.

Uit artikel 11 van de wet van 20 juli 2022 blijkt ook dat de wetgever de bewaring van gegevens oplegt voor een zeer groot aantal zones die volgens hem vatbaar zijn voor een bedreiging van de nationale veiligheid, zonder die maatregel, noch de noodzaak van de verzameling van de gegevens concreet te verantwoorden. Bovendien wordt in die verzameling voorzien voor zones die mogelijk vatbaar zijn voor bedreigingen van de nationale veiligheid, hetgeen niet in overeenstemming is met de rechtspraak van het Hof van Justitie, dat een reële en actuele, of voorzienbare, bedreiging van de nationale veiligheid vereist. Artikel 11 beoogt ook de potentiële bedreiging van de belangen van de internationale instellingen zonder dat dat redelijk verantwoord is. De verzoekende partij stelt vast dat ook erin is voorzien dat de Koning de lijst van de in artikel 11 opgesomde zones kan aanvullen, en de grenzen van de zones gedekt door de verplichting tot bewaring van gegevens kan aanpassen, hetgeen in strijd is met het wettigheidsbeginsel van artikel 22 van de Grondwet. Het Hof van Justitie legt bovendien op dat de bewaring van gegevens effectief wordt gecontroleerd door een rechterlijke instantie of door een onafhankelijke bestuurlijke autoriteit, waarvan de beslissing bindend is, om na te gaan of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien.

A.18. Wat betreft de regels omtrent de snelle bevriezing van gegevens, voert de verzoekende partij aan dat de in artikel 25 van de wet van 20 juli 2022 beoogde hypothesen ruimer zijn dan de hypothesen die zijn toegelaten door het Hof van Justitie, die zich beperken tot de gevallen van zware criminaliteit en niet de criminaliteit in het algemeen omvatten. Bovendien is de bewaartermijn van de gegevens kennelijk onevenredig ten aanzien van de nagestreefde doelstelling.

A.19.1. Wat betreft de toegang tot de gegevens, preciseert artikel 13 van de wet van 20 juli 2022 de bevoegde autoriteiten, met name de financiële autoriteiten, zodat de wetgever heeft geoordeeld dat de inbreuken op de reglementering omtrent marktmisbruik onder zware criminaliteit vallen. Het Hof van Justitie is evenwel van oordeel dat het inbreuken betreft die onder de criminaliteit in het algemeen vallen. Artikel 9 van de wet van 20 juli 2022 preciseert bovendien dat de Koning de lijst van bevoegde autoriteiten kan aanvullen, hetgeen in strijd is met het wettigheidsbeginsel vervat in artikel 22 van de Grondwet en in de artikelen 7, 8 en 52, lid 1, van het Handvest, die vereisen dat wordt gebruikgemaakt van een formele wet. Bovendien, volgens artikel 13 van die wet, worden in een ministeriële omzendbrief de autoriteiten opgesomd die gemachtigd zijn om de door de wet beoogde gegevens te verkrijgen, hetgeen ook in strijd is met het voormelde beginsel van de formele wettigheid. De verzoekende partij merkt nog op dat de in artikel 13 van die wet beoogde doeleinden ruimer zijn dan die welke zijn vastgesteld bij artikel 15, lid 1, van de richtlijn 2002/58/EG.

A.19.2. De voorwaarden om toegang te hebben tot de verzamelde gegevens worden gepreciseerd in artikel 13 van de wet van 20 juli 2022 en zij vereisen niet dat het verzoek tot toegang wordt gemotiveerd ten aanzien van de nagestreefde doelstelling, terwijl een verband met de doelstelling van de strijd tegen criminaliteit

wordt vereist. Bovendien laat artikel 26 van de wet van 20 juli 2022, dat de voorwaarden regelt voor de bevoegde autoriteiten om toegang te hebben tot de verzamelde gegevens voor strafrechtelijke doeleinden, de procureur des Konings of de officier van gerechtelijke politie toe om in geval van hoogdringendheid toegang te hebben tot de identificatiegegevens, terwijl het Hof van Justitie een voorafgaande controle door een rechterlijke instantie of een onafhankelijke bestuurlijke autoriteit oplegt. De procureur des Konings kan echter niet als een derde worden beschouwd in het kader van de procedure om toegang te krijgen tot de betrokken gegevens.

In geval van twijfel hierover dienen prejudiciële vragen te worden gesteld aan het Hof van Justitie om te bepalen, enerzijds, of artikel 15, lid 1, van de richtlijn 2002/58/EG, in samenhang gelezen met de artikelen 7, 8 en 52, lid 1, van het Handvest, eraan in de weg staat dat de procureur des Konings, of in geval van hoogdringendheid een officier van gerechtelijke politie, toegang heeft tot de identificatiegegevens die systematisch en ongedifferentieerd zijn verzameld omwille van de strijd tegen criminaliteit in het algemeen en, anderzijds, of het voormelde artikel 15, lid 1, in samenhang gelezen met dezelfde bepalingen van het Handvest, eraan in de weg staat dat de procureur des Konings in geval van hoogdringendheid toegang heeft tot de verkeers- en locatiegegevens omwille van de strijd tegen criminaliteit in het algemeen.

A.19.3. Bovendien laat artikel 26 van de wet van 20 juli 2022 de procureur des Konings toe om de medewerking van de gesloten centra en van de woonunits in de zin van de wet van 15 december 1980 « betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen » (hierna : de wet van 15 december 1980) op te leggen, zonder uit te leggen waarom die medewerking noodzakelijk is ten aanzien van de nagestreefde doelstelling, namelijk de strijd tegen criminaliteit.

A.19.4. Artikel 25 van de wet van 20 juli 2022 laat op zijn beurt de toegang tot de gegevens toe bij ernstige vermoedens van een strafbaar feit dat een hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kan hebben, hetgeen in werkelijkheid de grote meerderheid van de in het Strafwetboek vastgelegde strafbare feiten beoogt, die dus niet als zware criminaliteit kunnen worden gekwalificeerd.

In geval van twijfel hierover dient een prejudiciële vraag te worden gesteld aan het Hof van Justitie om te bepalen of artikel 15, lid 1, van de richtlijn 2002/58/EG, in samenhang gelezen met de artikelen 7, 8 en 52, lid 1, van het Handvest, eraan in de weg staat dat de onderzoeksrechter, of in geval van hoogdringendheid de procureur des Konings, toegang heeft tot de verkeers- en locatiegegevens omwille van de strijd tegen criminaliteit in het algemeen, aangezien op de beoogde strafbare feiten een straf staat van minimaal één jaar gevangenisstraf.

Artikel 24 van de wet van 20 juli 2022 geeft een officier van gerechtelijke politie, die geen derde is in de procedure en dus niet als onafhankelijke autoriteit kan worden gekwalificeerd zoals het Hof van Justitie vereist, toegang tot de gegevens. Bovendien kan die officier van gerechtelijke politie, in geval van hoogdringendheid, eisen dat de operator hem de metagegevens bezorgt, op voorwaarde dat de onderzoeksrechter dat later controleert. Het Hof van Justitie legt in die hypothese echter een voorafgaande rechterlijke toetsing op.

A.19.5. De verzoekende partij voegt eraan toe dat de wet van 20 juli 2022 niet erin voorziet dat een persoon op de hoogte wordt gebracht van de verwerking van gegevens eens de beperking van de verwerking niet meer verantwoord is ten aanzien van de nagestreefde doelstelling, hetgeen het geval is wanneer die informatie het door de autoriteiten gevoerde onderzoek niet in gevaar kan brengen, in tegenstelling tot hetgeen door het Hof van Justitie wordt vereist. In geval van twijfel hierover dient een prejudiciële vraag te worden gesteld aan dat rechtscollege om te bepalen of artikel 15, lid 1, van de richtlijn 2002/58/EG, in samenhang gelezen met de artikelen 7, 8, 47 en 52, lid 1, van het Handvest en de artikelen 13 en 54 van de richtlijn (EU) 2016/680, een dergelijke voorlichting oplegt.

De verzoekende partij stelt overigens vast dat de wet van 20 juli 2022 ook niet voorziet in een effectieve bescherming tegen risico's van misbruik en onrechtmatige toegang tot de gegevens voor de betrokken personen. In het geval waarin de autoriteiten toegang hebben tot de gegevens maar van mening zijn dat het niet noodzakelijk is om strafvervolgingen in te stellen, kan de persoon de wettigheid van de onderzoeksmaatregel immers niet betwisten, tenzij door een rechtsvordering inzake burgerlijke aansprakelijkheid voor de rechtbank van eerste aanleg in te stellen, hetgeen een weinig waarschijnlijke hypothese is en geen daadwerkelijk rechtsmiddel biedt. Vervolgens, in het geval waarin de betrokken persoon de wettigheid betwist van de onderzoeksmaatregel in het kader van een strafprocedure tijdens welke die persoon voor een rechter moet verschijnen, kan de betrokken maatregel niet noodzakelijk uit de debatten worden geweerd en kan er geen rekening mee worden gehouden in de beoordeling van de straf, gelet op artikel 32 van de voorafgaande titel van het Wetboek van strafvordering. Bovendien bieden de door de Ministerraad genoemde organen en autoriteiten ook geen mogelijkheid tot jurisdictioneel beroep aan de betrokken personen, aangezien het onafhankelijke bestuurlijke autoriteiten betreft.

Bijgevolg schendt de wet van 20 juli 2022 de in het middel genoemde bepalingen in zoverre zij niet erin voorziet dat de personen ervan op de hoogte worden gebracht dat de bevoegde nationale autoriteiten toegang hebben gehad tot hun gegevens, noch dat die personen over een rechtsmiddel tegen een onwettige toegang tot gegevens beschikken.

A.20. Wat betreft de versleuteling van de communicatie, merkt de verzoekende partij op dat artikel 3 van de wet van 20 juli 2022 bepaalt dat de operatoren, door gebruik te maken van een versleutelingssysteem, de uitvoering van een gericht verzoek tot toegang tot gegevens niet mogen verhinderen, enerzijds, en dat het gebruik van versleuteling door een buitenlandse operator niet tot gevolg mag hebben dat de operatoren wordt verhinderd om gegevens te bewaren wanneer een persoon een buitenlandse simkaart gebruikt op het Belgische grondgebied. Volgens de verzoekende partij is die maatregel kennelijk onevenredig. De versleutelingsmaatregelen laten immers toe de bescherming van de persoonsgegevens te waarborgen en dus bij te dragen aan de bescherming van het recht op eerbiediging van het privéleven. Verschillende instrumenten van het internationaal recht pleiten overigens voor de versleuteling van gegevens om de veiligheid van de stromen en de bescherming van de persoonsgegevens te waarborgen.

A.21. Ten slotte, wat betreft de gevolgen van de vernietiging van de wet van 20 juli 2022, voert de verzoekende partij aan dat de verwerking, in het kader van een strafrechtelijk onderzoek, van gegevens die in strijd met de richtlijn 2002/58/EG en met de artikelen 7 en 8 van het Handvest zijn verzameld, schade vormt die op effectieve wijze moet kunnen worden hersteld door een beoordeling en een weging van de informatie en van de bewijselementen, of zelfs door het illegale karakter ervan in aanmerking te nemen in het kader van de strafbepaling, zoals de rechtspraak van het Hof van Justitie vereist. De wet van 20 juli 2022 voorziet echter niet in dergelijke waarborgen.

Het Hof zou op zijn minst moeten preciseren dat het aan de strafrechter staat om vast te stellen dat de bewijselementen die in strijd met de van de richtlijn 2002/58/EG en met de artikelen 7 en 8 van het Handvest zijn verzameld en die niet uit de debatten kunnen worden geweerd, in elk geval in aanmerking moeten worden genomen, gelet op het onwettige karakter ervan, in het kader van de strafbepaling. De verzoekende partij voert aan dat het Hof wel degelijk bevoegd is in dat kader, op een wijze die vergelijkbaar is met hetgeen het Hof van Justitie in meerdere van zijn arresten doet.

In geval van twijfel hieromtrent dient een prejudiciële vraag te worden gesteld aan het Hof van Justitie om te bepalen, enerzijds, of het toegestaan is dat schendingen van het recht van de Europese Unie, in het bijzonder van de richtlijn 2002/58/EG alsook van de artikelen 7 en 8 van het Handvest, die de bewijsgaring in een nationale strafprocedure aantasten, zonder gevolg kunnen blijven, zelfs in geval van een zwaar strafbaar feit, en, anderzijds, of de voormelde schendingen ten gunste van de vervolgde persoon in aanmerking dienen te worden genomen, ten minste in het stadium van de beoordeling van het bewijs of van de strafbepaling.

Zaak nr. 7932

A.22. De verzoekende partijen leiden een eerste middel af uit de schending van de artikelen 10, 11, 13, 15, 22, 23 en 29 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 5, 6, 8, 9, 10, 11, 14 en 18 van het Europees Verdrag voor de rechten van de mens, met de artikelen 7, 8, 11, 47 en 52 van het Handvest, met artikel 5, lid 4, van het Verdrag betreffende de Europese Unie, alsook met artikel 6 van de richtlijn 2002/58/EG, met de richtlijn (EU) 2016/680 en met de AVG. Dat middel heeft betrekking op de verzameling en de bewaring van verkeers- en locatiegegevens.

A.23.1. In een eerste onderdeel voeren de verzoekende partijen aan dat de artikelen 4 en 5 van de wet van 20 juli 2022 voorzien in een algemene bewaring van gegevens die niet voldoet aan de vereisten van het recht van de Europese Unie.

A.23.2. Inzonderheid voorziet artikel 5 van de wet van 20 juli 2022 met name in de verplichting voor een operator om verkeers- en locatiegegevens gedurende vier maanden te bewaren teneinde eventuele fraude of kwaadwillig gebruik van het netwerk of van de dienst te kunnen vaststellen. Een dergelijke verwerking vormt een algemene en ongedifferentieerde bewaring van verkeersgegevens en leeft de vereisten van artikel 6 van de richtlijn 2002/58/EG niet na. Uit de vaste rechtspraak van het Hof van Justitie blijkt ook dat een dergelijke algemene en ongedifferentieerde bewaring van gegevens slechts toelaatbaar is in het kader van de bescherming van de nationale veiligheid. Fraude of kwaadwillig gebruik van het netwerk zijn fenomenen die absoluut niet aan die vereiste

voldoen. De voorziene verplichting tot bewaring valt dus kennelijk niet onder de in artikel 15, lid 1, van de richtlijn 2002/58/EG bedoelde uitzondering.

De verzoekende partijen merken op dat artikel 5 van de wet van 20 juli 2022 bovendien voorziet in de verplichting voor een operator om gedurende twaalf maanden het telefoonnummer of het IP-adres toegewezen aan de bron van de binnenkomende communicatie, de tijdstempel en de gebruikte poort, alsook de precieze datums en tijdstippen van het begin en einde van de communicatie te bewaren, om fraude of kwaadwillig gebruik van het netwerk of de dienst te kunnen vaststellen. Het betreft een verplichting tot bewaring die in strijd is met artikel 6 van de richtlijn 2002/58/EG en die een schending van de grondrechten veroorzaakt.

Bovendien voorziet artikel 5 van de wet van 20 juli 2022 in de mogelijkheid voor de operatoren om de verkeersgegevens te bewaren die nodig zijn om de veiligheid en correcte werking van hun netwerk of dienst te waarborgen, maar ook om een mogelijke of werkelijke aanslag op het netwerk op te sporen en te analyseren. De maximale bewaartermijn bedraagt twaalf maanden, maar in geval van een specifieke schending van de veiligheid, kunnen de gegevens zelfs langer worden bewaard. Volgens de verzoekende partijen betreft het een daadwerkelijk recht op bewaring dat in strijd is met artikel 6 van de richtlijn 2002/58/EG, dat vereist dat de verkeersgegevens worden gewist of anoniem worden gemaakt wanneer zij niet langer nodig zijn voor het doel van de transmissie. De bij artikel 15, lid 1, van die richtlijn bepaalde uitzondering is ook niet van toepassing, tenzij het zou gaan om zware criminaliteit of om een kwestie van nationale veiligheid. De wet past niettemin een veel ruimere definitie toe, die niet overeenstemt met het Europese toepassingsgebied.

A.23.3. Volgens de verzoekende partijen veroorzaakt de ongedifferentieerde bewaring van de voormelde gegevens, met schending van het recht van de Europese Unie, een schending van het gelijkheidsbeginsel. De gegevens van de verzoekende partijen worden immers op dezelfde wijze verwerkt als de gegevens die het voorwerp uitmaken van een strafrechtelijk onderzoek naar zware strafbare feiten, terwijl niets erop wijst dat de verzoekende partijen zich in eenzelfde situatie bevinden. Uit de rechtspraak van het Hof van Justitie blijkt dat ook het recht op eerbiediging van het privéleven in het gedrang komt.

A.24. In een tweede onderdeel voeren de verzoekende partijen aan dat de bewaring waarin artikel 6 van de wet van 20 juli 2022 voorziet, wat betreft de locatiegegevens voor de strijd tegen fraude en kwaadwillig gebruik van het netwerk, niet in overeenstemming is met het recht van de Europese Unie en met de grondrechten. De verzoekende partijen merken op dat artikel 6 van de wet van 20 juli 2022 de bewaring toelaat van andere locatiegegevens dan de verkeersgegevens. De bewaartermijn bedraagt twaalf maanden voor de goede werking en de veiligheid van het netwerk en vier maanden om fraude of kwaadwillig gebruik van het netwerk op te sporen. Artikel 9 van de richtlijn 2002/58/EG sluit een dergelijke verwerking echter uitdrukkelijk uit.

A.25.1. Het derde onderdeel heeft betrekking op de bewaring in specifieke geografische zones, bepaald bij de artikelen 9, 10 en 11 van de wet van 20 juli 2022. De verzoekende partijen merken allereerst op dat de bewaring in de andere zones dan de specifieke geografische zones niet nodig is. In dat opzicht voeren zij aan dat, hoewel uitdrukkelijk wordt aangegeven dat de gegevens worden bewaard omwille van de vrijwaring van de nationale veiligheid, de strijd tegen zware criminaliteit, de preventie van ernstige bedreigingen van de openbare veiligheid en de bescherming van de vitale belangen van een natuurlijk persoon, zodat het erop lijkt dat de vereisten van het Hof van Justitie formeel worden nageleefd, uit de concrete toepassing van dat systeem evenwel volgt dat zulks *de facto* een ongedifferentieerde bewaring van gegevens met zich meebrengt. De verzoekende partijen voeren bovendien aan dat de wet van 20 juli 2022 niet toelaat een onderscheid te maken tussen de verschillende doelstellingen en de hiërarchie ertussen niet naleeft wanneer zij de toegang tot gegevens regelt, in tegenstelling tot hetgeen het Hof van Justitie vereist. De gegevens die, bijvoorbeeld, worden bewaard omwille van de vrijwaring van de nationale veiligheid, kunnen niet worden gebruikt voor het onderzoek naar zware strafbare feiten en de strijd daartegen. De bevoegde autoriteiten inzake strafrechtelijke onderzoeken mogen dus geen toegang hebben tot de gegevens indien het gaat om een algemene en ongedifferentieerde bewaring. Bijgevolg is de wet van 20 juli 2022 onvoldoende voorzienbaar en schendt zij de in het middel genoemde richtlijnen.

Bovendien is de bewaringstermijn in principe vastgelegd op twaalf maanden, tenzij een kortere termijn wordt vastgesteld. Die standaardtermijn is onevenredig en overschrijdt de strikt noodzakelijke termijn. Voor het overige, in plaats van standaard een korte termijn te hanteren en de langere termijnen te beperken tot uitzonderlijke omstandigheden met een ernstige motivering, wordt ervoor gekozen standaard van de langst mogelijke termijn gebruik te maken, zodat het evenredigheidsbeginsel wordt geschonden. De gegevens dienen te worden bewaard wat betreft de communicatie zowel vanuit de bepaalde geografische zone als naar die zone. Bijgevolg worden de locatiegegevens van een eindgebruiker die communiceert met een eindgebruiker in een betrokken geografische zone bewaard, zelfs indien de eerste eindgebruiker zich niet in een geografische zone bevindt die is onderworpen

aan een verplichting tot bewaring. Een dergelijke verplichting, buiten de betrokken geografische zone, is niet strikt noodzakelijk. Ten slotte is de beschrijving van de verschillende geografische zones in artikel 11 van de wet van 20 juli 2022 extreem ruim en omvat zij zones die niet aan een verplichting tot bewaring hoeven te worden onderworpen, zodat die bewaring *de facto* ongedifferentieerd is, hetgeen niet in overeenstemming is met de vereisten van het Hof van Justitie, noch met het evenredigheidsbeginsel.

A.25.2. Wat betreft de bewaring van gegevens in de gerechtelijke arrondissementen en in de politiezones, bepaald bij artikel 11 van de wet van 20 juli 2022, merken de verzoekende partijen op dat een verplichting tot bewaring wordt opgelegd zodra een bepaald aantal strafbare feiten wordt overschreden. De in dat kader gebruikte statistieken reflecteren de criminaliteit evenwel niet op betrouwbare wijze, aangezien zij niet alleen veroordelingen of vastgestelde feiten betreffen, maar ook elke registratie van een feit dat eenzijdig door de politie wordt gecatalogeerd als potentieel strafbaar feit. Volgens de verzoekende partijen zouden die statistieken systematisch tot een overschatting van het werkelijke aantal strafbare feiten kunnen leiden, wegens dubbele registraties of wegens geregistreerde feiten die geen strafbare feiten zijn maar die toch als zodanig worden gecatalogeerd. Bovendien heeft de in aanmerking genomen drempel voor het aantal strafbare feiten tot gevolg dat zo goed als het volledige grondgebied aan de verplichting tot bewaring is onderworpen, zoals blijkt uit een analyse uitgevoerd op basis van de criminaliteitsstatistieken voor het kalenderjaar 2021. Bijgevolg heeft de wet van 20 juli 2022 tot gevolg dat een verplichting tot algemene en ongedifferentieerde bewaring van gegevens wordt ingevoerd. In werkelijkheid leidt het gecombineerde criterium van de statistieken op het niveau van het gerechtelijke arrondissement en van de politiezone slechts in uitzonderlijke gevallen niet tot een verplichting tot bewaring. Bovendien is de maatregel permanent van kracht. De door het Hof van Justitie vastgelegde voorwaarden voor een dergelijke verplichting tot bewaring, die slechts toelaatbaar is omwille van de nationale veiligheid, voor een beperkte duur en in concrete omstandigheden, worden dus niet nageleefd.

Voor het overige blijkt de keuze om de gerechtelijke arrondissementen aan te wijzen als geografische zones, volgens de verzoekende partijen onevenredig, aangezien het gaat om een zone met een grote omvang en de cijfers inzake criminaliteit voor het volledige arrondissement niet noodzakelijk representatief zijn voor de verschillende delen van de zone. Het gebruik van de gerechtelijke arrondissementen veroorzaakt dus een onevenredige verplichting tot bewaring, die niet strikt noodzakelijk is. Op dezelfde wijze is de vastgestelde bewaringstermijn bijzonder lang en geeft die aanleiding tot de bewaring van een enorme hoeveelheid gegevens, van extreem gevoelige aard en met betrekking tot tal van personen. Die termijn is dus onevenredig en niet strikt noodzakelijk, zodat hij de artikelen 10, 11 en 22 van de Grondwet, alsook de bij analoge bepalingen gewaarborgde grondrechten schendt.

A.26.1. De verzoekende partijen voeren aan dat de bepaling van de geografische zones waarvan het dreigingsniveau ten minste niveau 3 bedraagt, bedoeld in artikel 11 van de wet van 20 juli 2022, geen wettelijke basis heeft aangezien de dreigingsniveaus enkel bij koninklijk besluit en niet in een formele wet zijn gedefinieerd. Bijgevolg is niet voldaan aan de vereiste van artikel 22 van de Grondwet. Bovendien vereist het beginsel van voorzienbaarheid dat de burger, op basis van de bewoordingen van de wet, de betekenis van de dreigingsniveaus kan bepalen, wegens de gevolgen ervan voor de verplichte bewaring van zijn persoonsgegevens. Bovendien laat het Hof van Justitie een verplichting tot algemene en ongedifferentieerde bewaring wat betreft de nationale veiligheid toe in geval van een werkelijke, actuele of voorzienbare ernstige bedreiging. Het niveau 3 beantwoordt niet aan die vereiste, aangezien de bedreiging die het beoogt slechts mogelijk en waarschijnlijk moet zijn, en niet ernstig en werkelijk.

A.26.2. Volgens de verzoekende partijen voorziet de wet van 20 juli 2022 in geen enkele verwijdering van gegevens in geval van een daling van het dreigingsniveau in een specifieke zone of over het volledige grondgebied, noch in nadere regels omtrent de kennisgeving aan de burger op wie de bewaring van gegevens betrekking heeft, noch in de mogelijkheid om tegen die bewaring een beroep in te stellen, zoals het Hof van Justitie nochtans vereist. Bijgevolg schendt de wet van 20 juli 2022 de artikelen 10, 11 en 13 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 5, 6, 8, 9, 10, 11, 14, 15, 17 en 18 van het Europees Verdrag voor de rechten van de mens.

A.26.3. Wat betreft de specifieke geografische zones beoogd in artikel 11 van de wet van 20 juli 2022, merken de verzoekende partijen op dat de grenzen ervan niet worden gepreciseerd, maar dat het aan de Koning staat om de omvang ervan te bepalen. De verplichting tot bewaring is dus niet strikt noodzakelijk en leeft het in artikel 22 van de Grondwet vervatte wettigheidsbeginsel niet na. In dat opzicht dient te worden gepreciseerd dat artikel 9 van de wet van 20 juli 2022 reeds een uitbreiding van de betrokken zone toelaat. Volgens de verzoekende partijen is de grens van een zone overbodig wat betreft de vaste internetverbindingen, waarvan de locatie met precisie gekend is, zodat de maatregel onevenredig is ten aanzien daarvan. Bovendien is de duur van de bewaring van de gegevens onbepaald voor de meeste betrokken zones, hetgeen niet in overeenstemming is met de

rechtspraak van het Hof van Justitie, dat eist dat de maatregelen niet langer duren dan wat absoluut noodzakelijk is in het licht van de nagestreefde doelstelling en van de omstandigheden die de maatregelen verantwoorden. In dat opzicht voorziet de wet van 20 juli 2022 niet in een evaluatie van het noodzakelijke karakter van het systeem. De maatregelen tot permanente bewaring die die wet creëert, zijn onevenredig.

De verzoekende partijen voeren bovendien aan dat een verplichting tot algemene en ongedifferentieerde bewaring blijkt uit de definitie van de specifieke geografische zones, die tot gevolg heeft dat volledige grondgebieden van gemeenten zijn onderworpen aan een permante verplichting tot bewaring. Artikel 11 van de wet van 20 juli 2022 beoogt ook de datacentra en clouddiensten, hetgeen niet alleen gevolgen heeft voor de bezoekers van die infrastructuren maar ook voor de onlinegebruikers ervan en voor de derden aan wie die infrastructuren diensten leveren. Bijgevolg treft de verplichting tot bewaring alle gebruikers vanop afstand van die digitale diensten, zodat eenieder die een dienst gebruikt die toevallig op die servers staat, onderworpen is aan een verplichting tot algemene bewaring. Die staat niet in verhouding tot de beoogde bescherming van de infrastructuur, aangezien zij zijdelings van toepassing is op alle diensten die op afstand vanuit die infrastructuur worden aangeboden. Bovendien is een meer gerichte bescherming en verplichting mogelijk. De verzoekende partijen sommen andere geografische zones op die niet voldoen aan het criterium van strikte noodzakelijkheid wegens hun omvang. De aanwezigheid van een datacentrum heeft automatisch een verplichting tot bewaring tot gevolg die voor het gehele gebouw geldt. Volgens de verzoekende partijen vormt de bescherming van gebouwen bestemd voor rechtspersonen waarvan het economische of wetenschappelijke potentieel moet worden beschermd, evenwel een vaag criterium. Bovendien is de precieze lijst van betrokken plaatsen niet aan bekendmaking onderworpen. Ook de autosnelwegen, die een zeer ruime bewaring van gegevens met zich meebrengen van iedereen die zich er verplaatst met mobiele apparaten of die zich in de omgeving bevindt, zijn betrokken. In werkelijkheid vormt de bewaring van locatiegegevens op de autosnelwegen een permanente registratie van de verplaatsingen van alle voertuigen met een ingebouwde simkaart en laat zij toe de verplaatsingen van burgers te registreren.

A.26.4. Wat betreft de toepassing van de wet van 20 juli 2022 op de aanbieders van communicatiediensten zoals Skype of Whatsapp, die ook moeten overgaan tot de verplichte bewaring van verkeers- en locatiegegevens, merken de verzoekende partijen op dat zij niet over de locatie van de gebruiker beschikken en dat zij onmogelijk kunnen bepalen of die zich al dan niet in de betrokken geografische zone bevindt. Artikel 9 van de wet van 20 juli 2022 legt op dat in die situatie de satellietlocatie van de eindapparatuur wordt gebruikt. De « klassieke » operator van het communicatienetwerk waarmee de eindgebruiker verbindt, is echter reeds ertoe verplicht om gegevens te bewaren. Een bijkomende verplichting voor de elektronische-communicatiediensten zoals Skype of Whatsapp is dus niet noodzakelijk, noch evenredig.

A.26.5. De verzoekende partijen merken op dat de te bewaren gegevens, beoogd in artikel 10 van de wet van 20 juli 2022, een identificatie toelaten van de bron en van de bestemming, alsook van de datum en het tijdstip van de communicatie, van de aard ervan en de hoeveelheid gegevens die zijn doorgestuurd. De gegevens betreffen bovendien de locatie in het geval van mobiele communicatie, alsook de locatie op het moment van een communicatie, maar ook op elk moment dat de eindapparatuur wordt opgestart of uitgeschakeld of wanneer de operator wil nagaan welke eindapparatuur met zijn netwerk is verbonden. Die bepaling creëert met andere woorden een « volgrecht » ten aanzien van de eindgebruiker zonder dat een dergelijke maatregel noodzakelijk, noch evenredig is. Bovendien is de bewaring van verschillende gegevenselementen op zich onevenredig, aangezien die elementen niet bijdragen in de strijd tegen zware criminaliteit of de bescherming van de nationale veiligheid en aangezien de criteria dermate ruim zijn dat de gegevens op ongedifferentieerde wijze worden verzameld. Aangezien de gegevens met betrekking tot de bron en de bestemming van de communicatie reeds worden bewaard, heeft het volume van verzonden gegevens geen enkele toegevoegde waarde. Dat volume kan de inhoud van communicatie zelfs gedeeltelijk onthullen, zodat artikel 29 van de Grondwet wordt geschonden. Ten slotte is de bewaring van de grootte van de overgemaakte gegevens, die niet kan worden beschouwd als een louter verkeersgegeven, niet strikt noodzakelijk, net zomin als de bewaring van identificatiegegevens van de eindapparatuur bepaald bij artikel 10 van de wet van 20 juli 2022, aangezien andere gegevens reeds toelaten om de eindgebruiker te identificeren.

A.27. In een vierde onderdeel voeren de verzoekende partijen aan dat de gerichte verplichting tot bewaring waarin artikel 33 van de wet van 20 juli 2022 voorziet, de bij artikel 22 van de Grondwet vereiste voorzienbaarheid schendt, in zoverre de wetgever de verkeers- en locatiegegevens niet precies heeft omschreven. Er wordt gepreciseerd dat de bewaring in het belang van de uitoefening van de opdrachten van de inlichtingen- en veiligheidsdiensten is. Het Hof van Justitie vereist evenwel dat de bewaring strikt noodzakelijk is. Bovendien legt artikel 33 niet op dat het voorwerp van de bewaring enig verband met een verdachte of gevaarlijke gedraging heeft. Het onderwerpen van alle mogelijke gebruikers van bepaalde communicatiemiddelen, in grote geografische zones, aan de in artikel 33 beoogde maatregel, vormt een verplichting tot algemene en ongedifferentieerde bewaring.

Bovendien is in geen enkel rechtsmiddel, noch in de kennisgeving van de bewaring van gegevens voorzien, in tegenstelling tot hetgeen het Hof van Justitie vereist. De wetgever heeft ook niet voorzien in de voorafgaande tussenkomst van een rechter, noch in een maatregel waarbij de verzamelde gegevens in geval van onwettigheid worden verwijderd. Daaruit volgt dat een overheid onwettige elementen mag verzamelen zonder te worden bestraft, hetgeen niet ontradend is.

A.28. In een vijfde onderdeel bekritiseren de verzoekende partijen de verplichting tot algemene en ongedifferentieerde bewaring vervat in artikel 34 van de wet van 20 juli 2022. Zij merken hieromtrent op dat noch die bepaling, noch overigens artikel 33 van de wet van 20 juli 2022, het begrip « verkeers- en locatiegegevens » definieert, waarmee niet is voldaan aan het criterium van voorzienbaarheid opgelegd bij artikel 22 van de Grondwet en bij de rechtspraak van het Hof van Justitie. Bovendien, bij ontstentenis van een bevestiging bij koninklijk besluit, is in geen enkele vorm van openbaarheid voorzien om de personen te informeren die het voorwerp hebben uitgemaakt van de bij artikel 34 van de wet van 20 juli 2022 bepaalde maatregel, hetgeen hen belet op geldige wijze een rechtsmiddel in te stellen. Bijgevolg wordt de toegang tot de rechter verhinderd, terwijl die een essentieel element is in het geval van een maatregel met een dergelijke inmenging in het recht op de eerbiediging van het privéleven. De wetgever heeft ook niet gepreciseerd wat moet gebeuren met op onwettige wijze verzamelde gegevens, terwijl die volgens de vereisten van de rechtspraak van het Hof van Justitie dienen te worden gewist.

A.29. In een zesde onderdeel voeren de verzoekende partijen aan dat artikel 37 van de wet van 20 juli 2022 het begrip « verkeers- en locatiegegevens » niet definieert, hetgeen in strijd is met artikel 22 van de Grondwet en met de rechtspraak van het Hof van Justitie. De ontstentenis van een toetsing van de strikte noodzaak van de mededeling van gegevens en de ontstentenis van het noodzakelijke karakter van de raadpleging van gegevens worden ook aangeklaagd. Bijgevolg schendt artikel 37 de artikelen 10, 11 en 22 van de Grondwet.

A.30. In een zevende onderdeel wordt opgemerkt dat de wet van 20 juli 2022 in geen enkele bijzondere bepaling voorziet wat betreft de bewaring van de verkeers- en locatiegegevens van advocaten, artsen en journalisten, terwijl het om gevoelige gegevens gaat die onder het beroepsgeheim of het bronnengeheim vallen. Volgens de verzoekende partijen, gelet op de bijzondere bescherming die deze beroepsgroepen genieten, maar ook gelet op het recht op een eerlijk proces, het recht op eerbiediging van het privéleven, de vrijheid van meningsuiting en de persvrijheid, is vereist dat vanaf het niveau van de bewaring van de gegevens in afdoende waarborgen wordt voorzien om het strikt noodzakelijke karakter van de maatregel te verzekeren, hetgeen niet door de wetgever wordt gewaarborgd. Het beginsel van gelijkheid en niet-discriminatie wordt dus geschonden. Wat betreft de cliënt of de patiënt van de voormelde beroepsgroepen, vormt de wet van 20 juli 2022 een achteruitgang van de beschermingsgraad van het recht op bijstand in de zin van artikel 23 van de Grondwet en, bijgevolg, een schending van de *standstill*-verplichting die die grondwetsbepaling bevat. De wetgever heeft bovendien het vermoeden van onschuld en de rechten van verdediging geschonden, aangezien de advocaten hun cliënten zonder toezicht moeten kunnen bijstaan, alsook het recht op vrije meningsuiting, aangezien de gegevens van de contacten van journalisten worden beoogd, hetgeen het werk van de pers hindert.

A.31. Er wordt een tweede middel afgeleid uit de schending van de artikelen 10, 11, 15, 22 en 29 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 5, 6, 8, 9, 10, 11, 14 en 18 van het Europees Verdrag voor de rechten van de mens, met de artikelen 7, 8, 11, 47 en 52 van het Handvest, met artikel 5, lid 4, van het Verdrag betreffende de Europese Unie, alsook met de richtlijn 2002/58/EG, met de richtlijn (EU) 2016/680 en met de AVG.

A.32.1. In een eerste onderdeel voeren de verzoekende partijen aan dat het niet noodzakelijk is bepaalde door artikel 8 van de wet van 20 juli 2022 beoogde gegevens te bewaren tot twaalf maanden na het einde van de dienst, aangezien het gegevens betreft die overbodig zijn voor de vaststelling van de identiteit van de gebruiker als reeds andere gegevens worden bewaard. De bewaring zou minstens moeten worden beperkt tot situaties waarin geen andere gegevens voorhanden zijn. De verzoekende partijen twijfelen bovendien aan het adequate karakter van de bewaring van het IP-adres, aangezien er methodes bestaan die beletten om via dat adres terug te gaan tot de eindgebruiker. Ten slotte legt artikel 8 van de wet van 20 juli 2022 geen hiërarchie op tussen de gegevens die het beoogt, terwijl bepaalde gegevens niet nodig zijn wanneer andere reeds gekend zijn. Het is ook mogelijk dat bepaalde gegevens niet meer juist zijn, bijvoorbeeld bij een adreswijziging. Gelet op het voorgaande schendt artikel 8 van de wet van 20 juli 2022 het recht op eerbiediging van het privéleven en artikel 5, lid 1, *c)* en *d)*, van de AVG.

A.32.2. In een tweede onderdeel voeren de verzoekende partijen aan dat artikel 8 aan gratis elektronische-communicatiediensten zoals Whatsapp et Skype, bij ontstentenis van een betaling of van het gebruik van een

telefoonnummer, oplegt om het IP-adres te bewaren, niet alleen bij het intekenen of de activatie, maar ook het IP-adres aan de bron van de verbinding. Die verplichting impliceert een verzameling en permanente bewaring van de IP-adressen van de gebruiker, hetgeen leidt tot de identificatie ervan, terwijl de noodzaak van een dergelijke maatregel nergens uit blijkt aangezien de autoriteiten via de netwerkoperatoren reeds over de IP-adressen beschikken die aan de bron zijn toegewezen en, in de gevallen waarin de bewaring van verkeersgegevens is toegelaten, die IP-adressen kunnen koppelen aan de gebruikte gratis elektronische-communicatiedienst. Bovendien zien de verzoekende partijen niet in waarom die diensten aan de definitie van « operator » werden toegevoegd, terwijl tal van andere onlinediensten niet erin zijn opgenomen. Zij voeren aan dat het criterium om te bepalen wie een operator is, niet duidelijk is, zodat het gelijkheidsbeginsel, in samenhang gelezen met het wettigheidsbeginsel, is geschonden.

A.32.3. In een derde onderdeel voeren de verzoekende partijen aan dat artikel 12 van de wet van 20 juli 2022 het gebruik van gezichtsherkenningstechnologie toelaat, hetgeen een zeer ingrijpende maatregel is die bijzondere risico's met zich meebrengt, gelet op de gevoeligheid van de betrokken gegevens. Er bestaan evenwel andere oplossingen, toegelaten bij de wet van 20 juli 2022, zoals het gebruik van de elektronische identiteitskaart met pincode. Bovendien is het niet realistisch dat er in de context van een verkooppunt sprake is van een uitdrukkelijke en geïnformeerde toestemming van de gebruiker, zoals door de AVG is vereist. De wet van 20 juli 2022 voorziet ook niet in een schriftelijke toestemming. Een louter mondelinge toestemming volstaat te dezen nochtans niet. Volgens de verzoekende partijen schendt de wet van 20 juli 2022 bijgevolg artikel 22 van de Grondwet en de in het middel vermelde bepalingen van het recht van de Europese Unie.

A.32.4. Het vierde onderdeel heeft betrekking op in voertuigen ingebouwde simkaarten. Volgens de verzoekende partijen zorgt artikel 12 van de wet van 20 juli 2022, in zoverre het voorziet in de verplichte bewaring van het chassisnummer indien een simkaart in het voertuig is ingebouwd, bij wijze van alternatief voor de andere identificatiemethoden, voor de permanente tracking van een voertuig via de internetverbinding, aangezien de eindgebruiker van het voertuig weinig controle heeft over de simkaart en over die internetverbinding. Echter, uit niets blijkt dat die identificatie van het voertuig noodzakelijk is. In combinatie met de verplichte bewaring van de locatiegegevens op de autosnelwegen, is de maatregel onevenredig.

A.32.5. In een vijfde onderdeel voeren de verzoekende partijen aan dat artikel 8 van de wet van 20 juli 2022, in zoverre het voorziet in de bewaring van het aan de bron toegewezen IP-adres en van de identificatiegegevens van de eindapparatuur voor een termijn van twaalf of zes maanden, onevenredig is. Bovendien is het gebruik van de gegevens niet beperkt tot de door het Hof van Justitie bepaalde doeleinden, namelijk de bescherming van de nationale veiligheid, de voorkoming van ernstige bedreigingen van de openbare veiligheid en de strijd tegen zware criminaliteit, terwijl dat een essentiële voorwaarde is. Bovendien is de bewaring van de voormelde gegevens niet strikt noodzakelijk, aangezien andere gegevens reeds toelaten de eindgebruiker te identificeren.

A.32.6. Het zesde onderdeel heeft betrekking op het vermoeden van onschuld. De verzoekende partijen voeren aan dat artikel 12 van de wet van 20 juli 2022 het vermoeden invoert dat een elektronische-communicatiedienst wordt gebruikt door de geïdentificeerde persoon, hetgeen algemeen geldt, ook in het kader van het strafonderzoek en van het strafrecht. Volgens hen is dat vermoeden bijzonder problematisch in een situatie waarin reeds redelijke twijfel bestaat over de werkelijke gebruiker van een elektronische-communicatiedienst, hetgeen courant is. In werkelijkheid heeft die maatregel tot gevolg dat de vermoede eindgebruiker een negatief bewijs moet leveren, namelijk dat hij niet de persoon is die de datatransmissie heeft uitgevoerd, wat volstrekt onrealistisch is. Bijgevolg wordt de eindgebruiker in werkelijkheid geconfronteerd met de onmogelijkheid een tegenbewijs te leveren, hetgeen het recht op het vermoeden van onschuld en op een eerlijk proces schendt.

De verzoekende partijen voegen eraan toe dat, in tegenstelling tot hetgeen de Ministerraad aanvoert, het feit dat de wetgever de identificatie van de abonnee wil vergemakkelijken door de ontvangst van een sms van de operator bij gebruik van een vaste internettoegangsdienst, irrelevant is voor de situaties waarin de operator niet zelf tussenkomt in het verstrekken van de internetdienst, bijvoorbeeld in een café of een restaurant.

A.33. De verzoekende partijen leiden een derde middel af uit de schending van de artikelen 10, 11, 15, 22 en 29 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 5, 6, 8, 9, 10, 11, 14 en 18 van het Europees Verdrag voor de rechten van de mens, met de artikelen 7, 8, 11, 47 en 52 van het Handvest, met artikel 5, lid 4, van het Verdrag betreffende de Europese Unie, alsook met de richtlijn 2002/58/EG, met de richtlijn (EU) 2016/680 en met de AVG.

A.34.1. In een eerste onderdeel voeren de verzoekende partijen aan dat artikel 13 van de wet van 20 juli 2022 de rechtspraak van het Hof van Justitie van de Europese Unie, volgens welke een strikte hiërarchie tussen de

doeleinden bestaat, met dien verstande dat de gegevens die zijn verzameld voor de bescherming van de nationale veiligheid niet mogen worden gebruikt voor de strijd tegen zware criminaliteit, niet naleeft. De wet van 20 juli 2022 voorziet immers niet in een compartimentering van de gegevens bij de bewaring op grond van het nagestreefde doel en maakt dergelijk onderscheid ook niet bij de toegang tot die gegevens, zodat artikel 13 kennelijk in strijd is met de in het middel vermelde bepalingen.

A.34.2. De verzoekende partijen voegen eraan toe dat de definitie van « zware criminaliteit » opgenomen in artikel 13 van de wet van 20 juli 2022 te ruim is en het strikt noodzakelijke overstijgt, terwijl die definitie een impact heeft op de mogelijkheid om toegang te hebben tot de bewaarde verkeers- en locatiegegevens.

A.34.3. Overigens merken de verzoekende partijen op dat de artikelen 5 en 6 van de wet van 20 juli 2022 een verplichting tot algemene en ongedifferentieerde bewaring invoeren waarbij bepaalde autoriteiten toegang wordt verleend « in het kader van hun opdracht ». Die verplichting is in te vage en te ruime termen afgebakend. In dat opzicht laat artikel 13 van de wet een toegang voor andere doeleinden toe dan die welke door het Hof van Justitie zijn aanvaard, namelijk de opsporing van en de strijd tegen fraude en kwaadwillig gebruik van het netwerk of de dienst. Het beginsel van voorzienbaarheid wordt geschonden, aangezien toegang mogelijk is voor met name de voorkoming van ernstige bedreigingen van de openbare veiligheid, het vrijwaren van vitale belangen van natuurlijke personen en de preventie, het onderzoek, de opsporing of de vervolging van een feit dat onder zware criminaliteit valt. In dat kader zijn de bevoegdheden van de beoogde autoriteiten niet afgebakend, zodat hun bevoegdheid relatief ruim blijkt.

De verzoekende partijen voeren aan dat de lijst van autoriteiten die toegang kunnen krijgen tot de krachtens de artikelen 8 en 12 van de wet van 20 juli 2022 bewaarde gegevens, bepaald bij artikel 13 van die wet, bijzonder lang is en entiteiten omvat die bevoegd zijn voor de opsporing van strafrechtelijke inbreuken die geen zware criminaliteit uitmaken, in tegenstelling tot hetgeen door het Hof van Justitie wordt vereist. Bijgevolg worden de in het middel vermelde bepalingen geschonden.

A.34.4. Wat betreft de autoriteiten die toegang kunnen krijgen tot de verkeers- en locatiegegevens die bewaard zijn krachtens de artikelen 9 en 11 van de wet van 20 juli 2022, bepaald bij artikel 13 van die wet, merken de verzoekende partijen op dat geen rekening wordt gehouden met de door het Hof van Justitie vereiste hiërarchie tussen de doeleinden, zodat de gegevens kunnen worden gebruikt voor een doeleinde van een lager belang dan het doeleinde dat de bewaring toeliet, hetgeen in strijd blijkt met de bepalingen van het recht van de Europese Unie in het middel, alsook met het recht op eerbiediging van het privéleven.

A.35. In het tweede onderdeel voeren de verzoekende partijen aan dat de grieven gericht tegen artikel 13 van de wet van 20 juli 2022 ook gelden voor de specifieke nadere regels voor de toegang tot de gegevens waarin op basis van die bepaling is voorzien, opgesomd in de hoofdstukken 3 tot 10 van die wet. Die regels zijn immers te ruim en voorzien niet in de nodige procedurele waarborgen, zoals een onafhankelijke toetsing bij de toegang tot gevoelige gegevens zoals de aan de bron toegewezen IP-adressen. Slechts in bepaalde gevallen is voorzien in de tussenkomst van een onderzoeksrechter of van een onafhankelijk bestuurlijk orgaan wat betreft de toegang tot verkeers- en locatiegegevens. Bijgevolg zijn de in de artikelen 21, 24, 26, 27, 28, 33, 34, 35, 37, 40, 41, 42 en 44 van de wet van 20 juli 2022 bepaalde specifieke toegangsregelingen in strijd met de in het middel vermelde bepalingen van het recht van de Europese Unie, met het recht op eerbiediging van het privéleven en met het recht op toegang tot een rechter, in zoverre zij niet voldoen aan het beginsel van voorzienbaarheid en het wettigheidsbeginsel.

A.36. Het derde onderdeel is in het bijzonder gewijd aan de toegang tot gegevens van advocaten, artsen en journalisten. De verzoekende partijen voeren aan dat, behalve in het kader van artikel 27 van de wet van 20 juli 2022, geen specifieke bescherming bestaat voor die beroepen, zelfs in het geval waarin die wet voorziet in een tussenkomst van een onderzoeksrechter. Daaruit volgt een schending van het gelijkheidsbeginsel, gelet op de bijzondere aard van die beroepsgroepen. De gegevens die onder het beroepsgeheim of onder het journalistieke bronnengeheim vallen, worden immers op exact dezelfde wijze behandeld als die van andere personen. Gelet op de bijzondere bescherming die die beroepsgroepen genieten in het licht van het recht op een eerlijk proces, het recht op eerbiediging van het privéleven, de vrijheid van meningsuiting en de persvrijheid, dient te worden voorzien in afdoende waarborgen opdat de toegang strikt noodzakelijk is. Bovendien worden de gegevens van die beroepsgroepen anders behandeld naargelang de toegang al dan niet wordt verkregen op grond van artikel 27 van de wet van 20 juli 2022, hetgeen eveneens een schending van het gelijkheidsbeginsel is. Voor het overige preciseren de verzoekende partijen dat de uiteenzettingen met betrekking tot de gegevens van advocaten, artsen en journalisten in het zevende onderdeel van het eerste middel *mutatis mutandis* gelden in het kader van het derde onderdeel van het derde middel, wat betreft de toegang tot de gegevens.

A.37. Het vierde middel is afgeleid uit de schending van de artikelen 10, 11, 13 en 22 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 5, 6, 8, 9, 10, 11, 14 en 18 van het Europees Verdrag voor de rechten van de mens, met de artikelen 7, 8, 11, 47 en 52 van het Handvest, met artikel 5, lid 4, van het Verdrag betreffende de Europese Unie, alsook met de richtlijn 2002/58/EG, met de richtlijn (EU) 2016/680 en met de AVG. Volgens de verzoekende partijen moet het interne recht, met toepassing van de richtlijn (EU) 2016/680 en van de rechtspraak van het Hof van Justitie, voorzien in een kennisgeving aan de gebruiker van wie de verkeers- en locatiegegevens werden geraadpleegd door de met strafrechtelijke onderzoeken belaste autoriteiten. De wet van 20 juli 2022 voorziet niet in een dergelijke kennisgeving en maakt het instellen van een effectief rechtsmiddel bijgevolg illusoir. Artikel 13 van de Grondwet en de artikelen 6 en 13 van het Europees Verdrag voor de rechten van de mens worden dus geschonden.

Bovendien wordt ook het beginsel van gelijkheid en niet-discriminatie geschonden aangezien een persoon die het voorwerp uitmaakt van andere maatregelen die de grondrechten schenden, weet dat hij daarvan het voorwerp uitmaakt en dus ertegen kan optreden.

Voor het overige merken de verzoekende partijen op dat de wet van 20 juli 2022 ook buiten de context van het strafrechtelijk onderzoek niet in een kennisgeving voorziet, enerzijds, en dat wat betreft tal van bij die wet bepaalde inzageregelingen, niet erin is voorzien dat er een onafhankelijk toezicht is op de inzage, anderzijds. De wet van 20 juli 2022 schendt dus het recht op toegang tot de rechter en de mogelijkheid een effectief rechtsmiddel aan te wenden.

A.38. De verzoekende partijen leiden een vijfde middel af uit de schending van de artikelen 10, 11, 15, 22 en 29 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 5, 6, 8, 9, 10, 11, 14, 15, 17 en 18 van het Europees Verdrag voor de rechten van de mens, met de artikelen 7, 8, 11, 47 en 52 van het Handvest, met artikel 15, lid 4, van het Verdrag betreffende de Europese Unie, alsook met de richtlijn 2002/58/EG, met de richtlijn (EU) 2016/680 en met de AVG. Zij voeren aan dat het bij artikel 3 van de wet van 20 juli 2022 bepaalde verbod voor de operatoren om gebruik te maken van versleuteling indien die de identificatie van de eindgebruikers of de opsporing of lokalisatie van communicatie verhindert, een onevenredige inmenging vormt in het recht op eerbiediging van het privéleven van de betrokkenen en verder gaat dan wat nodig is in een democratische samenleving. Een dergelijk verbod is niet nodig en de bevoegde autoriteiten beschikken over tal van andere mogelijkheden om communicatie op te sporen en gebruikers te identificeren, die minder drastisch zijn dan een algemeen verbod voor de operator. Het verbod op versleuteling maakt de gegevens toegankelijk, terwijl een versleuteld gegeven niet per definitie een illegaal gegeven is. Zo worden gegevens waarmee de overheid niets te maken heeft ook toegankelijk. Een dergelijk verbod heeft ook gevolgen voor alle gebruikers van de operator, aangezien die zal moeten opteren voor een zwakkere beveiligingstechnologie om te kunnen voldoen aan de verzoeken van de bevoegde autoriteiten.

A.39. Ten slotte leiden de verzoekende partijen een zesde middel af uit de schending van de artikelen 10, 11, 22 en 29 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 5, 6, 8, 9, 10, 11, 14, 15, 17 en 18 van het Europees Verdrag voor de rechten van de mens, met de artikelen 7, 8, 11, 47 en 52 van het Handvest en met de richtlijn 2002/58/EG. Zij voeren aan dat de bij artikel 4, § 2, van de wet van 20 juli 2022 bepaalde maatregelen kunnen worden ingezet voor doeleinden die de loutere goede werking van de elektronische-communicatiediensten overschrijden, met name omwille van censuur. De wetgever heeft evenwel in geen enkele beoordeling door een onafhankelijk orgaan, noch in heldere beoordelingscriteria voorzien. In werkelijkheid wordt het volledig aan de operator gelaten om te beoordelen of is voldaan aan de definitie van « fraude » of « kwaadwillig gebruik van het netwerk of van de dienst » en om de gepastheid en de evenredigheid van een maatregel te beoordelen. De definitie van « kwaadwillig gebruik van het netwerk of van de dienst » is bovendien veel te ruim, aangezien zij elk gebruik van een elektronische-communicatienetwerk of -dienst om « schade te berokkenen » omvat. Een dergelijke definitie zet de deur open voor censuur en laat toe om, zonder rechterlijke controle, schadelijk geachte meningen te blokkeren. Bijgevolg schendt artikel 4 van de wet van 20 juli 2022 de vrijheid van meningsuiting en van informatie.

Wat betreft het standpunt van de Ministerraad

Zaak nr. 7907

A.40.1. Wat betreft het eerste en het tweede onderdeel van het enige middel, voert de Ministerraad aan dat artikel 27, 2°, van de wet van 20 juli 2022 de inmenging in het beroepsgeheim van de advocaten drastisch beperkt.

Hij preciseert dat de door die bepaling beoogde maatregel bestaat in de toegang, bevolen door de onderzoeksrechter, tot metagegevens met betrekking tot het elektronische-communicatiemiddel van een advocaat of van een arts. Die maatregel kan slechts worden uitgevoerd indien de advocaat of de arts zelf ervan wordt verdacht een in artikel 88*bis*, § 1, van het Wetboek van strafvordering beoogd ernstig strafbaar feit te hebben gepleegd of eraan te hebben deelgenomen, of indien precieze feiten doen vermoeden dat derden die ervan worden verdacht een dergelijk strafbaar feit te hebben gepleegd, gebruikmaken van het betrokken communicatiemiddel. Wat de advocaten betreft, wordt de stafhouder systematisch van de maatregel op de hoogte gebracht. De Ministerraad voegt eraan toe dat artikel 27, 2°, van de wet van 20 juli 2022 geen enkele actieve medewerking van de advocaat veronderstelt en geen betrekking heeft op de inhoud van de communicatie, maar enkel op de metagegevens met betrekking tot het betrokken communicatiemiddel.

Bovendien is de Ministerraad van mening dat de inmenging in het beroepsgeheim van de advocaat verantwoord is ten aanzien van precieze doelstellingen van algemeen belang die gedocumenteerd zijn in de parlementaire voorbereiding van de wet van 20 juli 2022. Daarmee wordt immers een doelstelling inzake de bescherming van de burgers mee nagestreefd, met inbegrip van de advocaten, gelet op de digitale wending die de maatschappij doormaakt, die ook voelbaar is in de ergste vormen van criminaliteit en van verstoring van de nationale veiligheid. Het betreft legitieme doelstellingen. In dat kader geeft artikel 27, 2°, van de wet van 20 juli 2022 slechts toegang tot de metagegevens in de hypothese van inbreuken waarvan wordt beschouwd dat ze onder zware criminaliteit vallen.

A.40.2. Volgens de Ministerraad is de interpretatie van artikel 27, 2°, van de wet van 20 juli 2022 door de verzoekende partij in de zaak nr. 7907 onjuist aangezien die bepaling de communicatiemiddelen van de advocaten in hun geheel beoogt, dat wil zeggen als verzender én als ontvanger van elektronische communicatie, zoals in de parlementaire voorbereiding is gepreciseerd. Bijgevolg berusten de eerste twee onderdelen van het enige middel op een onjuiste interpretatie van de bestreden bepaling en zijn zij niet gegrond. Indien er twijfel zou bestaan over de correcte interpretatie van artikel 27, 2°, van de wet van 20 juli 2022, staat het aan het Hof een interpretatie van die bepaling vast te stellen die in overeenstemming is met de in het middel vermelde bepalingen.

A.40.3. De Ministerraad voegt eraan toe dat artikel 27, 2°, van de wet van 20 juli 2022 een klassieke, adequate en evenredige vorm van een bepaling is die het beroepsgeheim van advocaten beschermt. Zij werd overigens geformuleerd op een wijze die vergelijkbaar is met andere bepalingen uit het Wetboek van strafvordering met het oog op de bescherming van het beroepsgeheim van advocaten, die overigens door het Grondwettelijk Hof werden gevalideerd, namelijk de artikelen 39*bis*, § 9, 56*bis*, § 3, en 90*octies* van dat Wetboek, die zich richten op de beroepsinstrumenten van de advocaat, zoals de communicatiemiddelen, de informaticasystemen, de lokalen of de woonplaatsen, veeleer dan op de interactie van de cliënten met die instrumenten. Zoals het bij die bepalingen vastgestelde systeem, brengt de specifieke bij artikel 27, 2°, van de wet van 20 juli 2022 bepaalde bescherming het beroepsgeheim dat is verbonden aan de metagegevens met betrekking tot andere communicatiemiddelen, bijvoorbeeld die van de cliënt, niet in het geding. In het kader van het onderzoek staat het aan de onderzoeksrechter om de verzamelde metagegevens met betrekking tot andere communicatiemiddelen te sorteren, teneinde de gegevens die door het beroepsgeheim van de advocaat zijn beschermd terzijde te schuiven.

De Ministerraad herinnert eraan dat de specifieke procedurele bescherming die *a priori* bij artikel 27, 2°, van de wet van 20 juli 2022 is ingevoerd, enkel de communicatiemiddelen van advocaten beoogt, net omdat zij krachtens artikel 458 van het Strafwetboek houder van het beroepsgeheim zijn, omdat zij een vertrouwensrelatie met hun cliënten onderhouden en omdat zij onder bij de wet georganiseerde instellingen vallen die ermee zijn belast te waken over de naleving van de beroepsdeontologie. In dat opzicht is de bij de bestreden bepaling vastgestelde verplichte tussenkomst van de stafhouder een belangrijke waarborg voor het beroepsgeheim van de advocaat.

A.40.4. De Ministerraad voegt eraan toe dat de elementen die zijn beschermd door het beroepsgeheim niet in het proces-verbaal worden opgetekend. Die elementen worden niet onmiddellijk vernietigd, maar bewaard aangezien de afweging tussen de door het beroepsgeheim beschermde belangen en de belangen die daarboven zouden kunnen staan een essentieel casuïstische analyse is, zoals blijkt uit de rechtspraak van het Hof en uit die van het Hof van Cassatie. De definitieve verwijdering van bewaarde gegevens gebeurt slechts na verloop van de verschillende bewaartermijnen die zijn ingesteld bij de wet van 20 juli 2022. Bovendien voorziet de bestreden bepaling in de systematische tussenkomst van de onderzoeksrechter, hetgeen in overeenstemming is met de rechtspraak van het Hof van Justitie.

A.41.1. Wat betreft het derde en het vierde onderdeel, is de Ministerraad allereerst van mening dat de bewaring van metagegevens met betrekking tot het communicatiemiddel van advocaten geen inmenging in het

beroepsgeheim impliceert. In werkelijkheid verwart de « Ordre des barreaux francophones et germanophones » de bewaring van metagegevens met de toegang tot die gegevens. Volgens de Ministerraad dient een onderscheid te worden gemaakt tussen de bescherming van het beroepsgeheim van de advocaat en de bescherming van het privéleven van individuen. Wat betreft het beroepsgeheim, kan enkel de toegang tot metagegevens een concrete inmenging veroorzaken, in tegenstelling tot de bewaring van gegevens, die ten aanzien van het beroepsgeheim neutraal blijkt, aangezien de gegevens worden bewaard door de operatoren, die de beroepsactiviteit van hun abonnees niet kennen. Bovendien stelt de wet van 20 juli 2022 elke ongeoorloofde toegang tot door de operatoren op grond van die wet bewaarde metagegevens strafbaar.

A.41.2. Volgens de Ministerraad zou de invoering van een preventieve filter, zoals aangehaald door de « Ordre des barreaux francophones et germanophones », onuitvoerbaar, contraproductief en mogelijk discriminerend zijn, naast het feit dat het niet aan het Hof staat zich in de plaats te stellen van de wetgever wat betreft de opportuniteit van een wetgevende maatregel, die een beleidskeuze van de wetgever is. Een dergelijk systeem zou immers technische moeilijkheden met zich meebrengen omtrent de uitvoering, die blijken uit de parlementaire voorbereiding van de wet van 20 juli 2022. De databanken van de operatoren zouden verplicht verbonden moeten zijn aan de professionele hoedanigheid van advocaten, hetgeen alle advocaten ertoe zou verplichten over een professionele telefoonlijn te beschikken. De operatoren zouden bovendien ertoe verplicht zijn hun professionele cliënten te bevragen om hun activiteiten te bepalen en om die informatie na te gaan bij de betrokken beroepsorde. Bovendien verandert de lijst van advocaten onophoudelijk wegens nieuwe toetredingen tot de balie, schrappingen en pensioneringen, hetgeen het constante bijwerken ervan zou vereisen, wat een onpraktische werklast voor de operatoren en voor de betrokken beroepsordes zou veroorzaken. Voor de IP-adressen zou een schifting bij binnenkomst onwerkzaam zijn aangezien de meerderheid ervan dynamische adressen zijn waarvan de toekenning voortdurend varieert. Andere moeilijkheden zouden zich voordoen wanneer de communicerende personen geabonneerd zijn bij verschillende operatoren, die permanent gegevens zouden moeten uitwisselen om de te bewaren gegevens te identificeren. De advocaten ingeschreven bij buitenlandse balies maar die in Brussel verblijven, zouden op hun beurt niet gedekt zijn door de filter bij binnenkomst, hetgeen een discriminatie zou creëren tussen de advocaten die zijn ingeschreven bij een Belgische balie en de andere advocaten, terwijl zij nochtans allen aan het beroepsgeheim gebonden zijn.

De Ministerraad voegt eraan toe dat die filter contraproductief zou zijn aangezien advocaten dan van meet af aan geïdentificeerd zouden moeten worden in de databanken die met toepassing van de wet zijn opgezet, waardoor systematisch conclusies zouden kunnen worden getrokken uit de metagegevens van cliënten. Ten slotte, uit juridisch oogpunt, zou dat systeem tot gevolg hebben dat de plicht verbonden aan het beroepsgeheim wordt omgevormd tot een privilege voor de advocaat alsook voor de personen die erin zouden slagen misbruik te maken van de communicatiemiddelen waarover een advocaat beschikt. De metagegevens zouden immers in elk geval gevrijwaard blijven, zelfs indien het communicatiemiddel werd gebruikt voor criminele doeleinden. In werkelijkheid kan de bewaring van metagegevens van de advocaat hem ook beschermen aangezien in een specifieke toegangsprocedure voor de metagegevens is voorzien in geval van de onrustwekkende verdwijning van een persoon waarbij er ernstige aanwijzingen bestaan dat de fysieke integriteit van die persoon in onmiddellijk gevaar is, hetgeen het geval van een advocaat kan zijn.

A.41.3. De Ministerraad voegt overigens eraan toe dat de wet van 20 juli 2022 een gerichte bewaring van metagegevens invoert, verantwoord door de nagestreefde doelstellingen en in overeenstemming met de rechtspraak van het Hof. Hoewel de bewaring van gegevens gericht is op basis van geografische criteria, is de toegang tot metagegevens immers strikt geregeld bij artikel 13 van de wet van 20 juli 2022. In de memorie van toelichting van die wet wordt bovendien op transparante wijze gepreciseerd waarom de bewaring niet alleen op basis van geografische criteria gericht kan zijn. De Ministerraad preciseert bovendien dat de wetgever, met de aanneming van de wet van 20 juli 2022, de beoordelingsbevoegdheid uitoefent die hem bij de Europese rechtspraak inzake de bescherming van gegevens wordt toegekend, waarbij erover wordt gewaakt zich te voegen naar de door die rechtspraak geleverde aanwijzingen. Dat is met name het geval voor het gebruik van de voormelde geografische criteria, die verwijzen naar vijf categorieën van plaatsen, die overeenstemmen met de door het Hof van Justitie zelf aangehaalde categorieën. Het gaat om zones die worden gekenmerkt door een hoge graad van zware criminaliteit, door een ernstig dreigingsniveau, door een bijzondere blootstelling aan zware criminaliteit, door een potentiële ernstige bedreiging van de vitale belangen van het land of van de essentiële noden van de bevolking, en door een potentiële ernstige bedreiging van de belangen van internationale instellingen op het nationale grondgebied. De bewaartermijn van gegevens wordt bovendien aangepast aan de intensiteit van de criminaliteit in elke zone. Die keuzes zijn verantwoord in de parlementaire voorbereiding aan de hand van concrete voorbeelden, met de rechtspraak van het Hof en die van het Hof van Justitie als referentie. In elk geval toont de verzoekende partij niet aan hoe de bij de rechtspraak van het Hof van Justitie toegekende beoordelingsbevoegdheid op

onevenredige wijze zou zijn aangewend, noch hoe de minutieuze verantwoording van de maatregel onjuistheden of lacunes zou bevatten.

De Ministerraad benadrukt dat de wet van 20 juli 2022 voortvloeit uit een complex evenwicht gerealiseerd door de wetgever, met name op technisch vlak. Die complexiteit wordt bevestigd door de bij artikel 45, eerste lid, van die wet bepaalde uitgestelde inwerkingtreding, die getuigt van het evenwicht dat de wetgever heeft gevonden tussen verschillende legitieme belangen, namelijk de bescherming van de Staat en zijn burgers, de eerbiediging van het privéleven en de technische capaciteiten van de operatoren. De Ministerraad herinnert bovendien eraan dat het Hof geen jurisdictionele controle uitoefent over de inhoud van de parlementaire voorbereiding, noch over het proces van totstandkoming van de wet. Bovendien valt de beoordeling van mogelijke technische middelen onder de beoordelingsbevoegdheid van de wetgevende macht, in het bijzonder in de technisch complexe domeinen.

Zaken nrs. 7929, 7930, 7931 en 7932

De bewaring van gegevens

A.42.1. Wat betreft de kritiek van de verzoekende partijen op de bewaring van gegevens, betoogt de Ministerraad dat de artikelen 8 en 12 van de wet van 20 juli 2022, die de operatoren verplichten om de identificatiegegevens van eindgebruikers te bewaren gedurende een periode van twaalf maanden, abonnees te identificeren en bepaalde gegevens waarmee zij kunnen worden geïdentificeerd te bewaren, evenredig zijn. Volgens hem is het in de praktijk niet steeds eenvoudig om een eindgebruiker, apparatuur of een dienst te identificeren, zodat het soms noodzakelijk is om aanvullende gegevens te bewaren of gegevens te kruisen om te komen tot een juiste identificatie in de zin van artikel 5, lid 1, *d)*, van de AVG, zoals in de parlementaire voorbereiding van de wet van 20 juli 2022 wordt gepreciseerd. Het is overigens essentieel dat de operatoren voldoende identificatiegegevens bewaren opdat de autoriteiten de personen, apparatuur of diensten die van belang zijn voor het onderzoek, snel, precies en nauwkeurig zouden kunnen identificeren. In dat verband bevat de parlementaire voorbereiding, voor elk soort identificatiegegeven, een minutieuze verantwoording. De lijst met de beoogde gegevens is overigens het resultaat van een openbare raadpleging en van de technische inbreng van de operatoren. Bovendien worden de databanken op geautomatiseerde wijze gerealiseerd met toepassing van artikel 8 van de wet van 20 juli 2022, waardoor een individueel geval pas in aanmerking kan worden genomen in het stadium van de toegang tot een bewaard gegeven. Voor het overige komt het de Koning toe de beoogde gegevens te preciseren, met inachtneming van de AVG en van de wet van 30 juli 2018, om de databanken aan te passen aan toekomstige technische ontwikkelingen.

Met betrekking tot de periode van twaalf maanden gedurende welke de gegevens moeten worden bewaard, voert de Ministerraad aan dat die termijn is verantwoord in de parlementaire voorbereiding en dat aan die algemene termijn kan worden gesleuteld opdat hij zou beantwoorden aan de technische realiteit waarmee de operatoren worden geconfronteerd. De wetgever heeft bijgevolg ervoor gezorgd dat termijnen worden vastgesteld die beantwoorden aan zijn behoeften met betrekking tot de nagestreefde doeleinden.

A.42.2. Wat betreft de kritiek inzake de noodzaak om de verplichting tot bewaring van gegevens uit te breiden tot operatoren als WhatsApp of Skype, wijst de Ministerraad erop dat krachtens de richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 « tot vaststelling van het Europees wetboek voor elektronische communicatie (herschikking) », bepaalde diensten die door die operatoren worden verleend, voortaan zijn opgenomen in de definitie van « elektronische communicatiedienst », zodat laatstgenoemden de hoedanigheid van operator hebben op dezelfde voet als de traditionele operatoren. In werkelijkheid bekritiseren de verzoekende partijen de definitie zelf, en niet de wet van 20 juli 2022. Aangezien de voormelde ondernemingen elektronische-communicatiediensten verlenen, is het hoe dan ook gerechtvaardigd hen, met inachtneming van de beginselen van gelijke behandeling, niet-discriminatie en technologische neutraliteit, op dezelfde manier te behandelen als de aanbieders van traditionele communicatiediensten wat de bewaring van identificatiegegevens betreft, temeer omdat personen tegen wie een onderzoek loopt steeds meer de diensten van de « nieuwe » operatoren gebruiken.

A.42.3. De Ministerraad merkt op, met betrekking tot de kritiek op artikel 12 van de wet van 20 juli 2022, artikel dat een operator de mogelijkheid biedt om een van zijn abonnees te identificeren via de in een voertuig ingebouwde simkaart, dat die bepaling geenszins een tracking van personen toestaat. Het is slechts een manier om de identiteit van de hoofdbestuurder van een voertuig terug te vinden, die in de parlementaire voorbereiding nauwkeurig wordt verantwoord, wat aantoont dat de belangen op dat punt daadwerkelijk tegen elkaar zijn

afgewogen. De Ministerraad voegt eraan toe dat die maatregel is toegestaan door de rechtspraak van het Hof van Justitie, aangezien die het niet concreet mogelijk maakt om informatie af te leiden over de communicaties van de bestuurder.

A.42.4. Volgens de Ministerraad is de identificatie van het IP-adres aan de bron, waarin artikel 13 van de wet van 20 juli 2022 voorziet, in overeenstemming met de rechtspraak van het Hof van Justitie. De noodzaak om de *identifier* van de eindapparatuur van een eindgebruiker, met name de internationale identiteit van de mobiele apparatuur, de permanente *identifier* van de apparatuur en het adres van de *controller* van de toegang tot het netwerk, bedoeld in artikel 8 van die wet, is overigens nauwkeurig toegelicht in de parlementaire voorbereiding. De bewaring van die gegevens is bovendien geregeld bij artikel 13 van de wet.

A.42.5. Bij zijn arrest nr. 158/2021 van 18 november 2021 (ECLI:BE:GHCC:2021:ARR.158) heeft het Hof overigens reeds geantwoord op de kritiek inzake het vermoeden van gebruik door de geïdentificeerde persoon, waarin artikel 12 van de wet van 20 juli 2022 voorziet. In het kader van het gebruik van een wifinetwerk kan de abonnee van een operator immers het in die bepaling bedoelde vermoeden weerleggen door aan te tonen dat hij niet de enige gebruiker van dat netwerk is. Wat meer bepaald de vaste internettoegangsdiensten betreft die door natuurlijke personen worden gebruikt buiten hun verblijfplaats en de plaats waar zij hun beroepsactiviteit uitoefenen, zoals de elektronische-communicatiediensten die kosteloos worden verstrekt door middel van wifihotspots, wil de wetgever de identificatie van een abonnee vergemakkelijken, met name via de ontvangst van een sms van de operator. Wat ten slotte de kritiek op het gebruik van een wifihotspot buiten medeweten van de abonnee betreft, preciseert de Ministerraad dat die laatste de passende en noodzakelijke maatregelen moet nemen om een dergelijke indringing te verhinderen. Uit het voorgaande blijkt geen enkele schending van het vermoeden van onschuld of van de rechten van verdediging.

A.42.6. De Ministerraad merkt, in verband met de algemene kritiek inzake het bewaren van metagegevens, op dat artikel 5 van de wet van 20 juli 2022 tot doel heeft fraude en kwaadwillig gebruik van netwerken te bestrijden alsook de veiligheid en de correcte werking van netwerken mogelijk te maken. Daartoe legt het met name de verplichting op om bepaalde noodzakelijk geachte metagegevens te bewaren, wat veronderstelt dat de operatoren de belangen in kwestie tegen elkaar afwegen voor elk geval van bewaring, zoals blijkt uit de parlementaire voorbereiding. In het kader van de bestrijding van fraude en kwaadwillig gebruik van netwerken zijn de operatoren immers het meest geschikt om de noodzaak van het bewaren van metagegevens concreet te beoordelen in het kader van de door de wetgever vastgelegde doelstellingen. Het noodzakelijke karakter van die maatregel werd overigens zorgvuldig verantwoord in de parlementaire voorbereiding. Er is trouwens in een noodzakelijkheidstoets voorzien voordat de operatoren overgaan tot bewaring. Tot slot overlapt artikel 5 van de wet van 20 juli 2022 in geen enkel opzicht met artikel 107/2 van de wet van 13 juni 2005, aangezien de verhouding tussen die bepalingen is toegelicht in de parlementaire voorbereiding van de wet van 20 juli 2022. In werkelijkheid zijn die bepalingen complementair aangezien artikel 107/2 van de wet van 13 juni 2005 de operatoren verplicht om de nodige maatregelen te nemen teneinde het risico inzake veiligheid van netwerken en diensten te beheersen, terwijl artikel 5 van de wet van 20 juli 2022 de operatoren toestaat om gegevens te verzamelen en te bewaren zodat zij aan de voormelde wettelijke verplichting kunnen voldoen. Artikel 107/2 van de wet van 13 juni 2005, afzonderlijk beschouwd, vormt immers geen toereikende wettelijke grondslag om de verwerking en de bewaring van de beoogde gegevens mogelijk te maken, aangezien het gaat om een inmenging in het recht op eerbiediging van het privéleven en rekening houdend met de bijzondere bescherming voor verkeers- en locatiegegevens. Zonder artikel 5 van de wet van 20 juli 2022 zouden de operatoren met andere woorden niet in staat zijn om die gegevens te verzamelen en te bewaren conform de richtlijn 2002/58/EG, die minder soepel en strenger is dan de AVG, ten opzichte waarvan zij een *lex specialis* vormt. De rechten en vrijheden van de betrokken personen zijn dus geenszins afgezwakt door de aanneming van artikel 5 van de wet van 20 juli 2022.

A.42.7. Wat betreft de voorzienbaarheid en de wettigheidscontrole inzake de bewaring en de door de inlichtingendiensten gevorderde toegang tot verkeers- en locatiegegevens, voert de Ministerraad aan dat artikel 34 van de wet van 20 juli 2022 de rechtspraak van het Hof van Justitie met betrekking tot de richtlijn 2002/58/EG nauwgezet ten uitvoer legt. Uit de in het voormelde artikel 34 gehanteerde juridische begrippen blijkt trouwens dat de voorzienbaarheid van de maatregel gewaarborgd is en dat, in elke situatie van ernstige bedreiging van de nationale veiligheid, alleen de gegevens die strikt noodzakelijk zijn voor het bereiken van het nagestreefde doel, worden bewaard. Eenzelfde redenering geldt voor artikel 37 van de wet van 20 juli 2022, waarvoor overigens in een controle door een onafhankelijke autoriteit is voorzien.

A.43.1. In zijn memorie van wederantwoord geeft de Ministerraad nadere toelichtingen bij de kritiek van de verzoekende partijen met betrekking tot de bewaring van de gegevens.

A.43.2. De Ministerraad voert allereerst aan dat wel degelijk een onderscheid moet worden gemaakt tussen de identificatiegegevens en de metagegevens in het kader van de wet van 20 juli 2022. De alternatieve definitie van de metagegevens die door de verzoekende partij in de zaak nr. 7931 wordt voorgesteld, is in dat opzicht niet correct. Bovendien heeft de rechtspraak van het Hof van Justitie noch de gegevens die het voorwerp konden uitmaken van een bewaarplicht, noch de identificatiegegevens die het voorwerp kunnen uitmaken van een inmenging in de vorm van een algemene bewaarplicht, op exhaustieve wijze geïdentificeerd. In werkelijkheid heeft de Belgische wetgever een volledigere en nauwkeurigere oefening gemaakt dan het Hof van Justitie, dat zich enkel heeft uitgesproken over het IP-adres en over de burgerlijke-identiteitsgegevens. Die gegevens zijn overigens onvoldoende om het doel van identificatie te verwezenlijken, aangezien de inlichtingen over de burgerlijke identiteit moeten worden gekruist om de betrouwbaarheid ervan te waarborgen. Bovendien worden de gegevens omtrent de burgerlijke identiteit niet verzameld door de operatoren van nummeronafhankelijke interpersoonlijke communicatiediensten. Het IP-adres aan de bron blijkt overigens ook onvoldoende in zoverre bepaalde misdrijven kunnen worden gepleegd aan de hand van een elektronische-communicatiedienst waarvoor het IP-adres niet wordt gebruikt. Ten slotte laat de bewaring van enkel het IP-adres, zonder de datum en het tijdstip van de communicatie of de gebruikte poort, niet toe de gebruiker te identificeren in het geval van gedeelde IP-adressen.

De Ministerraad voegt eraan toe dat, in tegenstelling tot hetgeen de verzoekende partij in de zaak nr. 7930 aanvoert, het IP-adres aan de bron het op zich niet mogelijk maakt de volledige zoekgeschiedenis van een internetgebruiker te traceren. Het is in die logica dat de wetgever ervoor heeft gekozen het IP-adres te verwerken als identificatiegegeven wanneer het enkel daarvoor wordt gebruikt, en als metagegeven waarvoor een zeer strikte regeling geldt in de andere gevallen. Hetzelfde geldt voor de andere technische gegevens waarmee de gebruiker van een dienst kan worden geïdentificeerd. In het algemeen merkt de Ministerraad op dat alle gegevens beoogd in artikel 8 van de wet van 20 juli 2022 beantwoorden aan het enige doel de gebruiker te identificeren. De omstandigheid dat die gegevens talrijk zijn, brengt geen ernstigere inmenging met zich mee dan wanneer zij minder talrijk zouden zijn, aangezien geen van die gegevens iets anders onthult dan de identiteit van de geviseerde persoon.

A.43.3. Wat betreft de voorwaarden van de verplichting om gegevens te bewaren, wijst de Ministerraad erop dat de bewaringstermijn pertinent is om de mate van inmenging van de maatregel in de grondrechten te beoordelen. Te dezen blijkt uit het feit dat de wet van 20 juli 2022 meerdere termijnen onderscheidt dat de wetgever de bewaarplicht, met inbegrip van de duur ervan, tot het strikt noodzakelijke wilde beperken. Voor het overige is de rechtspraak van het Hof van Justitie die door de verzoekende partij in de zaak nr. 7930 wordt geciteerd, te dezen niet relevant omdat zij betrekking heeft op de verkeers- en locatiegegevens, en niet op de identificatiegegevens. De Ministerraad geeft daarnaast toe dat de bewaring van gegevens, enerzijds, en de toegang tot gegevens, anderzijds, verschillende verrichtingen zijn. De bewaring op zich is echter nutteloos om criminaliteit te bestrijden of de nationale veiligheid te waarborgen. Het is dus artificieel te overwegen om gegevens te bewaren zonder in regels te voorzien voor de toegang tot die gegevens. De Ministerraad onderstreept overigens dat de verschillende adviezen die in het kader van de totstandkoming van de wet van 20 juli 2022 werden ingewonnen, getuigen van een evenwicht tussen verschillende doelstellingen, die geïllustreerd worden door het standpunt van de actoren op het terrein. Wat overigens het ontbreken van statistische gegevens betreft, die volgens de verzoekende partij in de zaak nr. 7930 noodzakelijk zouden zijn om een inmenging in het recht op eerbiediging van het privéleven toe te staan, merkt de Ministerraad op dat de wetgever niet verplicht is om informatiebronnen over te leggen of te verifiëren dat een bepaalde methode is toegepast, onverminderd de vereisten die bij de Grondwet of bij de wet zijn vastgelegd. Het Hof is niet bevoegd om de werkwijze van de wetgever of de wetenschappelijke grondslag van een wettelijke maatregel te verifiëren.

A.43.4. De Ministerraad voegt eraan toe, wat betreft de bestrijding van fraude en van kwaadwillig gebruik van netwerken alsook de veiligheid en de correcte werking van de netwerken, waarvan sprake is in artikel 5 van de wet van 20 juli 2022, dat de in die bepaling beoogde gegevens inlichtingen zijn die steeds noodzakelijk zijn om de Ombudsdienst in staat te stellen zijn opdracht te vervullen en aan de klager de identiteit mee te delen van de persoon die kwaadwillige oproepen pleegt. Er moet dus geen beoordelingsmarge aan de operator worden gelaten. Bovendien worden de bestrijding van fraude en van kwaadwillig gebruik van netwerken alsook de veiligheid en een correcte werking van netwerken, als doeleinden, niet uitgesloten door de rechtspraak van het Hof van Justitie, die zich niet over die onderwerpen heeft uitgesproken. Daarnaast worden bepaalde gegevens bedoeld in artikel 5 van de wet van 20 juli 2022 hoe dan ook reeds door de operatoren gebruikt om incidenten of anomalieën op te sporen en om verkeersstromen op hun netwerken te beheren en te optimaliseren. Tot slot vormen artikel 15, lid 1, van de richtlijn 2002/58/EG en artikel 23 van de AVG volgens de Ministerraad een geldige rechtsgrond voor artikel 5 van de wet van 20 juli 2022, zoals in de parlementaire voorbereiding van die wet wordt onderstreept.

De verplichting tot gerichte bewaring van gegevens en het criterium van geografische differentiatie

A.44.1. Wat betreft de kritiek van de verzoekende partijen op de verplichting tot gerichte bewaring van metagegevens en op het criterium van geografische differentiatie, merkt de Ministerraad eerst op dat het Hof van Justitie weliswaar de verplichting tot een algemene bewaring van gegevens heeft veroordeeld, maar niettemin voorstellen voor alternatieve benaderingen heeft geformuleerd, met name een differentiatie van de categorieën van personen en een differentiatie op geografische basis. Volgens de Ministerraad heeft de wetgever dat tweede voorstel gevolgd door artikel 9 van de wet van 20 juli 2022 aan te nemen. De in die bepaling opgesomde geografische criteria resulteren uit de zoektocht naar een evenwicht tussen de aanwezige belangen en zijn overigens een strikte toepassing van de rechtspraak van het Hof van Justitie, die suggereert dat een geografisch criterium moet steunen op het risico dat een misdrijf wordt voorbereid of gepleegd, dat op een objectieve manier wordt ingeschat. De wetgever is op die suggestie ingegaan door vijf categorieën van plaatsen te onderscheiden die overeenstemmen met de door het Hof van Justitie opgelijste categorieën, maar die nauwkeuriger zijn omschreven.

De Ministerraad onderstreept bovendien dat de wetgever heeft toegezien op de evenredigheid van de maatregel door progressieve kwantitatieve criteria vast te leggen zodat, zelfs op de plaatsen waarvoor de bewaarplicht geldt, een onderscheid wordt gemaakt naargelang van de intensiteit waarmee het gekozen geografisch criterium zich concreet voordoet. Het bepalen van het niveau van die criteria behoort overigens tot de beoordelingsmarge van de wetgever en ontsnapt aan de toetsing van het Hof. De Ministerraad voegt eraan toe dat de plaatsen waarvoor in een bewaring is voorzien, verbonden zijn aan een variabele, dat wil zeggen een gegeven dat kan evolueren in de tijd, zodat voor de betrokken plaats al dan niet een bewaarplicht zal gelden naargelang van de evolutie van de variabele. De wetgever heeft dus een duidelijke en precieze regeling uitgewerkt, waarvan de toepassing niet vaststaat. Er is overigens voorzien in een periodiek controlemechanisme om te waarborgen dat de gegevensbewaring niet wordt gehandhaafd wanneer de plaats niet langer beantwoordt aan de wettelijk bepaalde criteria wegens de evolutie van de concrete situatie. De bewaarplicht is dus beperkt tot het strikt noodzakelijke en die noodzaak is onderworpen aan een strikte periodieke controle. Bovendien heeft de wetgever bepaald dat het bereiken van een drempelwaarde, wat een kwantitatief criterium betreft, wegens de evolutie van een variabele die eraan verbonden is, volstrekt geobjectiveerd is. Hij heeft immers zelf nauwgezet een betrouwbare en objectieve bron bepaald die in aanmerking moet worden genomen om de evolutie van de variabelen te beoordelen, in artikel 11 van de wet, dat de in aanmerking te nemen bronnen vermeldt. Wat betreft de uitgestelde inwerkingtreding van de wet van 20 juli 2022 waarin artikel 45, eerste lid, voorziet, wijst de Ministerraad erop dat het in de eerste plaats de wetgever toekomt om de temporele werking van de nieuwe wetsbepalingen te regelen. Voor het overige toont de uitgestelde inwerkingtreding aan dat een evenwicht is gevonden tussen uiteenlopende legitieme belangen, namelijk de doeleinden van bescherming van de Staat en zijn burgers, de eerbiediging van het privéleven en de technische capaciteit van de operatoren. Aangezien de wetgever heeft gekozen voor een gerichte bewaarplicht, levert dat bepaalde technische moeilijkheden op voor de operatoren, zodat het verantwoord en evenredig is hun de nodige tijd te geven om de nieuwe maatregelen door te voeren.

A.44.2. De concrete uitvoering van de geografische differentiatie leidt volgens de Ministerraad niet tot een ongedifferentieerde bewaarplicht, zoals in de parlementaire voorbereiding wordt onderstreept. De omstandigheid dat de wet van 20 juli 2022 op een bepaald moment tot een algemene bewaarplicht kan leiden, doet niets af aan die vaststelling aangezien in dat theoretische geval, de verplichting gedifferentieerd zou zijn. Indien overigens het gehele grondgebied zou worden beoogd, zou dat zijn door een gecombineerde toepassing van objectieve en evenredige criteria. Bovendien worden de geografische criteria gebruikt op basis van variabelen die niet bevroren zijn in de tijd, zodat het, indien alle zones van het grondgebied zouden worden gekenmerkt door een hoog criminaliteitscijfer, om een uitzonderlijke en tijdelijke situatie zou gaan. De kritiek van de verzoekende partijen dat het aantal zones en plaatsen bedoeld in de wet van 20 juli 2022 bijzonder hoog zou zijn terwijl België een Staat van beperkte omvang is, is niet gegrond. In de parlementaire voorbereiding wordt immers zorgvuldig uiteengezet om welke redenen de wet een bepaalde plaats of een bepaald criterium van geografische differentiatie bevat. Bovendien vertoont België bepaalde specifieke kenmerken die het onderscheiden van zijn buurlanden en die een groter aantal en een grotere dichtheid van plaatsen tot gevolg hebben waardoor het gericht opleggen van een bewaarplicht voor metagegevens gerechtvaardigd is.

De Ministerraad voegt eraan toe dat de criteria van geografische differentiatie die door het Hof van Justitie als voorbeeld worden aangehaald, niet cumulatief zijn. Voor het overige, ook al is het niet mogelijk om vooraf te bepalen op welk percentage van het grondgebied of van de bevolking de verplichting tot gedifferentieerde bewaring van metagegevens betrekking zou kunnen hebben, dient die maatregel daarom niet als onevenredig te worden beschouwd. Integendeel, het systeem is evenredig wegens precies het evolutieve en niet-vaststaande karakter van de variabelen die in aanmerking worden genomen door de criteria die de wetgever heeft vastgesteld. De Ministerraad voert in het bijzonder aan dat het criterium dat gekoppeld is aan de feiten van zware criminaliteit

op het niveau van het gerechtelijk arrondissement of de politiezone, niet ongerechtvaardigd of onevenredig is. Het gerechtelijk arrondissement is immers het niveau waarop de relevante statistische gegevens hoofdzakelijk worden vastgesteld. Door het hanteren van de politiezone als geografische zone kan overigens het effect van te grote verschillen binnen eenzelfde gerechtelijk arrondissement worden verzacht, en is meer precisie mogelijk. Tot slot is het niet opportuun het grondgebied in kleinere zones dan een politiezone op te delen, aangezien de betrouwbaarheid van de gegevens kan worden aangetast, enerzijds, en dit kan leiden tot een onevenredige werklast, met name voor de operatoren, anderzijds. Wat de betrouwbaarheid van de verzamelde statistische gegevens betreft, betoogt de Ministerraad dat de wetgever zorgvuldig de zo objectief mogelijke bronnen heeft gekozen voor de waarneming van de evolutie van de gebruikte variabelen, dat de betrokken politiestatistieken actueel zijn en dat die betrekking hebben op feiten los van de procedurele gevolgen ervan, zodat met die gegevens een getrouw beeld kan worden gegeven van het criminogene karakter van een zone.

A.44.3. Wat betreft de verwijzing, door artikel 11 van de wet van 20 juli 2022, naar de zware strafbare feiten die zijn omschreven bij artikel 90*ter* van het Wetboek van strafvordering, merkt de Ministerraad op dat het Hof van Justitie het begrip « zware criminaliteit » niet zelf definieert, zodat het de lidstaten toekomt dat begrip te omschrijven. In de parlementaire voorbereiding wordt in dat kader veel verduidelijkt. Hoe dan ook tonen de verzoekende partijen niet aan in welk opzicht de verwijzing naar artikel 90*ter* van het Wetboek van strafvordering afwijkt van het doel van bestrijding van zware criminaliteit, rekening houdend met de bevoegdheden van de lidstaten van de Europese Unie, noch in welk opzicht de wetgever de grenzen van de nationale beoordelingsmarge zou hebben overschreden. Voor het overige voert de Ministerraad aan dat de verwijzing naar artikel 90*ter* van het Wetboek van strafvordering gepast is, aangezien die bepaling betrekking heeft op strafbare feiten waarvoor de onderzoeksrechter over specifieke onderzoeksbevoegdheden beschikt precies omdat het voormelde Wetboek die strafbare feiten als zwaar beschouwt. Het was dus niet relevant een definitie *ad hoc* van het begrip « zwaar strafbaar feit » te hanteren in de wet van 20 juli 2022.

A.44.4. De omstandigheid dat artikel 11 van de wet van 20 juli 2022 de Koning machtigt om de lijst uit te breiden van de plaatsen en zones waarop de gerichte bewaarplicht voor metagegevens betrekking heeft, schendt geenszins het wettigheidsbeginsel, aangezien er geen enkele beoordelingsmarge bestaat in het kader van die uitbreiding, omdat een toevoeging van geografische zones moet beantwoorden aan de criteria van de wet en omdat het op die basis genomen koninklijk besluit om de drie jaar moet worden vernieuwd. In vergelijking met de wet maakt die maatregel bijgevolg een soepelere aanpassing van de lijst mogelijk, maar zonder dat het wettigheidsbeginsel geschonden wordt. Hetzelfde geldt voor de kwestie van de vaststelling van de perimeter van de zones, die werd onderzocht door de afdeling wetgeving van de Raad van State, die oordeelde dat het van belang was de vaststelling van die perimeter toe te wijzen aan één enkele autoriteit, namelijk, te dezen, de Koning.

A.44.5. Met betrekking tot de kritiek van de verzoekende partijen op de bewaring van metagegevens buiten de geïdentificeerde geografische zones, voert de Ministerraad aan dat de wet van 20 juli 2022 niet tot doel heeft de metagegevens te bewaren van een persoon die zich buiten een in de wet bedoelde zone of plaats bevindt, maar wel de bestemming te achterhalen van een communicatie die wordt uitgezonden vanuit een dergelijke zone of plaats.

A.45. In zijn memorie van wederantwoord voegt de Ministerraad eraan toe, wat betreft de kritiek van de verzoekende partijen op de verplichting tot bewaring van metagegevens, gericht op basis van een geografische differentiatie en de toepassing van die differentiatie, dat het criterium dat gebaseerd is op het aantal feiten van zware criminaliteit onmiskenbaar objectief is. De Ministerraad wijst erop dat de verzoekende partij in de zaak nr. 7930 niet aantoont in welk opzicht de gekozen drempel voor criminaliteit onevenredig is. Wat betreft de variabelen die zijn vastgesteld bij de wet van 20 juli 2022, voert de Ministerraad aan dat zij gegevens vormen die op regelmatige wijze zijn verzameld en die geaggregeerd worden over een periode van drie jaar om eventuele anomalieën verbonden aan een eenmalige gebeurtenis te corrigeren. Voor het overige is het onmogelijk op voorhand de plaats te bepalen waar het risico op strafbare feiten het hoogst is. Bovendien maken de zones bedoeld in artikel 11 van de wet van 20 juli 2022 het voorwerp uit van een jaarlijkse statistische evaluatie. Daarnaast kan de uitgestelde inwerkingtreding van die bepaling worden verklaard door technische redenen, aangezien bepaalde zones overeenkomen met een vooraf bestaande indeling, terwijl het invoeren van andere zones technisch ingewikkelder is, zowel voor de overheid als voor de operatoren.

De snelle bevriezing van gegevens

A.46. Wat betreft de kritiek van de verzoekende partijen op de « *quick-freeze* »-techniek , die neerkomt op een maatregel van snelle gegevensbewaring, merkt de Ministerraad op dat artikel 25 van de wet van 20 juli 2022

ertoe strekt artikel 88*bis* van het Wetboek van strafvordering aan te vullen, dat, voor strafrechtelijke doeleinden, de toegang van de gerechtelijke autoriteiten tot verkeers- en locatiegegevens die reeds door de operatoren worden bewaard, reglementeert. Het gaat dus om een aanvullende regeling met betrekking tot het bevriezen van gegevens voor de toekomst in het kader van een gerechtelijk onderzoek. Artikel 25 van de wet van 20 juli 2022 betreft dus dezelfde categorieën van gegevens als die welke worden beoogd door artikel 88*bis* van het Wetboek van strafvordering. De maatregel moet overigens beperkt blijven tot de gegevens die kunnen bijdragen tot het identificeren van de pleger van een strafbaar feit, zodat de draagwijdte van de gegevensbevriezing op duidelijke en specifieke wijze wordt beperkt in de beslissing van de procureur des Konings.

Artikel 25 van de wet van 20 juli 2022 kan enkel worden aangewend wanneer er ernstige aanwijzingen zijn dat een misdrijf een correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kan hebben, om zich ervan te vergewissen dat de maatregel enkel wordt toegepast in het kader van de opsporing en vervolging van strafbare feiten van een zekere ernst, wat in overeenstemming is met de lering van de rechtspraak van het Hof van Justitie. De Ministerraad merkt verder op dat de maatregel van gegevensbevriezing gepaard gaat met strikte procedurele waarborgen om risico's van misbruik en ongeoorloofde toegang te voorkomen. Hij merkt op dat de bevriezing gericht is, beperkt in de tijd en toegespitst op een opsporingsonderzoek of een gerechtelijk onderzoek. De essentiële beginselen inzake het opsporingsonderzoek en het gerechtelijk onderzoek worden ambtshalve toegepast, de duur van de bevriezingsmaatregel is beperkt tot twee maanden en de periode van gegevensbewaring door de operatoren is zes maanden. De voormelde periodes kunnen onder dezelfde voorwaarden worden hernieuwd, zodat er geen sprake is van een automatische verlenging. Zoals in de parlementaire voorbereiding wordt aangegeven, zijn die waarborgen overigens in overeenstemming met de lering uit de rechtspraak van het Hof en van het Hof van Justitie.

De toegang tot de gegevens

A.47.1. Wat de kritiek van de verzoekende partijen op de toegang tot de gegevens betreft, wijst de Ministerraad in eerste instantie erop dat artikel 13 van de wet van 20 juli 2022, dat de autoriteiten die bevoegd zijn in financiële aangelegenheden toegang verschaft tot verkeers- en locatiegegevens, in overeenstemming is met de lering van het Hof van Justitie, waarbij het aan de lidstaten wordt overgelaten om te bepalen of een strafbaar feit onder de noemer « zware criminaliteit » valt. In dat kader worden bij artikel 13 de inbreuken inzake marktmisbruik in dat begrip opgenomen, met dien verstande dat die classificatie, die overigens wordt toegestaan door het afgeleide recht van de Europese Unie, uitvoerig wordt verantwoord in de parlementaire voorbereiding. In tegenstelling tot hetgeen de verzoekende partijen aangeven, kan de Koning de lijst van de bevoegde autoriteiten die worden beoogd bij artikel 13 van de wet van 20 juli 2022, niet uitbreiden of aanvullen. Hij vermag enkel de beginselen die in de wet zijn neergelegd, operationeel ten uitvoer te leggen. Bovendien is de uitvoeringsbevoegdheid van de Koning bedoeld in artikel 9 van de wet facultatief, zoals in de parlementaire voorbereiding wordt bevestigd, en is zij strikt afgebakend. Tot slot bevat artikel 13 van de wet geen delegatie inzake bevoegde autoriteiten, aangezien het niet die kwestie betreft en een formele wetskrachtige norm van Belgisch recht beoogt.

De Ministerraad betoogt overigens dat de lijst van de doeleinden die zijn opgesomd in artikel 13 van de wet van 20 juli 2022, in overeenstemming is met artikel 15, lid 1, van de richtlijn 2002/58/EG, zoals het door het Hof van Justitie wordt geïnterpreteerd. De lidstaten kunnen immers voorzien in uitzonderingsgronden in de zin van artikel 15, lid 1, van die richtlijn, wanneer zij betrekking hebben op het voorkomen, onderzoeken, opsporen en vervolgen van onbevoegd gebruik van het elektronische communicatiesysteem, namelijk vormen van gebruik die de goede werking of de veiligheid zelf van het systeem aantasten, enerzijds, en wanneer zij zijn vastgelegd bij artikel 23, lid 1, van de AVG, anderzijds. De Ministerraad preciseert dat artikel 13 van de wet van 20 juli 2022 een onderscheid maakt tussen de gegevens bedoeld in de artikelen 126 en 127 van de wet van 13 juni 2005, waartoe overheden toegang kunnen hebben voor de doeleinden vermeld in artikel 13 van de wet van 20 juli 2022, en de IP-adressen toegewezen aan de bron van een verbinding, waarvoor een specifieke regeling geldt. De doeleinden met betrekking tot de eerste categorie van gegevens zijn volledig in overeenstemming met het recht van de Europese Unie, aangezien zij voortkomen uit de rechtspraak van het Hof van Justitie en uit artikel 23 van de AVG. Zij worden ook verantwoord in de parlementaire voorbereiding van de wet van 20 juli 2022. Een soortgelijke redenering geldt voor de IP-adressen, aangezien de kaderregeling van die tweede categorie van gegevens een nauwkeurige overname is van het kader dat is vastgelegd bij de Europese rechtspraak. Tot slot wordt de toegang tot de gegevens die op een geografische basis worden bewaard, waarin artikel 11 van de wet van 20 juli 2022 voorziet, slechts toegestaan in het kader van doeleinden die nogmaals in overeenstemming blijken met de rechtspraak van het Hof van Justitie of althans evenredig zijn met het nagestreefde doel.

A.47.2. Wat in het bijzonder de voorwaarden voor de toegang tot de gegevens betreft, merkt de Ministerraad op dat artikel 13 van de wet van 20 juli 2022 de beoogde autoriteiten niet ervan vrijstelt een verzoek tot toegang tot de gegevens te motiveren in het licht van een van de vastgelegde doeleinden. Bovendien is de kritiek van de verzoekende partijen dat de artikelen 26 en 27 van die wet niet zouden voorzien in een voorafgaande toetsing van de toegang tot bewaarde gegevens voor strafrechtelijke doeleinden, niet gegrond. Artikel 46*bis*, § 1, van het Wetboek van strafvordering, gewijzigd bij artikel 26 van de wet van 20 juli 2022, heeft immers geen betrekking op de toegang tot verkeers- en locatiegegevens, zodat de vereiste van een voorafgaande toetsing, die wordt opgelegd door het Hof van Justitie, te dezen niet van toepassing is. Daarnaast bevat artikel 46*bis* van het Wetboek van strafvordering passende waarborgen rond de erin beoogde toegang tot de gegevens. Artikel 27 van de wet van 20 juli 2022 wijzigt overigens artikel 88*bis* van het Wetboek van strafvordering om te voorzien in een systematisch optreden van de onderzoeksrechter, wat in overeenstemming is met de rechtspraak van het Hof van Justitie.

Tot slot wordt de aan de Koning verleende mogelijkheid om de medewerking te vorderen van de gesloten centra of woonunits in de zin van de wet van 15 december 1980, waarin artikel 26 van de wet van 20 juli 2022 voorziet, nauwgezet verantwoord in de parlementaire voorbereiding van de wet van 20 juli 2022, die de doelstellingen vermeldt die aantonen dat zulk een medewerking noodzakelijk is. Artikel 26 van de wet van 20 juli 2022 beoogt overigens slechts een geval van indirecte identificatie, op basis van de contactgegevens van het centrum dat of de woonunit die wordt beoogd in de informatie die rechtstreeks van de operator werd verkregen. Zonder die maatregel zou de procureur des Konings niet in staat zijn om een abonnee die in een gesloten centrum of in een woonunit in de zin van de wet van 15 december 1980 verblijft, te identificeren.

A.47.3. In zijn memorie van wederantwoord geeft de Ministerraad nadere toelichting bij de kritiek van de verzoekende partijen inzake de toegang tot de gegevens. Hij wijst eerst erop dat de kritiek van de verzoekende partij in de zaak nr. 7930 op de gelijkstelling van marktmisbruik met een strafbaar feit dat zware criminaliteit uitmaakt, voortvloeit uit een andere politieke mening dan die waarvoor de wetgever heeft gekozen, wat niet volstaat om een vernietigingsmiddel te rechtvaardigen. Vervolgens preciseert de Ministerraad dat de omzendbrief bedoeld in artikel 13 van de wet van 20 juli 2022 niets toevoegt aan de wettekst. Het betreft een interpretatieve omzendbrief om de autoriteiten te bepalen die toegang mogen hebben tot de bewaarde gegevens, aangezien artikel 13 in samenhang moet worden gelezen met andere formele wettelijke bepalingen, waardoor het minder leesbaar is. De omzendbrief mag echter geen machtiging verlenen aan een autoriteit die niet door de wet wordt beoogd.

Daarnaast stelt de Ministerraad dat, aangezien bepaalde strafbare feiten door administratieve, niet-rechterlijke autoriteiten worden vervolgd, die autoriteiten toegang moeten kunnen hebben tot de gegevens en metagegevens die noodzakelijk zijn voor de uitoefening van hun opdracht, wat geenszins is verboden door het afgeleide recht van de Europese Unie. Vervolgens worden bij de wet van 20 juli 2022 de mogelijkheden van toegang tot de beoogde gegevens in wezen niet uitgebreid, aangezien verschillende bij die wet aangewezen autoriteiten reeds beschikten over een mogelijkheid om toegang te verkrijgen tot die informatie krachtens de vroegere wetgeving. Indien bepaalde autoriteiten die bevoegdheid daadwerkelijk krijgen krachtens de wet van 20 juli 2022, is dat wegens het feit dat een groeiend aantal strafbare feiten online of met behulp van elektronische-communicatiediensten wordt gepleegd. In tegenstelling tot hetgeen de verzoekende partij in de zaak nr. 7930 aangeeft, vindt het begrip « vrijwaring van iemands vitale belangen » in de zin van artikel 13 van de wet van 20 juli 2022, tot slot wel degelijk steun in de AVG, met name in overweging 73 ervan.

De rechtsmiddelen

A.48. Wat betreft de kritiek van de verzoekende partijen over de rechtsmiddelen met betrekking tot de toegang tot de bewaarde gegevens, die ontoereikend zouden zijn doordat de betrokkenen ter zake niet worden geïnformeerd, voert de Ministerraad eerst aan dat artikel 37 van de wet van 30 juli 2018 op algemene wijze in een recht op informatie voorziet. Daarop zijn evenwel bepaalde uitzonderingen vastgelegd om de effectiviteit van strafrechtelijke onderzoeken, de bescherming van de openbare veiligheid, de bescherming van de nationale veiligheid en de bescherming van de grondrechten van anderen te waarborgen. Voor bepaalde specifieke autoriteiten voorziet de wet van 20 juli 2022 overigens in specifieke en aangepaste vereisten op het vlak van informatie, met dien verstande dat de andere soorten van toegang de algemene bescherming van artikel 37 van de wet van 30 juli 2018 genieten. Bijgevolg is een breed scala aan daadwerkelijke rechtsmiddelen toegankelijk voor de personen op wie de gegevensbewaring bedoeld in de wet van 20 juli 2022 en de toegang tot die bewaarde gegevens betrekking hebben. Voor het overige betoogt de Ministerraad dat de kritiek van de verzoekende partijen op dat gebied bijzonder summier is.

Versleutelde gegevens en de blokkering van nummers of diensten

A.49. Wat betreft de kritiek van de verzoekende partijen met betrekking tot versleutelde gegevens en de blokkering van nummers of diensten, wijst de Ministerraad erop dat artikel 3 van de wet van 20 juli 2022 opnieuw de vrijheid bevestigt om gegevens te versleutelen, maar daarbij in drie beperkingen voorziet die strikt begrensd zijn en beantwoorden aan duidelijk verantwoorde doelstellingen. De eerste beperking strekt ertoe de doeltreffendheid van noodcommunicatie naar de hulpdiensten te waarborgen. De tweede beperking is bedoeld om de doeltreffendheid van de wet van 20 juli 2022 zelf te waarborgen teneinde te vermijden dat een operator versleutelingssystemen zou gebruiken om te ontsnappen aan de toepassing van de verplichtingen inzake gegevensbewaring. De derde beperking betreft uitsluitend het specifieke geval van de buitenlandse simkaarten die geactiveerd zijn op het Belgische grondgebied, om zich ervan te vergewissen dat het sluiten van roamingovereenkomsten met buitenlandse operatoren in overeenstemming is met de vereisten van de Belgische wetgeving, zodat de Belgische operatoren zich kunnen conformeren aan dezelfde wettelijke bepalingen als voor hun eigen gebruikers. Artikel 3 van de wet van 20 juli 2022 is bijgevolg verantwoord en evenredig ten opzichte van het nagestreefde doel.

Met betrekking tot de bij artikel 4 van de wet van 20 juli 2022 toegestane blokkering van nummers bevestigt de Ministerraad dat die bepaling tot doel heeft de ontoereikendheid van het juridische kader te verhelpen, zodat de strijd efficiënter kan worden gevoerd gelet op de aard van de fraude en van ander kwaadwillig gebruik, in het belang van zowel de gebruikers als de elektronische-communicatiediensten. Artikel 4 laat het aan de operatoren over om de te nemen gepaste maatregelen te bepalen, zoals antispam-maatregelen of een blokkering van nummers, aangezien zij het meest geschikt zijn om de gepastheid van die maatregelen te beoordelen. Inzake fraude en kwaadwillig gebruik is het overigens essentieel om zeer snel te handelen. Bovendien geeft artikel 4 voorbeelden van maatregelen met het oog op een grotere rechtszekerheid en is voorzien in beperkingen. In dat kader mogen de operatoren geen kennis nemen van de inhoud van de communicatie, is bepaald dat het BIPT het bestaan van fraude of kwaadwillig gebruik van een netwerk kan verifiëren om aan de operatoren instructies op te leggen ter bescherming van de belangen van de gebruikers, en komt het de Koning toe om, zo nodig, de te nemen maatregelen te preciseren.

Onwettig verkregen bewijselementen

A.50. Wat betreft de kritiek van de verzoekende partijen met betrekking tot het lot van onwettig verkregen bewijselementen, voert de Ministerraad aan dat het niet aan het Hof staat zich over dat element uit te spreken, aangezien een dergelijk verzoek buiten het kader valt van de objectieve grondwettigheidstoetsing van de wet van 20 juli 2022. In werkelijkheid wordt het lot van onwettig verkregen strafrechtelijke bewijzen geregeld door het Wetboek van strafvordering en door de voorafgaande titel van het Wetboek van strafvordering. Het komt in voorkomend geval de feitenrechter toe de pertinente bepalingen toe te passen, in elke concrete zaak, rekening houdend met de omstandigheden van de zaak en met de toepasselijke Europese rechtspraak.

De bescherming van het beroepsgeheim

A.51. Wat betreft de kritiek van de verzoekende partijen inzake de bescherming van het beroepsgeheim, verwijst de Ministerraad in eerste instantie naar zijn proceduregeschriften in de zaak nr. 7907. Voor het overige preciseert hij dat uit het arrest van het Hof nr. 26/96 van 27 maart 1996 (ECLI:BE:GHCC:1996:ARR.026) blijkt dat het verschil in behandeling tussen de artsen en advocaten, enerzijds, en de boekhoudkundige en fiscale professionals, anderzijds, niet discriminerend is. De bij de wet van 20 juli 2022 ingevoerde procedurele bescherming geldt immers enkel voor de artsen en de advocaten omdat zij houder zijn van het beroepsgeheim krachtens artikel 458 van het Strafwetboek, een vertrouwensrelatie met hun cliënten en patiënten onderhouden en afhangen van bij de wet georganiseerde instanties die waken over de naleving van de beroepsdeontologie.

De verzoeken om prejudiciële vragen te stellen aan het Hof van Justitie van de Europese Unie

A.52.1. Wat betreft de door de verzoekende partij in de zaak nr. 7931 geformuleerde verzoeken om prejudiciële vragen te stellen aan het Hof van Justitie, preciseert de Ministerraad dat hij in principe niet gekant is tegen die verzoeken, op voorwaarde dat de vragen worden geherformuleerd. De formulering die door die

verzoekende partij wordt voorgesteld, is immers te tendentieus in zoverre zij suggereert dat de bestreden bepalingen niet in overeenstemming zijn met het Unierecht.

A.52.2. Wat de prejudiciële vraag over de bewaring van communicatiegegevens betreft, is de Ministerraad van oordeel dat de lering uit het arrest van het Hof van Justitie van 6 oktober 2020 in zake *La Quadrature du Net e.a.* (C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791) te dezen kan worden overgenomen. In geval van twijfel daarover zou aan het Hof van Justitie een vraag kunnen worden gesteld om te bepalen of artikel 15, lid 1, van de richtlijn 2002/58/EG, in samenhang gelezen met de artikelen 7, 8, 11 en 52, lid 1, van het Handvest, een wettelijke maatregel toestaat die de aanbieders van elektronische-communicatiediensten verplicht om de technische gegevens te bewaren waarmee de plegers van online of offline strafbare feiten kunnen worden geïdentificeerd.

A.52.3. Wat betreft de prejudiciële vraag over het bewaren en het verwerken van bepaalde verkeers- en locatiegegevens om een vermeend geval van fraude of een vermeend kwaadwillig gebruik van een elektronische-communicatienetwerk op te sporen en te analyseren, voert de Ministerraad aan dat die maatregelen binnen de grenzen vallen die zijn toegestaan bij de richtlijn 2002/58/EG. In geval van twijfel daarover zou aan het Hof van Justitie een vraag kunnen worden gesteld om te bepalen of artikel 15, lid 1, van de richtlijn 2002/58/EG, in samenhang gelezen met de artikelen 7, 8 en 52, lid 1, van het Handvest, een wettelijke maatregel toestaat die ertoe strekt bepaalde verkeers- en locatiegegevens die noodzakelijk zijn ter bescherming van de belangen van de operator en van de eindgebruiker tegen fraude en kwaadwillig gebruik van het netwerk, te bewaren en te verwerken.

A.52.4. Wat betreft de prejudiciële vraag over de bewaring van verkeers- en locatiegegevens om bepaalde specifieke strafbare feiten te bestrijden, namelijk computermisbruik, informaticabedrog en diefstal met geweld, zonder rekening te houden met de strafdrempel, stelt de Ministerraad dat het begrip « zware criminaliteit » een dynamisch en evolutief begrip is, maar ook dat het aan de lidstaten is om de strafbare feiten te bepalen die tot die categorie behoren. Het staat niet aan het Hof van Justitie om zich uit te spreken over de vraag of een specifiek strafbaar feit, afhankelijk van de omstandigheden, kan vallen onder zware criminaliteit.

In geval van twijfel daarover zou aan het Hof van Justitie een vraag kunnen worden gesteld om te bepalen of artikel 15, lid 1, van de richtlijn 2002/58/EG, in samenhang gelezen met de artikelen 7, 8 en 52, lid 1, van het Handvest, toestaat dat een wettelijke maatregel verwijst naar bepalingen van nationaal recht om te bepalen welke strafbare feiten onder zware criminaliteit vallen.

A.52.5. Wat betreft de prejudiciële vragen over de mogelijkheden die aan de onderzoeksrechter, de procureur des Konings en de officieren van gerechtelijke politie worden geboden, brengt de Ministerraad in herinnering dat de artikelen 26 en 27 van de wet van 20 juli 2022 in overeenstemming zijn met de richtlijn 2002/58/EG. In geval van twijfel daarover zouden die vragen aan het Hof van Justitie kunnen worden voorgelegd om te bepalen, in eerste instantie, of artikel 15, lid 1, van de richtlijn 2002/58/EG, in samenhang gelezen met de artikelen 7, 8 en 52, lid 1, van het Handvest, een wettelijke maatregel toestaat waarbij de procureur des Konings wordt gemachtigd om een abonnee of gewoonlijke gebruiker van een elektronische-communicatiedienst of –middel te laten identificeren, alsook om de elektronische-communicatiediensten waarop een bepaalde persoon geabonneerd is of die gewoonlijk door een bepaalde persoon worden gebruikt, te laten identificeren. Vervolgens zou een andere prejudiciële vraag kunnen worden gesteld om te bepalen of artikel 15, lid 1, van de richtlijn 2002/58/EG, in samenhang gelezen met de artikelen 7, 8 en 52, lid 1, van het Handvest, een wettelijke maatregel toestaat waarbij de onderzoeksrechter of, in geval van ontdekking op heterdaad, de procureur des Konings wordt gemachtigd om toegang te verkrijgen tot verkeers- en locatiegegevens ten behoeve van de bestrijding van zware criminaliteit.

A.52.6. Wat de prejudiciële vraag over het inlichten van de betrokken persoon betreft, betoogt de Ministerraad dat die vraag niet nodig is voor de oplossing van het geschil. Hij is er evenwel niet ertegen gekant dat de vraag wordt gesteld. Wat daarentegen de laatste prejudiciële vraag betreft, over de bewijselementen die zijn verzameld met toepassing van de wet van 20 juli 2022 in het geval dat die wet zou worden vernietigd, herinnert de Ministerraad eraan dat het aan de betrokken strafrechter staat om zich uit te spreken over het lot van die bewijzen, zodat de vraag niet nodig is.

- B –

Ten aanzien van de bestreden wet en de context ervan

B.1. De beroepen tot vernietiging hebben betrekking op de wet van 20 juli 2022 « betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten » (hierna : de wet van 20 juli 2022).

Die wet brengt wijzigingen aan in de wet van 13 juni 2005 « betreffende de elektronische communicatie » (hierna : de wet van 13 juni 2005) (artikelen 2 tot 17 van de wet van 20 juli 2022), de wet van 1 juli 2011 « betreffende de beveiliging en de bescherming van de kritieke infrastructuren » (hierna : de wet van 1 juli 2011) (artikel 18 van de wet van 20 juli 2022), de wet van 17 januari 2003 « met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector » (hierna : de wet van 17 januari 2003) (artikelen 19 tot 24 van de wet van 20 juli 2022), het Wetboek van strafvordering (artikelen 25 tot 27 van de wet van 20 juli 2022), de wet van 5 augustus 1992 « op het politieambt » (hierna : de wet van 5 augustus 1992) (artikel 28 van de wet van 20 juli 2022), de wet van 30 november 1998 « houdende regeling van de inlichtingen- en veiligheidsdiensten » (hierna : de wet van 30 november 1998) (artikelen 29 tot 39 van de wet van 20 juli 2022), de wet van 2 augustus 2002 « betreffende het toezicht op de financiële sector en de financiële diensten » (hierna : de wet van 2 augustus 2002) (artikelen 40 en 41 van de wet van 20 juli 2022), de wet van 7 april 2019 « tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid » (hierna : de wet van 7 april 2019) (artikelen 42 en 43 van de wet van 20 juli 2022) en de wet van 24 januari 1977 « betreffende de bescherming van de gezondheid van de gebruikers op het stuk van de voedingsmiddelen en andere produkten » (artikel 44 van de wet van 20 juli 2022). De wet van 20 juli 2022 bevat eveneens verschillende « overgangsbepalingen » (artikelen 45 tot 48 van de wet van 20 juli 2022).

B.2.1. Met de wet van 20 juli 2022 heeft de wetgever willen tegemoetkomen aan de vernietiging, bij het arrest van het Hof nr. 57/2021 van 22 april 2021 (ECLI:BE:GHCC:2021:ARR.057), van de wet van 29 mei 2016 « betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie » (hierna : de wet van 29 mei 2016) (*Parl. St.,* Kamer, 2021-2022, DOC 55-2572/001, p. 4). Het Hof heeft

dat arrest gewezen na meerdere prejudiciële vragen te hebben gesteld aan het Hof van Justitie van de Europese Unie (hierna : het Hof van Justitie) (zie arrest nr. 96/2018 van 19 juli 2018, ECLI:BE:GHCC:2018:ARR.096), dat daarop bij een in grote kamer gewezen arrest van 6 oktober 2020 heeft geantwoord in zake *La Quadrature du Net e.a.* (C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791).

B.2.2. In de parlementaire voorbereiding van de wet van 20 juli 2022 wordt in dat verband gepreciseerd :

« Ten gevolge van het arrest-*La Quadrature du Net*, gewezen door het Hof van Justitie van de Europese Unie (HvJ-EU) op 6 oktober 2020 (samengevoegde zaken C-511/18, C-512/18 en C-520/18), heeft het Belgisch Grondwettelijk Hof, bij arrest van 22 april 2021, de artikelen 2, *b)*, 3 tot 11 en 14 van de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie (de zogeheten ‘ dataretentiewet ’) vernietigd. Het voorliggende wetsontwerp is er voornamelijk op gericht die wet te herstellen en een juridisch kader te scheppen dat strookt met de rechtspraak inzake de bewaring van de ‘ verkeers- en locatiegegevens ’ in de zin van Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie, ook bekend als de ‘ e-privacyrichtlijn ’). Deze richtlijn zal worden vervangen door een verordening die een nieuwe terminologie hanteert, met name ‘ metagegevens ’ in plaats van ‘ verkeers- en locatiegegevens ’.

De dataretentiewet voorzag in de verplichting voor aanbieders van openbare telefoniediensten, waaronder ook via het internet, van internettoegang, van e-mail via het internet (ongeacht of ze bij het BIPT al dan niet een kennisgeving hadden gedaan) om bepaalde categorieën locatie- en verkeersgegevens, bepaald bij koninklijk besluit, gedurende een periode van twaalf maanden te bewaren, opdat deze gegevens beschikbaar zouden zijn voor rechtshandhavingsdoeleinden (strafrechtelijk onderzoek) dan wel voor de vervulling van de opdrachten van de inlichtingendiensten.

De vice-eersteminister merkt op dat deze gegevens geen betrekking hebben op de inhoud van de communicatie. Daarom betreft het ‘ metagegevens ’ (bijvoorbeeld ‘ wie belt wie ’). Het gaat dus niet om de inhoud van de telefoongesprekken.

De wet van 29 mei 2016 voorzag in een verplichting tot algemene en ongedifferentieerde bewaring van bepaalde metagegevens.

Het HvJ-EU heeft in zijn arrest-*La Quadrature du Net* echter geoordeeld dat de algemene en ongedifferentieerde bewaring zoals bepaald bij de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie, een schending inhield van bepaalde principes van Europees recht, meer bepaald het recht op privacy. Op basis van de e-privacyrichtlijn en van het Handvest van de grondrechten van de Europese Unie heeft het arrest van het HvJ-EU bepaalde alternatieve pistes voor de algemene en ongedifferentieerde databewaring te allen tijde voorgesteld :

1) de algemene en ongedifferentieerde bewaring van metagegevens in geval van een reële en actuele dan wel voorzienbare bedreiging van de nationale veiligheid;

2) de algemene en ongedifferentieerde bewaring van burgerlijke-identiteitsgegevens voor het onderzoek naar strafbare feiten die niet onder zware criminaliteit ressorteren;

3) de algemene en ongedifferentieerde bewaring van bron-IP-adressen, ter bestrijding van zware criminaliteit, de voorkoming van ernstige bedreigingen voor de openbare veiligheid en de bescherming van de nationale veiligheid;

4) met het oog op de bestrijding van zware criminaliteit en ter bescherming van de openbare veiligheid, de gerichte bewaring van metagegevens, op een geografische basis of op basis van personen in bepaalde gebieden of voor bepaalde categorieën van personen van wie vooraf is vastgesteld dat zij een specifiek risico vormen, en snelle bewaring van metagegevens (‘ *quick freeze* ’), waarbij wordt verzocht de metagegevens van een persoon gedurende een korte periode te bevriezen.

In zijn vernietigingsarrest van 22 april 2021 heeft het Grondwettelijk Hof de analyse van het HvJ-EU overgenomen.

In het wetsontwerp zijn sommige van de door het HvJ-EU aangegeven pistes gevolgd en uitgewerkt, andere dan weer niet, zoals de gerichte bewaring op basis van personen in bepaalde gebieden of voor bepaalde categorieën van personen van wie vooraf is vastgesteld dat zij een specifiek risico vormen.

De vice-eersteminister benadrukt voorts dat ook extra waarborgen zijn toegevoegd met betrekking tot de verwerking van deze gegevens door de operatoren (de aan de operatoren opgelegde veiligheidsmaatregelen werden uitgediept), alsook met betrekking tot de verstrekking van deze gegevens aan de autoriteiten (een strikter toezicht op de voorwaarden voor deze verstrekking en een voorafgaande controle van het verzoek van de autoriteit aan de operator). Aldus is uitvoering gegeven aan de vereisten van de rechtspraak.

Ten slotte beoogt dit wetsontwerp tevens in te spelen op de maatschappelijke verwachtingen van een almaar digitaler wordende wereld. Het is duidelijk dat de elektronische transacties (e-commerce) in heel wat sectoren de norm worden. Ter bestrijding van bepaalde vormen van strafbare feiten die uitsluitend online worden gepleegd, is het derhalve noodzakelijk dat de autoriteiten die zijn belast met de preventie, de opsporing en de vervolging van deze feiten, de gegevens kunnen opvragen bij de operatoren die deze in hun bezit hebben, voorzover zulks nodig is om hun respectieve opdrachten te vervullen. Daartoe wordt in hoofdstuk 10 van het wetsontwerp beoogd de inspectiedienst consumptieproducten van de FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu, in de mogelijkheid te stellen rechtspersonen of natuurlijke personen te identificeren op basis van een telefoonnummer of een IP-adres. Het gaat met andere woorden alleen om gegevens die geen precieze informatie geven over het privéleven van de betrokken personen, aangezien het identificatiegegevens betreft. Zonder deze toegang zou het deze dienst materieel niet mogelijk zijn diens wettelijke taak te vervullen en zouden de onderzoeken altijd ten laste van ‘ X ’ blijven vallen.

Het vernietigingsarrest van het Grondwettelijk Hof van 22 april 2021 heeft tevens tot gevolg dat het koninklijk besluit van 19 september 2013 tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie moet worden gewijzigd.

Bovendien noopte het vernietigingsarrest tot de wijziging van bepaalde organieke wetten, met name het Wetboek van Strafvordering en de wet op het politieambt. Deze organieke wetten bepalen de voorwaarden voor de verstrekking van de door de operatoren bewaarde gegevens aan de diverse betrokken autoriteiten » (*Parl. St.,* Kamer, 2021-2022, DOC 55-2572/003, pp. 3 tot 6).

B.2.3. Bij zijn voormelde arrest nr. 57/2021 heeft het Hof geoordeeld :

« B.18. Bij het arrest van het Hof van Justitie van 6 oktober 2020 wordt een verandering van gezichtspunt opgelegd ten opzichte van de keuze die de wetgever heeft gemaakt : de verplichting tot bewaring van gegevens met betrekking tot elektronische communicatie moet de uitzondering zijn, en niet de regel. De regeling waarbij in een dergelijke verplichting wordt voorzien, moet daarenboven onderworpen zijn aan duidelijke en nauwkeurige regels over de reikwijdte en de toepassing van de betrokken maatregel, waarbij een minimum aan vereisten worden opgelegd (punt 133). Die regeling moet waarborgen dat de inmenging tot het strikt noodzakelijke wordt beperkt en moet steeds ‘ beantwoorden aan objectieve criteria die een verband leggen tussen de te bewaren gegevens en het nagestreefde doel ’ (punten 132 en 133).

B.19. Het staat aan de wetgever een regeling tot stand te brengen waarbij de beginselen in acht worden genomen die van toepassing zijn inzake bescherming van persoonsgegevens, in het licht van de rechtspraak van het Hof van Justitie, en, in voorkomend geval, rekening te houden met de door dat Hof aangebrachte preciseringen wat betreft de verschillende soorten wettelijke maatregelen die verenigbaar worden geacht met artikel 15, lid 1, van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8, 11 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie. In het bijzonder staat het, in die context, ook aan de wetgever tussen de verschillende soorten aan bewaring onderworpen gegevens het onderscheid te maken dat geboden is, zodat wordt gewaarborgd dat, voor elk soort gegeven, de inmenging tot het strikt noodzakelijke wordt beperkt ».

B.2.4. Bij dat arrest heeft het Hof geoordeeld dat het aan de wetgever toekomt een nieuwe regelgeving uit te werken met betrekking tot de verplichting om gegevens betreffende de elektronische communicatie te bewaren, met inachtneming van de ter zake geldende beginselen, in het licht van de rechtspraak van het Hof van Justitie met betrekking tot artikel 15, lid 1, van de richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 « betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie » (hierna : de richtlijn 2002/58/EG), zelf in het licht gelezen van de artikelen 7, 8, 11 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie (hierna : het Handvest).

B.2.5. Artikel 15, lid 1, van de richtlijn 2002/58/EG vermeldt :

« De lidstaten kunnen wettelijke maatregelen treffen ter beperking van de reikwijdte van de in de artikelen 5 en 6, artikel 8, leden 1, 2, 3 en 4, en artikel 9 van deze richtlijn bedoelde rechten en plichten, indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale [veiligheid], d.w.z. de staatsveiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronische-communicatiesysteem als bedoeld in artikel 13, lid 1, van Richtlijn 95/46/EG. Daartoe kunnen de lidstaten o.a. wetgevingsmaatregelen treffen om gegevens gedurende een beperkte periode te bewaren om de redenen die in dit lid worden genoemd. Alle in dit lid bedoelde maatregelen dienen in overeenstemming te zijn met de algemene beginselen van het Gemeenschapsrecht, met inbegrip van de beginselen als bedoeld in artikel 6, leden 1 en 2, van het Verdrag betreffende de Europese Unie ».

B.2.6. In het dictum van zijn voormelde arrest van 6 oktober 2020 heeft het Hof van Justitie voor recht gezegd :

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

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

- die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een gerichte bewaring van verkeers- en locatiegegevens, die op basis van objectieve en niet-discriminatoire factoren wordt afgebakend aan de hand van categorieën betrokken personen of

aan de hand van een geografisch criterium, voor een periode die niet langer is dan strikt noodzakelijk, maar die kan worden verlengd;

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

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

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

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

B.3.1. Bovendien blijkt uit de parlementaire voorbereiding van de wet van 20 juli 2022 dat de wetgever eveneens heeft willen tegemoetkomen aan de vernietiging, bij het arrest van het Hof nr. 158/2021 van 18 november 2021 (ECLI:BE:GHCC:2021:ARR.158), van de wet van 1 september 2016 « tot wijziging van artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 16/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst » (hierna : de wet van 1 september 2016) (*Parl. St.,* Kamer, 2021-2022, DOC 55-2572/003, p. 7).

B.3.2. De parlementaire voorbereiding van de wet van 20 juli 2022 vermeldt daaromtrent :

« Het Grondwettelijk Hof heeft op 18 november 2021 inderdaad een arrest gewezen met betrekking tot de wet van 1 september 2016. Deze wet werd aangenomen na de aanslagen van Parijs, om een einde te maken aan de anonimiteit van de gebruikers van voorafbetaalde kaarten aan de hand waarvan mobiele diensten kunnen worden gebruikt (bellen, internettoegang, sms'en versturen enzovoort), door de operatoren te verplichten deze laatsten te identificeren.

In dat arrest stelt het Hof het principe van identificatie van de gebruikers van voorafbetaalde kaarten niet ter discussie, maar vernietigt het de wijziging aangebracht bij de wet van 1 september 2016 in artikel 127 van de wet van 13 juni 2005 ' zij het slechts in zoverre het niet bepaalt welke identificatiegegevens worden verzameld en verwerkt en welke identificatiedocumenten in aanmerking komen '. Volgens het Hof bepaalt artikel 22 van de

Grondwet dat deze gegevens en documenten moeten worden opgesomd in de wet. Het Hof behoudt de gevolgen van de vernietigde bepaling tot de inwerkingtreding van een wetskrachtige norm waarin die identificatiegegevens en identificatiedocumenten worden opgesomd en uiterlijk tot en met 31 december 2022.

Het arrest van het Grondwettelijk Hof van 18 november 2021 heeft enkel betrekking op artikel 127 van de wet van 13 juni 2005. Na analyse van het arrest is echter gebleken dat de lessen van het arrest - namelijk dat de door de operatoren te bewaren gegevens in de wet moeten worden opgenomen - ook van toepassing zijn op de artikelen 126 en 126/1 van die wet zoals deze in het wetsontwerp ‘ dataretentie ’ zijn voorzien. Daaruit volgt dat die artikelen 126 en 126/1 eveneens gewijzigd moeten worden » (*ibid.*, p. 7).

B.4. Uit de parlementaire voorbereiding van de wet van 20 juli 2022 blijkt dat de wetgever zowel het voormelde arrest nr. 57/2021 van 22 april 2021 als het daaraan ten grondslag liggende arrest van het Hof van Justitie van 6 oktober 2020, grondig heeft onderzocht, maar ook het voormelde arrest nr. 158/2021 van 18 november 2021.

Ten aanzien van de omvang van de beroepen tot vernietiging

B.5.1. Het Hof dient de omvang van de beroepen tot vernietiging te bepalen op basis van de inhoud van de verzoekschriften.

Het Hof kan slechts uitdrukkelijk bestreden wetskrachtige bepalingen vernietigen waartegen middelen worden aangevoerd en, in voorkomend geval, bepalingen die niet worden bestreden maar die onlosmakelijk zijn verbonden met de bepalingen die moeten worden vernietigd.

B.5.2.1. De verzoekende partij in de zaak nr. 7907 vordert de vernietiging van de artikelen 5, 4° en 6°, 8 tot 11, 13 tot 15, 19, 21, 22, 24 tot 42 en 44 van de wet van 20 juli 2022.

B.5.2.2. De verzoekende partijen in de zaak nr. 7929 vorderen de vernietiging van de artikelen 2 tot 17 van de wet van 20 juli 2022.

B.5.2.3. De verzoekende partijen in de zaken nrs. 7930, 7931 en 7932 vorderen de vernietiging van de wet van 20 juli 2022 in haar geheel.

De verzoekende partij in de zaak nr. 7930 zet echter alleen middelen uiteen tegen de artikelen 5, 6, 8, 9, 11, 12, 13, 27 en 45 van de wet van 20 juli 2022. Zij klaagt bovendien aan dat er een lacune bestaat in de wetgeving wat betreft de gegevens die worden gedekt door het beroepsgeheim.

Daarnaast is het enige middel van de verzoekende partij in de zaak nr. 7931 alleen gericht tegen de artikelen 3, 5, 8, 9, 10, 11, 13, 24, 25, 26 en 27 van de wet van 20 juli 2022.

Bovendien zetten de verzoekende partijen in de zaak nr. 7932 alleen middelen uiteen tegen de artikelen 3, 4, 5, 6, 8, 9, 10, 11, 12, 13, 15, 33, 34 en 37 van de wet van 20 juli 2022. Zij klagen eveneens aan dat er een lacune is in de wetgeving wat betreft de gegevens die worden gedekt door het beroepsgeheim.

B.6. Het onderzoek van het Hof heeft dus betrekking op de artikelen 3 tot 6, 8 tot 15, 19, 21, 22, 24 tot 42 en 45 van de wet van 20 juli 2022, alsook op de voormelde lacune in de wetgeving.

Ten aanzien van het belang

B.7.1. De Ministerraad betwist het belang om in rechte te treden van de « Ordre des barreaux francophones et germanophone » (hierna : de OBFG), verzoekende partij in de zaak nr. 7907.

Het belang van de OBFG zou zijn beperkt tot artikel 27, 2°, van de wet van 20 juli 2022, aangezien de grieven die gericht zijn tegen de andere bepalingen geen betrekking zouden hebben op het beroepsgeheim van de advocaat.

B.7.2. De Grondwet en de bijzondere wet van 6 januari 1989 op het Grondwettelijk Hof vereisen dat elke natuurlijke persoon of rechtspersoon die een beroep tot vernietiging instelt, doet blijken van een belang. Van het vereiste belang doen slechts blijken de personen wier situatie door de bestreden norm rechtstreeks en ongunstig zou kunnen worden geraakt; bijgevolg is de *actio popularis* niet toelaatbaar.

B.7.3. Artikel 495 van het Gerechtelijk Wetboek, eerste en tweede lid, bepaalt :

« De Orde van Vlaamse Balies en de Ordre des Barreaux francophones et germanophone hebben, elk voor de balies die er deel van uitmaken, de taak te waken over de eer, de rechten en de gemeenschappelijke beroepsbelangen van hun leden en zijn bevoegd voor de juridische bijstand, de stage, de beroepsopleiding van de advocaten-stagiairs en de vorming van alle advocaten behorende tot de balies die er deel van uitmaken.

Ze nemen initiatieven en maatregelen die nuttig zijn voor de opleiding, de tuchtrechtelijke regels en de loyauteit in het beroep en voor de behartiging van de belangen van de advocaat en van de rechtzoekende ».

B.7.4. De Ordes van de balies zijn publiekrechtelijke beroepscorporaties die bij wet zijn opgericht en die op verplichte wijze al diegenen die het beroep van advocaat uitoefenen, groeperen.

De Ordes van de balies kunnen, behoudens de gevallen waarin zij hun persoonlijk belang verdedigen, slechts in rechte treden binnen de opdracht die de wetgever hun heeft toevertrouwd. Aldus kunnen zij in de eerste plaats in rechte treden wanneer zij de beroepsbelangen van hun leden verdedigen of wanneer de uitoefening van het beroep van advocaat in het geding is. Volgens artikel 495, tweede lid, van het Gerechtelijk Wetboek kunnen de Ordes ook initiatieven en maatregelen nemen « die nuttig zijn [...] voor de behartiging van de belangen van de advocaat en van de rechtzoekende ».

B.7.5. Uit artikel 495 van het Gerechtelijk Wetboek, in samenhang gelezen met de artikelen 2 en 87 van de bijzondere wet van 6 januari 1989, blijkt dat de Ordes van de balies slechts als verzoekende of tussenkomende partij voor het Hof in rechte kunnen treden ter verdediging van het collectieve belang van de rechtzoekenden in zoverre dit verbonden is met de taak en de rol van de advocaat bij de behartiging van de belangen van de rechtzoekende.

Maatregelen die geen enkele weerslag hebben op het recht op toegang tot de rechter, op de rechtsbedeling of op de bijstand die advocaten aan hun cliënten kunnen verlenen, ongeacht of dat gebeurt tijdens een administratief beroep, via een minnelijke schikking of via een geschil dat wordt voorgelegd aan de gewone of administratieve rechtscolleges, vallen bijgevolg buiten het bereik van artikel 495 van het Gerechtelijk Wetboek, in samenhang gelezen met de artikelen 2 en 87 van de bijzondere wet van 6 januari 1989.

B.7.6. De bestreden bepalingen zijn erop gericht een juridisch kader te scheppen inzake de bewaring van en de toegang tot persoonsgegevens in de sector van de elektronische communicatie, na de vernietiging van de wet van 1 september 2016 bij het voormelde arrest nr. 57/2021 van het Hof.

Uit de vaststelling dat de door de OBFG bestreden bepalingen, behalve artikel 27, 2°, van de wet van 20 juli 2022, niet uitdrukkelijk de elektronische-communicatiemiddelen van de advocaten betreffen, kan niet worden afgeleid dat die bepalingen niet op hen van toepassing zijn.

De wet van 20 juli 2022 heeft een algemene draagwijdte en is van toepassing op alle elektronische-communicatiemiddelen, waaronder die welke de bescherming van artikel 458 van het Strafwetboek genieten.

De vertrouwelijke informatie die wordt toevertrouwd aan een advocaat bij de uitoefening van zijn beroep geniet de bescherming die voor de rechtzoekende voortvloeit uit de waarborgen die zijn neergelegd in artikel 6 van het Europees Verdrag voor de rechten van de mens, aangezien de aan de advocaat opgelegde regel van het beroepsgeheim een fundamenteel element is van de rechten van de verdediging van de rechtzoekende die hem in vertrouwen neemt (zie met name arrest nr. 174/2018 van 6 december 2018, ECLI:BE:GHCC:2018:ARR.174, B.25).

B.7.7. Uit het voorgaande vloeit voort dat de wet van 20 juli 2022 in maatregelen voorziet die een weerslag kunnen hebben op de uitoefening van het beroep van advocaat.

B.7.8. De exceptie van niet-ontvankelijkheid wordt verworpen.

Ten gronde

B.8.1. Artikel 6 van de voormelde bijzondere wet van 6 januari 1989 preciseert dat het verzoekschrift « het onderwerp van het beroep [vermeldt] en [...] een uiteenzetting van de feiten en middelen [bevat] ».

B.8.2. Om te voldoen aan de vereisten van artikel 6 van de voormelde bijzondere wet van 6 januari 1989 moeten de middelen en middelonderdelen te kennen geven welke van de regels waarvan het Hof de naleving waarborgt, zouden zijn geschonden, alsook welke de bepalingen zijn die deze regels zouden schenden, en uiteenzetten in welk opzicht die regels door de bedoelde bepalingen zouden zijn geschonden.

Die vereiste is niet louter formeel. Zij strekt ertoe aan het Hof alsook aan de instellingen en personen die aan het Hof een memorie kunnen richten een duidelijke en ondubbelzinnige uiteenzetting van de middelen te geven.

B.8.3. De middelen in de samengevoegde zaken bevatten een groot aantal grieven, die elkaar vaak overlappen en herhalingen bevatten. Die middelen hebben in hoofdzaak betrekking op de bestaanbaarheid van de bestreden bepalingen met het recht op eerbiediging van het privéleven en met het recht op bescherming van de persoonsgegevens, gewaarborgd bij artikel 22 van de Grondwet, artikel 8 van het Europees Verdrag voor de rechten van de mens, de artikelen 7 en 8 van het Handvest en bij meerdere bepalingen van het recht van de Europese Unie. Nog andere referentienormen worden aangehaald, evenwel zonder dat de schending ervan systematisch wordt uiteengezet. Het Hof beperkt zijn onderzoek tot de referentienormen die de partijen uiteenzetten, overeenkomstig de in B.8.2 vermelde vereisten.

B.8.4. In zoverre de middelen in de samengevoegde zaken voldoen aan de voormelde vereisten, onderzoekt het Hof de grieven van de verzoekende partijen in onderstaande volgorde :

1. Het gebruik van versleuteling (artikel 3);

2. De gebruikte maatregelen op netwerkniveau of op het niveau van de eindgebruiker om fraude en kwaadwillig gebruik van de netwerken en diensten op te sporen (artikel 4);

3. Het bewaren van de verkeersgegevens (artikel 5);

4. Het bewaren van de locatiegegevens (artikel 6);

5. Het bewaren van de inschrijvings- en identificatiegegevens (artikel 8)*;*

6. De verplichting tot identificatie van de abonnees en van de eindgebruikers van elektronische-communicatiediensten (artikel 12);

7. De gerichte bewaring van de gegevens op basis van een geografisch criterium (artikelen 9 tot 11);

8. De opsomming van de bevoegde autoriteiten en van de doeleinden in het kader van de toegang tot de gegevens (artikel 13);

9. De bevoegdheden van de officieren van gerechtelijke politie van het BIPT (artikel 24);

10. De bevoegdheden van de procureur des Konings (artikelen 25 en 26);

11. De bevoegdheden van de onderzoeksrechter (artikel 27);

12. De bevoegdheden van de inlichtingen- en veiligheidsdiensten (artikelen 33, 34 en 37);

13. De inwerkingtreding (artikel 45);

14. De bescherming van het beroepsgeheim.

1. Het gebruik van versleuteling (artikel 3)

B.9. Het enige middel in de zaak nr. 7931 en het vijfde middel in de zaak nr. 7932 hebben betrekking op artikel 3 van de wet van 20 juli 2022, dat artikel 107/5 van de wet van 13 juni 2005 als volgt vervangt :

« § 1. Ter bevordering van de digitale veiligheid is het gebruik van versleuteling vrij binnen de in de paragrafen 2 tot 4 gestelde grenzen.

§ 2. Het gebruik van versleuteling mag noodcommunicatie, met inbegrip van de identificatie van de oproepende lijn of het verstrekken van de identificatiegegevens van de oproeper, niet verhinderen.

§ 3. Het gebruik van versleuteling door een operator, met als doel de veiligheid van de communicatie te waarborgen, mag geen beletsel vormen voor de uitvoering van een gericht verzoek van een bevoegde autoriteit, onder de bij wet bepaalde voorwaarden, met als doel de identificatie van de eindgebruiker, de opsporing en de lokalisatie van niet voor het publiek toegankelijke communicatie.

§ 4. Het gebruik van versleuteling door een buitenlandse operator, wiens eindgebruiker of abonnee zich op het Belgisch grondgebied bevindt, mag de uitvoering van een verzoek van een bevoegde overheid, zoals bedoeld in de paragrafen 2 en 3, niet verhinderen.

Elk contractueel beding dat door de operatoren wordt opgesteld en de uitvoering van het eerste lid belemmert, is verboden en van rechtswege nietig ».

B.10.1. In haar enige middel, afgeleid uit de schending van de artikelen 11, 12, 22 en 29 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 7, 8, 11, 47 en 52, lid 1, van het Handvest, met artikel 8 van het Europees Verdrag voor de rechten van de mens, met de artikelen 5, 6 en 15 van de richtlijn 2002/58/EG en met de artikelen 13 en 54 van de richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 « betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad » (hierna : de richtlijn (EU) 2016/680), voert de verzoekende partij in de zaak nr. 7931 aan dat artikel 107/5, §§ 3 en 4, van de wet van 13 juni 2005, ingevoegd bij artikel 3 van de wet van 20 juli 2022, onevenredig is aangezien de versleutelingsmaatregelen net toelaten om de bescherming van de persoonsgegevens te waarborgen en om het recht op eerbiediging van het privéleven te beschermen.

B.10.2. In hun vijfde middel, afgeleid uit de schending van de artikelen 10, 11, 15, 22 en 29 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 5, 6, 8, 9, 10, 11, 14, 15, 17 en 18 van het Europees Verdrag voor de rechten van de mens, met de artikelen 7, 8, 11, 47 en 52 van het Handvest, met artikel 5, lid 4, van het Verdrag betreffende de Europese Unie en met de richtlijn 2002/58/EG, de richtlijn (EU) 2016/680 en de verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 « betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) » (hierna : de AVG), voeren de verzoekende partijen in de zaak nr. 7932 aan dat artikel 107/5, § 3, van de wet van 13 juni 2005, zoals vervangen bij artikel 3 van de wet

van 20 juli 2022, een onevenredige inmenging vormt in het recht op eerbiediging van het privéleven en voorziet in een maatregel die niet nodig is in een democratische maatschappij.

B.11.1. Uit het voormelde blijkt dat de verzoekende partij in de zaak nr. 7931 en de verzoekende partijen in de zaak nr. 7932 slechts grieven formuleren tegen artikel 107/5 van de wet van 13 juni 2005, zoals vervangen bij artikel 3 van de wet van 20 juli 2022, wat betreft de aantasting van het recht op eerbiediging van het privéleven en van het recht op bescherming van de persoonsgegevens, zoals gewaarborgd bij artikel 22 van de Grondwet, bij artikel 8 van het Europees Verdrag voor de rechten van de mens en bij de artikelen 7, 8 en 52 van het Handvest. Het Hof beperkt zijn onderzoek tot die bepalingen.

B.11.2. Artikel 22 van de Grondwet bepaalt :

« Ieder heeft recht op eerbiediging van zijn privé leven en zijn gezinsleven, behoudens in de gevallen en onder de voorwaarden door de wet bepaald.

De wet, het decreet of de in artikel 134 bedoelde regel waarborgen de bescherming van dat recht ».

Artikel 8 van het Europees Verdrag voor de rechten van de mens bepaalt :

« 1. Eenieder heeft recht op eerbiediging van zijn privé leven, zijn gezinsleven, zijn huis en zijn briefwisseling.

2. Geen inmenging van enig openbaar gezag is toegestaan met betrekking tot de uitoefening van dit recht dan voor zover bij de wet is voorzien en in een democratische samenleving nodig is in het belang van 's lands veiligheid, de openbare veiligheid, of het economisch welzijn van het land, de bescherming van de openbare orde en het voorkomen van strafbare feiten, de bescherming van de gezondheid of de goede zeden, of voor de bescherming van de rechten en vrijheden van anderen ».

Artikel 7 van het Handvest bepaalt :

« Eenieder heeft recht op eerbiediging van zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn communicatie ».

Artikel 8 van het Handvest bepaalt :

« 1. Eenieder heeft recht op bescherming van zijn persoonsgegevens.

2. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Eenieder heeft recht van inzage in de over hem verzamelde gegevens en op rectificatie daarvan.

3. Een onafhankelijke autoriteit ziet erop toe dat deze regels worden nageleefd ».

Artikel 52, lid 1, van het Handvest bepaalt :

« Beperkingen op de uitoefening van de in dit Handvest erkende rechten en vrijheden moeten bij wet worden gesteld en de wezenlijke inhoud van die rechten en vrijheden eerbiedigen. Met inachtneming van het evenredigheidsbeginsel kunnen slechts beperkingen worden gesteld, indien zij noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen ».

Artikel 52, lid 3, van het Handvest bepaalt :

« Voor zover dit Handvest rechten bevat die corresponderen met rechten welke zijn gegarandeerd door het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, zijn de inhoud en reikwijdte ervan dezelfde als die welke er door genoemd verdrag aan worden toegekend. Deze bepaling verhindert niet dat het recht van de Unie een ruimere bescherming biedt ».

B.11.3. De Grondwetgever heeft gestreefd naar een zo groot mogelijke concordantie tussen artikel 22 van de Grondwet en artikel 8 van het Europees Verdrag voor de rechten van de mens (*Parl. St.*, Kamer, 1992-1993, nr. 997/5, p. 2).

De draagwijdte van dat artikel 8 is analoog aan die van de voormelde grondwetsbepaling, zodat de waarborgen die beide bepalingen bieden, een onlosmakelijk geheel vormen.

Wanneer het Handvest rechten bevat die corresponderen met rechten die zijn gewaarborgd door het Europees Verdrag voor de rechten van de mens, « zijn de inhoud en reikwijdte ervan dezelfde als die welke er door genoemd verdrag aan worden toegekend ». Die bepaling stemt de inhoud en reikwijdte van de door het Handvest gewaarborgde rechten af op de corresponderende rechten die worden gewaarborgd door het Europees Verdrag voor de rechten van de mens.

In de toelichtingen bij het Handvest (2007/C 303/02), bekendgemaakt in het *Publicatieblad* van 14 december 2007, wordt aangegeven dat, onder de artikelen « met dezelfde inhoud en reikwijdte als de daarmee corresponderende artikelen van het EVRM », artikel 7 van het Handvest correspondeert met artikel 8 van het Europees Verdrag voor de rechten van de mens.

Het Hof van Justitie herinnert in dat verband eraan dat « artikel 7 van het Handvest, inzake de eerbiediging van het privéleven en van het familie- en gezinsleven, rechten bevat die corresponderen met de [...] rechten [die worden gegarandeerd door artikel 8, lid 1, van het Europees Verdrag voor de rechten van de mens, ondertekend te Rome op 4 november 1950 (hierna : het EVRM),] en dat, overeenkomstig artikel 52, lid 3, van het Handvest, aan dat artikel 7 dus dezelfde inhoud en reikwijdte moeten worden toegekend als die welke aan artikel 8, lid 1, van het EVRM worden toegekend, zoals uitgelegd in de rechtspraak van het Europees Hof voor de Rechten van de Mens » (HvJ, 17 december 2015, C-419/14, *WebMindLicenses Kft.*, ECLI:EU:C:2015:832, punt 70; 14 februari 2019, C-345/17, *Buivids*, ECLI:EU:C:2019:122, punt 65).

Wat artikel 8 van het Handvest betreft, oordeelt het Hof van Justitie dat « zoals in artikel 52, lid 3, tweede zin, daarvan uitdrukkelijk wordt bepaald, [artikel 52, lid 3, eerste zin, van dat Handvest] niet [verhindert] dat het Unierecht een ruimere bescherming biedt dan het EVRM », en dat « artikel 8 van het Handvest van de grondrechten van de Europese Unie betrekking heeft op een ander grondrecht dan het in artikel 7 van het Handvest van de grondrechten van de Europese Unie geformuleerde grondrecht, dat geen equivalent heeft in het EVRM » (HvJ, grote kamer, 21 december 2016, C-203/15 en C-698/15, *Tele2 Sverige AB*, ECLI:EU:C:2016:970, punt 129).

Uit het voorgaande volgt dat, binnen de werkingssfeer van het Europees Unierecht, artikel 22 van de Grondwet, artikel 8 van het Europees Verdrag voor de rechten van de mens en artikel 7 van het Handvest analoge grondrechten waarborgen, net zoals artikel 8 van dat Handvest, dat specifiek de rechtsbescherming van persoonsgegevens beoogt.

B.12.1. Artikel 107/5 van de wet van 13 juni 2005, ingevoegd bij artikel 3 van de wet van 20 juli 2022, bepaalt dat het gebruik van versleuteling vrij is, onder voorbehoud van drie uitzonderingen die erin worden opgesomd.

B.12.2. De parlementaire voorbereiding van de bestreden bepaling maakt duidelijk dat de wetgever het gebruik van versleuteling heeft willen bevorderen, aangezien het een efficiënt systeem is om de veiligheid van de communicatie te waarborgen, hetgeen toelaat het privéleven, het wetenschappelijke en economische potentieel, de competitiviteit van de ondernemingen, het medisch geheim en het bedrijfsgeheim te vrijwaren (*Parl. St.*, Kamer, 2021-2022, DOC 55-2572/001, p. 17).

B.12.3. Artikel 107/5 van de wet van 13 juni 2005, zoals vervangen bij artikel 3 van de wet van 20 juli 2022, bepaalt uitzonderingen op het vrije gebruik van versleuteling, om te vermijden dat het gebruik ervan noodcommunicatie verhindert, met inbegrip van de identificatie van de oproepende lijn of het verstrekken van de identificatiegegevens van de oproeper (§ 2), om te vermijden dat een operator geen uitvoering kan geven aan een gericht verzoek van een bevoegde autoriteit, onder de bij de wet bepaalde voorwaarden, met als doel de identificatie van de eindgebruiker, de opsporing en de lokalisatie van niet voor het publiek toegankelijke communicatie (§ 3) en om te vermijden dat een buitenlandse operator, wiens eindgebruiker of abonnee zich op het Belgische grondgebied bevindt, de uitvoering van een verzoek van een bevoegde overheid verhindert, met dien verstande dat, in dat laatste geval, elk strijdig contractueel beding nietig is (§ 4).

B.12.4. Zoals in B.10.1 en B.10.2 is vermeld, hebben de grieven van de verzoekende partijen betrekking op de laatste twee uitzonderingen.

B.12.5. Die uitzonderingen beogen te vermijden dat het gebruik van versleuteling een operator verhindert te voldoen aan de verplichtingen inzake dataretentie die bij de wet zijn vastgesteld, met name in het geval van een gebruiker die een beroep zou hebben gedaan op de diensten van een buitenlandse operator (*ibid.*, pp. 19-21). Dat zijn legitieme doelstellingen in de zin van artikel 8 van het Europees Verdrag voor de rechten van de mens, van artikel 52, lid 1, van het Handvest en van artikel 15, lid 1, van de richtlijn 2002/58/EG, die bij de wet van 20 juli 2022 is omgezet.

B.13.1. Uit zowel het voormelde arrest van het Hof nr. 57/2021 als uit het voormelde arrest van het Hof van Justitie van 6 oktober 2020, waarop het is gebaseerd, blijkt dat artikel 15, lid 1, van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8 en 52, lid 1, van het Handvest, niet in de weg staat aan de bewaring van identificatiegegevens, van verkeersgegevens

en van locatiegegevens, met inachtneming van bepaalde voorwaarden, met name dat de betrokken maatregelen, krachtens duidelijke en nauwkeurige regels, erin voorzien dat de gegevens slechts worden bewaard indien aan de daarvoor geldende materiële en procedurele voorwaarden wordt voldaan, en dat de betrokken personen over effectieve waarborgen tegen het risico van misbruik beschikken.

B.13.2. Het Europees Hof voor de Rechten van de Mens oordeelde in verband met de bewaring van en toegang tot versleutelde internetcommunicatie (EHRM, 13 februari 2024, *Podchasov t. Rusland*, ECLI:CE:ECHR:2024:0213JUD003369619) :

« 63. In de context van het verzamelen en het verwerken van persoonsgegevens, is het van essentieel belang om duidelijke en gedetailleerde regels te hebben inzake de reikwijdte en toepassing van de maatregelen, alsook minimumwaarborgen inzake, onder andere, de duurtijd, de bewaring, het gebruik, de toegang van derden, procedures voor het behoud van de integriteit en vertrouwelijkheid van gegevens en procedures voor de vernietiging ervan, zodat er voldoende waarborgen zijn tegen het risico van misbruik en willekeur (*ibid.*, § 99; zie ook *P.N. t. Duitsland*, nr. 74440/17, § 62, 11 juni 2020). Het interne recht moet meer bepaald ervoor zorgen dat de bewaarde gegevens ter zake dienend en niet overmatig zijn uitgaande van de doeleinden waarvoor zij worden opgeslagen, en dat zij worden bewaard in een zodanige vorm dat de betrokkene hierdoor niet langer te identificeren is dan noodzakelijk is voor het doel waarvoor de gegevens zijn opgeslagen. Het interne recht moet ook afdoende waarborgen bevatten om de bewaarde persoonsgegevens op doeltreffende wijze te beschermen tegen oneigenlijk gebruik en misbruik (zie *S. en Marper*, voormeld, § 103). De essentiële beginselen inzake gegevensbescherming vereisen dat de bewaring van de gegevens evenredig moet zijn met het doel waarvoor zij werden verzameld en moet worden beperkt in de tijd (*ibid.*, § 107).

64. In de context van geheim toezicht, waarbij een bevoegdheid van de uitvoerende macht in het geheim wordt uitgeoefend, is er een duidelijk risico op willekeur. Om aan de vereiste van ‘ voorzienbaarheid ’ te voldoen, moet het interne recht voldoende duidelijk zijn om de burgers op een adequate manier aan te geven in welke omstandigheden en onder welke voorwaarden de overheid dergelijke maatregelen vermag te nemen. Daar de toepassing van maatregelen van geheim toezicht op communicatie in de praktijk aan de controle van de betrokkenen of van het grote publiek ontsnapt, zou het bovendien in strijd zijn met het beginsel van de rechtstaat indien de aan de uitvoerende macht of aan de rechter toegekende beoordelingsbevoegdheid niet aan grenzen zou zijn gebonden. De wet moet bijgevolg de omvang en de wijze van uitoefening van een dergelijke aan de bevoegde autoriteiten verleende discretionaire bevoegdheid voldoende duidelijk omschrijven om het individu naar behoren tegen willekeur te beschermen (zie *Roman Zakharov*, voormeld, §§ 229-30). Voor een gedetailleerde omschrijving van de waarborgen die de wet moet bevatten om te voldoen aan de vereisten met betrekking tot de ‘ kwaliteit van de wet ’ en om ervoor te zorgen dat maatregelen van geheim toezicht enkel worden toegepast wanneer zij ‘ nodig zijn in een democratische samenleving ’, zie *Roman Zakharov*, voormeld, §§ 231-34, en *Big Brother Watch and Others*, voormeld, §§ 335-39.

65. Het Hof herhaalt ten slotte dat de vertrouwelijkheid van de communicatie een essentieel element van het in artikel 8 vastgelegde recht op eerbiediging van het privéleven en

van de briefwisseling is. Aan gebruikers van telecommunicatie en internetdiensten dient te worden gewaarborgd dat hun privéleven en hun vrijheid van meningsuiting worden geëerbiedigd, hoewel een dergelijke waarborg niet absoluut kan zijn en soms moet wijken voor andere legitieme dwingende vereisten, zoals de bescherming van de openbare orde, het voorkomen van strafbare feiten of de bescherming van de rechten en vrijheden van anderen (zie *K.U. t. Finland*, nr. 2872/02, § 49, EHRM, 2008, en *Delfi AS t. Estland* [GK], nr. 64569/09, § 149, EHRM, 2015) » (eigen vertaling).

Het Europees Hof voor de Rechten van de Mens heeft in dat arrest geoordeeld dat de in het geding zijnde Russische wetgeving niet evenredig is aan de nagestreefde legitieme doelstellingen, namelijk de bescherming van de nationale veiligheid, de handhaving van de openbare orde en het voorkomen van strafbare feiten en de bescherming van de rechten van anderen. In de afweging die het Europees Hof voor de Rechten van de Mens maakt, werd de verplichting die krachtens de Russische wetgeving op de organisatoren van digitale communicatie rust om alle op verzoek van de bevoegde overheden bewaarde gegevens te ontcijferen, inclusief de inhoud van *end-to-end* versleutelde communicatie, onevenredig geacht wegens het risico dat het versleutelingsmechanisme wordt verzwakt voor alle gebruikers van digitale-communicatiediensten (EHRM, 13 februari 2024, *Podchasov t. Rusland*, voormeld, §§ 68-80).

B.13.3. In tegenstelling tot de Russische wetgeving die in het geding is in het arrest *Podchasov t. Rusland* zet artikel 107/5, §§ 3 en 4, van de wet van 13 juni 2005 aan tot het gebruik van versleuteling (§ 1) en beperkt het zich ertoe de nadere regels te bepalen omtrent de reikwijdte van de bevoegdheden van de operatoren inzake het gebruik van versleuteling, opdat een gericht verzoek van een bevoegde autoriteit, met als doel de identificatie van de eindgebruiker, de opsporing en de lokalisatie van niet voor het publiek toegankelijke communicatie, effectief mogelijk is, in het geval waarin bij een andere wetsbepaling in die mogelijkheid is voorzien en onder de voorwaarden bedoeld in artikel 15, lid 1, van de richtlijn 2002/58/EG.

De gegevens die dienen te worden bewaard om aan een gericht verzoek van een bevoegde overheid te kunnen voldoen, zijn bovendien nauwkeurig bepaald en hebben geen betrekking op de inhoud van de communicatie. Het blijkt niet in welk opzicht de in artikel 107/5, §§ 3 en 4, van de wet van 13 juni 2005 beoogde voorwaarden onevenredige gevolgen voor de gebruikers zouden veroorzaken.

B.13.4. In zoverre zij betrekking hebben op artikel 3 van de wet van 20 juli 2022, zijn het enige middel in de zaak nr. 7931 en het vijfde middel in de zaak nr. 7932 niet gegrond.

2. De gebruikte maatregelen op netwerkniveau of op het niveau van de eindgebruiker om fraude en kwaadwillig gebruik van de netwerken en diensten op de sporen (artikel 4)

B.14. Het zesde middel in de zaak nr. 7932 heeft betrekking op artikel 4 van de wet van 20 juli 2022, waarbij in de wet van 13 juni 2005 een artikel 121/8 wordt ingevoegd, dat als volgt luidt :

« § 1. Zonder kennis te nemen van de inhoud van de communicatie, treffen de operatoren de gepaste, evenredige, preventieve en curatieve maatregelen, rekening houdende met de meest recente technische mogelijkheden, om fraude en kwaadwillig gebruik op hun netwerken en diensten op te sporen en om te vermijden dat de eindgebruikers schade lijden of lastiggevallen worden.

De Koning kan de door de operatoren krachtens het eerste lid te treffen maatregelen preciseren.

Het Instituut is bevoegd om bindende instructies te geven, met inbegrip van instructies betreffende de uitvoeringstermijnen, met het oog op de toepassing van deze paragraaf.

§ 2. Wanneer dat gerechtvaardigd is ten aanzien van de ernst van de omstandigheden, die per geval onderzocht moeten worden, kunnen de in paragraaf 1, eerste lid, bedoelde gepaste maatregelen met name het volgende omvatten :

- maatregelen op netwerkniveau, zoals de blokkering van nummers, diensten, URL's, domeinnamen, IP-adressen of elk ander element ter identificatie van de elektronische communicatie;

- maatregelen op het niveau van de eindgebruiker, zoals de volledige of gedeeltelijke deactivering van bepaalde diensten of apparatuur ».

B.15.1. De verzoekende partijen voeren aan dat artikel 121/8, § 2, van de wet van 13 juni 2005, ingevoegd bij artikel 4 van de wet van 20 juli 2022, niet bestaanbaar is met de artikelen 10, 11, 22 en 29 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 5, 6, 8, 9, 10, 11, 14, 15, 17 en 18 van het Europees Verdrag voor de rechten van de mens, met de artikelen 7, 8, 11, 47 en 52 van het Handvest en met de richtlijn 2002/58/EG. Volgens hen kunnen blokkerings- en deactiveringsmaatregelen worden toegepast voor ruimere doeleinden dan die bedoeld in artikel 121/8, § 1, van de wet van 13 juni 2005, met name voor censuur.

Bovendien is er geen enkele evaluatie door een onafhankelijk orgaan noch enig evaluatiecriterium vastgesteld om na te gaan of die maatregelen passen in de doeleinden bepaald in voormeld artikel 121/8, § 1. Bijgevolg schendt artikel 121/8, § 2, van de wet van 13 juni 2005, volgens de verzoekende partijen, de vrijheid van meningsuiting en van informatie.

B.15.2. Uit het voorgaande blijkt dat de verzoekende partijen grieven formuleren tegen artikel 4 van de wet van 20 juli 2022 wat betreft de vrijheid van meningsuiting en van informatie.

B.15.3. Artikel 10 van het Europees Verdrag voor de rechten van de mens bepaalt :

« 1. Eenieder heeft recht op vrijheid van meningsuiting. Dit recht omvat de vrijheid een mening te koesteren en de vrijheid om inlichtingen of denkbeelden te ontvangen of door te geven, zonder inmenging van overheidswege en ongeacht grenzen. Dit artikel belet niet dat Staten radio-omroep-, bioscoop- of televisie-ondernemingen kunnen onderwerpen aan een systeem van vergunningen.

2. Daar de uitoefening van deze vrijheden plichten en verantwoordelijkheden met zich brengt, kan zij worden onderworpen aan bepaalde formaliteiten, voorwaarden, beperkingen of sancties, welke bij de wet worden voorzien en die in een democratische samenleving nodig zijn in het belang van 's lands veiligheid, de bescherming van de openbare orde en het voorkomen van strafbare feiten, de bescherming van de gezondheid of de goede zeden, de bescherming van de goede naam of de rechten van anderen, om de verspreiding van vertrouwelijke mededelingen te voorkomen of om het gezag en de onpartijdigheid van de rechterlijke macht te waarborgen ».

Artikel 11 van het Handvest bepaalt :

« 1. Eenieder heeft recht op vrijheid van meningsuiting. Dit recht omvat de vrijheid een mening te hebben en de vrijheid kennis te nemen en te geven van informatie of ideeën, zonder inmenging van enig openbaar gezag en ongeacht grenzen.

2. De vrijheid en de pluriformiteit van de media worden geëerbiedigd ».

B.15.4. In zoverre het recht op vrijheid van meningsuiting daarin wordt erkend, hebben artikel 10 van het Europees Verdrag voor de rechten van de mens en artikel 11, lid 1, van het Handvest een draagwijdte die analoog is aan die van artikel 19 van de Grondwet, waarin de vrijheid om op elk gebied zijn mening te uiten, wordt erkend.

De bij die bepalingen geboden waarborgen vormen derhalve een onlosmakelijk geheel.

B.15.5. Artikel 19 van de Grondwet bepaalt :

« De vrijheid van eredienst, de vrije openbare uitoefening ervan, alsmede de vrijheid om op elk gebied zijn mening te uiten, zijn gewaarborgd, behoudens bestraffing van de misdrijven die ter gelegenheid van het gebruikmaken van die vrijheden worden gepleegd ».

Artikel 19 van de Grondwet verbiedt dat de vrijheid van meningsuiting aan preventieve beperkingen wordt onderworpen, maar niet dat misdrijven die ter gelegenheid van het gebruikmaken van die vrijheid worden gepleegd, worden bestraft.

B.15.6. Het Hof betrekt bij zijn onderzoek van artikel 19 van de Grondwet, enkel artikel 10 van het Europees Verdrag voor de rechten van de mens en de artikelen 11 en 52 van het Handvest, aangezien er over de schending van de andere in B.15.1 vermelde bepalingen geen enkele uiteenzetting is.

B.16.1. De vrijheid van meningsuiting kan, krachtens artikel 10, lid 2, van het Europees Verdrag voor de rechten van de mens, onder bepaalde voorwaarden worden onderworpen aan formaliteiten, voorwaarden, beperkingen of sancties, met het oog op de nationale veiligheid, de territoriale integriteit, de openbare veiligheid, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden, de bescherming van de goede naam of de rechten van anderen, om de verspreiding van vertrouwelijke mededelingen te voorkomen of om het gezag en de onpartijdigheid van de rechterlijke macht te waarborgen. De uitzonderingen waarmee zij gepaard gaat, dienen echter « eng te worden geïnterpreteerd, en de noodzaak om haar te beperken moet op overtuigende wijze worden aangetoond » (EHRM, grote kamer, 20 oktober 2015, *Pentikäinen t. Finland*, ECLI:CE:ECHR:2015:1020JUD001188210, § 87).

B.16.2. Een inmenging in de vrijheid van meningsuiting dient te worden vastgesteld bij een voldoende toegankelijke en nauwkeurige wet. Zij dient aldus in duidelijke en voldoende nauwkeurige bewoordingen te worden geformuleerd die het mogelijk maken dat eenieder - desnoods met gepast advies - in de gegeven context in redelijke mate de gevolgen van zijn handelen kan voorzien. Die vereisten dienen evenwel niet te leiden tot overdreven rigiditeit die zou verhinderen dat bij de interpretatie van een wetskrachtige norm rekening wordt gehouden met veranderende omstandigheden of opvattingen (EHRM, grote kamer, 22 oktober 2007, *Lindon, Otchakovsky-Laurens en July t. Frankrijk*,

ECLI:CE:ECHR:2007:1022JUD002127902, § 41; grote kamer, 7 juni 2012, *Centro Europa 7 S.r.l. en Di Stefano t. Italië*, ECLI:CE:ECHR:2012:0607JUD003843309, §§ 141-142; grote kamer, 15 oktober 2015, *Perinçek t. Zwitserland*, ECLI:CE:ECHR:2015:1015JUD002751008, §§ 131-133). Voorts moet worden aangetoond dat de beperking noodzakelijk is in een democratische samenleving, aan een dwingende maatschappelijke behoefte beantwoordt en evenredig is aan de wettige doelstellingen die daarmee worden nagestreefd.

B.17. Uit de parlementaire voorbereiding blijkt dat de wetgever met artikel 121/8, § 2, van de wet van 13 juni 2005, ingevoegd bij artikel 4 van de wet van 20 juli 2022, het hoofd wou bieden aan de situatie waarin de eindgebruiker van het communicatienetwerk het slachtoffer is van fraude, door de operatoren aan te sporen ten gunste van die gebruiker te reageren en door erin te voorzien dat in ernstige gevallen van fraude of kwaadwillig gebruik van een netwerk snelle en « krachtige maatregelen » kunnen worden genomen. In dat kader heeft de opsomming van de in dat artikel beoogde blokkerings- en deactiveringsmaatregelen ook als doel een grotere rechtszekerheid aan de operatoren te bieden (*Parl. St.,* Kamer, 2021-2022, DOC 55-2572/001, pp. 21-22).

Die doelstellingen zijn legitiem en kunnen een beperkingsgrond voor de vrijheid van meningsuiting vormen. Er dient nog te worden onderzocht of de bestreden maatregel relevant en evenredig is ten aanzien van die doelstellingen.

B.18. Om ernstige gevallen van fraude of kwaadwillig gebruik van het netwerk ten nadele van de eindgebruiker te vermijden, vermocht de wetgever te voorzien in de mogelijkheid om de bij artikel 121/8, § 2, beoogde maatregelen te nemen, aangezien daarmee de voormelde doelstellingen kunnen worden bereikt. Bovendien tonen de verzoekende partijen niet aan in welk opzicht die maatregelen niet pertinent zijn ten aanzien van die doelstellingen.

B.19.1. Ten slotte gaan de in artikel 121/8, § 2, van de wet van 13 juni 2005 beoogde maatregelen niet verder dan nodig om de door de wetgever nagestreefde doelstellingen te realiseren.

B.19.2. Allereerst worden de begrippen « fraude » en « kwaadwillig gebruik van het netwerk of van de dienst » gedefinieerd in artikel 2, 5/5° en 5/6°, van de wet van 13 juni 2005,

zoals gewijzigd bij artikel 2 van de wet van 20 juli 2022. Krachtens die bepalingen komt fraude neer op « een oneerlijke daad gepleegd met de bedoeling om te misleiden, indruisend tegen de wet, de reglementen of een contract, om voor zichzelf of iemand anders een onrechtmatig voordeel te verkrijgen, ten nadele van de operator of eindgebruiker, via het gebruik van een elektronische-communicatiedienst » (5/5°), terwijl het kwaadwillig gebruik van het netwerk of van de dienst bestaat in het « gebruik van het elektronische-communicatienetwerk of van de elektronische-communicatiedienst om overlast te veroorzaken aan zijn correspondent of om schade te berokkenen » (5/6°).

B.19.3. Het staat aan de operatoren om fraude of kwaadwillig gebruik van het netwerk of van de dienst op te sporen en, geval per geval, « de ernst van de omstandigheden » te beoordelen alvorens de bij artikel 121/8, § 2, van de wet van 13 juni 2005, zoals ingevoegd bij artikel 4 van de wet van 20 juli 2022, bepaalde maatregelen te kunnen nemen. Uit de parlementaire voorbereiding van de bestreden bepaling blijkt dat, in die hypothese, de operatoren ofwel op eigen initiatief, ofwel ingevolge een melding van de eindgebruiker of van een derde handelen; het is voor de operatoren in ieder geval verboden om kennis te nemen van de inhoud van de communicatie (*Parl. St.,* Kamer, 2021-2022, DOC 55-2572/003, pp. 85-87).

In dat kader handelen de operatoren onder het toezicht van het Belgisch Instituut voor Postdiensten en Telecommunicatie (hierna : het BIPT), dat, krachtens artikel 14, § 1, 3°, *a)*, van de wet van 17 januari 2003, ermee belast is de naleving van de wet van 13 juni 2005 en van de uitvoeringsbesluiten ervan te controleren. Artikel 121/8 van de wet van 13 juni 2005 voegt eraan toe dat het BIPT « bevoegd [is] om bindende instructies te geven, met inbegrip van instructies betreffende de uitvoeringstermijnen » (§ 1, derde lid), wat betreft de maatregelen die door de operatoren worden genomen op basis van die bepaling.

Naar aanleiding van het toezicht dat het uitoefent op de maatregelen die door de operatoren worden genomen op basis van artikel 121/8, § 2, van de wet van 13 juni 2005, gaat het BIPT met name het bestaan van fraude of van kwaadwillig gebruik van het netwerk, het gepaste en evenredige karakter van de maatregel, alsook de ernst van de omstandigheden van het geval na.

Ten slotte kan, krachtens artikel 2, § 1, van de wet van 17 januari 2003 « betreffende de rechtsmiddelen en de geschillenbehandeling naar aanleiding van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en

telecommunicatiesector », tegen de besluiten van het BIPT « beroep met volle rechtsmacht worden ingesteld bij het Marktenhof, rechtsprekend zoals in kort geding », met dien verstande dat « iedere persoon die een belang heeft om op te treden, [...] het [...] beroep [mag] indienen ».

B.20. Het zesde middel in de zaak nr. 7932 is niet gegrond.

3. Het bewaren van de verkeersgegevens (artikel 5)

B.21.1. Het eerste en tweede middel in de zaak nr. 7930, het enige middel in de zaak nr. 7931, het eerste onderdeel van het eerste middel en het eerste onderdeel van het derde middel in de zaak nr. 7932 hebben betrekking op artikel 5 van de wet van 20 juli 2022, dat bepaalt :

« In artikel 122 van [de wet van 13 juni 2005], laatstelijk gewijzigd bij de wet van 21 december 2021, worden de volgende wijzigingen aangebracht :

1° in paragraaf 1 wordt het tweede lid opgeheven;

2° in paragraaf 2 worden de volgende wijzigingen aangebracht :

a) het eerste lid wordt vervangen als volgt :

‘ In afwijking van paragraaf 1 en met als enig doel de facturering van abonnees of het doen van interconnectiebetalingen, mogen de operatoren de daartoe noodzakelijke verkeersgegevens bewaren en verwerken. ’;

b) in het tweede lid worden de woorden ‘ van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens ’ vervangen door de woorden ‘ van de AVG en van de wet van 30 juli 2018 ’;

c) in het derde lid wordt het woord ‘ opgesomd ’ vervangen door het woord ‘ bedoeld ’;

3° in paragraaf 3 worden de volgende wijzigingen aangebracht :

a) in het eerste lid, 2°, worden de woorden ‘ de vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene of zijn wettelijke vertegenwoordiger aanvaardt dat verkeersgegevens die op hem betrekking hebben worden verwerkt ’ vervangen door de woorden ‘ de toestemming in de zin van artikel 4, 11), van de AVG ’;

b) in het eerste lid, 3°, worden de woorden ‘ op eenvoudige wijze ’ vervangen door de woorden ‘ makkelijk en te allen tijde ’;

c) in het tweede lid worden de woorden ‘ van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens ’ vervangen door de woorden ‘ van de AVG en van de wet van 30 juli 2018 ’;

4° paragraaf 4 wordt vervangen als volgt :

‘ § 4. In afwijking van paragraaf 1, teneinde de gepaste maatregelen bedoeld in artikel 121/8, § 1, te kunnen nemen en om fraude of kwaadwillig gebruik van het netwerk of de dienst te kunnen vaststellen of om de dader en de herkomst ervan te kunnen identificeren, en voor zover hij deze verwerkt of genereert in het kader van de verstrekking van dat netwerk of van die dienst :

1° bewaart de operator, in het kader van de verstrekking van een interpersoonlijke communicatiedienst en gedurende vier maanden vanaf de datum van de communicatie, de daartoe noodzakelijke verkeersgegevens onder de volgende verkeersgegevens :

- de identifier van de bron van de communicatie;

- de identifier van de bestemming van de communicatie;

- de precieze datums en tijdstippen van het begin en het einde van de communicatie;

- de locatie van de eindapparatuur van de communicerende partijen bij de aanvang en bij het einde van de communicatie;

2° bewaart de operator gedurende twaalf maanden vanaf de datum van de communicatie de volgende verkeersgegevens betreffende de binnenkomende communicatie in het kader van de verstrekking van interpersoonlijke communicatiediensten, teneinde de persoon die de communicatie doet, te identificeren :

- het telefoonnummer aan de bron van de binnenkomende communicatie, of;

- het IP-adres dat werd gebruikt om de binnenkomende communicatie te versturen, het tijdstempel en de gebruikte poort, en;

- de precieze datums en tijdstippen van begin en einde van de binnenkomende communicatie;

3° bewaart de operator de in 1° bedoelde gegevens die betrekking hebben op een specifieke geïdentificeerde fraude of een specifiek geïdentificeerd kwaadwillig gebruik van het netwerk gedurende de periode die nodig is voor de analyse en het verhelpen ervan, in voorkomend geval langer dan de termijn van vier maanden bedoeld in 1°;

4° bewaart de operator de verkeersgegevens bedoeld in 2° en met betrekking tot een specifiek kwaadwillig gebruik van het netwerk gedurende de periode die nodig is voor de verwerking van dit kwaadwillig gebruik, in voorkomend geval langer dan de termijn van twaalf maanden bedoeld in 2°;

5° verwerkt de operator de noodzakelijke verkeersgegevens voor deze doeleinden, met inbegrip van de gegevens bedoeld in paragraaf 2 indien nodig.

In afwijking van paragraaf 1, teneinde de gepaste maatregelen bedoeld in artikel 121/8, § 1, te kunnen nemen, om fraude of kwaadwillig gebruik van het netwerk of de dienst te kunnen vaststellen of om de dader en de herkomst ervan te kunnen identificeren, mag de operator andere gegevens dan deze bedoeld in het eerste lid bewaren en verwerken, die voor deze doeleinden nodig worden geacht.

De Koning kan, bij een besluit vastgesteld na overleg in de Ministerraad en na advies van het Instituut en van de Gegevensbeschermingsautoriteit, de verkeersgegevens waarvan de bewaring als noodzakelijk moet worden beschouwd voor het nastreven van de in deze paragraaf bedoelde doeleinden, preciseren en uitbreiden.

In geval van vermeende fraude of van vermeend kwaadwillig gebruik, kunnen de operatoren aan de bevoegde autoriteiten alle wettelijk bewaarde gegevens in verband met de vermeende fraude of het vermeende kwaadwillig gebruik doorsturen. ';

5° een paragraaf 4/1 wordt ingevoegd, luidende :

' § 4/1. In afwijking van paragraaf 1 mogen de operatoren die verkeersgegevens bewaren en verwerken die nodig zijn om de veiligheid en correcte werking van hun elektronische-communicatienetwerken en -diensten te garanderen, en in het bijzonder om een mogelijke of werkelijke aanslag op die veiligheid op te sporen en te analyseren, inclusief om de oorsprong van die aanslag te identificeren.

De operatoren mogen deze bewaren voor een duur van twaalf maanden vanaf de datum van de communicatie.

De operatoren mogen de in het eerste lid bedoelde gegevens met betrekking tot een specifieke schending van de veiligheid van het netwerk bewaren gedurende de periode die nodig is om deze te behandelen, in voorkomend geval langer dan de termijn van twaalf maanden bedoeld in het tweede lid.

In geval van schending van de veiligheid van hun elektronische-communicatienetwerken en -diensten, kunnen de operatoren aan de bevoegde autoriteiten alle wettelijk bewaarde gegevens in verband met de schending van de veiligheid van hun elektronische-communicatienetwerken en -diensten doorsturen. ';

6° een paragraaf 4/2 wordt ingevoegd, luidende :

' § 4/2. In afwijking van paragraaf 1 bewaren en verwerken de operatoren de verkeersgegevens die nodig zijn om te voldoen aan een verplichting opgelegd krachtens een formele wettelijke norm, voor de daartoe benodigde duur. ';

7° paragraaf 5 wordt vervangen als volgt :

' § 5. De gegevens vermeld in dit artikel mogen alleen worden verwerkt door personen die in opdracht van de operator belast zijn met de facturering of het beheer van het verkeer, de behandeling van verzoeken om inlichtingen van abonnees, de bestrijding van fraude of het kwaadwillig gebruik van het netwerk, de veiligheid van het netwerk, de naleving van zijn wettelijke verplichtingen, de marketing van de eigen elektronische-communicatiediensten of de

levering van diensten die gebruik maken van verkeersgegevens of locatiegegevens en door de leden van zijn Coördinatiecel bedoeld in artikel 127/3. ';

8° in paragraaf 6 worden de woorden ' Het Instituut ' vervangen door de woorden ' Het Instituut, de Ombudsdienst voor telecommunicatie, ' ».

B.21.2. Ingevolge die wijziging bepaalt artikel 122 van de wet van 13 juni 2005 :

« § 1. De operatoren verwijderen de verkeersgegevens met betrekking tot abonnees of eindgebruikers uit hun verkeersgegevens of maken deze gegevens anoniem, zodra zij niet langer nodig zijn voor de transmissie van de communicatie.

§ 2. In afwijking van paragraaf 1 en met als enig doel de facturering van abonnees of het doen van interconnectiebetalingen, mogen de operatoren de daartoe noodzakelijke verkeersgegevens bewaren en verwerken.

Onverminderd de toepassing van de AVG en van de wet van 30 juli 2018 stelt de operator de abonnee of, in voorkomend geval, de eindgebruiker waarop de gegevens betrekking hebben, voorafgaand aan de verwerking in kennis van :

1° de soorten verkeersgegevens die worden verwerkt;

2° de precieze doeleinden van de verwerking;

3° de duur van de verwerking.

De verwerking van de gegevens bedoeld in het eerste lid, is slechts toegestaan tot het einde van de periode van de betwisting van de factuur of tot het einde van de periode waarin de betaling gerechtelijk kan worden afgedwongen.

§ 3. In afwijking van § 1 en met als enig doel de marketing te verzorgen van de eigen elektronische-communicatiediensten[,] het gebruikspatroon bedoeld in artikel 110, § 4, eerste lid, artikel 110/1 en artikel 111, § 3, tweede lid, op te stellen, of diensten met verkeersgegevens of locatiegegevens te leveren, mogen de operatoren de in § 1 bedoelde gegevens slechts verwerken onder de volgende voorwaarden :

1° De operator stelt de abonnee of, in voorkomend geval, de eindgebruiker waarop de gegevens betrekking hebben, voorafgaand aan het verkrijgen van diens toestemming voor de verwerking, in kennis van :

a) de soorten verkeersgegevens die worden verwerkt;

b) de precieze doeleinden van de verwerking;

c) de duur van verwerking.

2° De abonnee of, in voorkomend geval, de eindgebruiker, heeft voorafgaand aan de verwerking zijn toestemming gegeven voor de verwerking.

Onder toestemming voor de verwerking in de zin van dit artikel wordt verstaan de toestemming in de zin van artikel 4, 11), van de AVG.

3° De betrokken operator biedt zijn abonnees of eindgebruikers gratis de mogelijkheid om makkelijk en te allen tijde de gegeven toestemming in te trekken.

4° De verwerking van de betrokken gegevens blijft beperkt tot de handelingen en de duur die nodig zijn voor de levering van de betrokken dienst met verkeersgegevens of locatiegegevens voor het opstellen van het gebruikspatroon bedoeld in artikel 110, § 4, eerste lid, artikel 110/1 en artikel 111, § 3, tweede lid, of voor de marketingactie in kwestie.

Deze voorwaarden zijn van toepassing onverminderd de bijkomende voorwaarden die voortvloeien uit de toepassing van de AVG en van de wet van 30 juli 2018.

§ 4. In afwijking van paragraaf 1, teneinde de gepaste maatregelen bedoeld in artikel 121/8, § 1, te kunnen nemen en om fraude of kwaadwillig gebruik van het netwerk of de dienst te kunnen vaststellen of om de dader en de herkomst ervan te kunnen identificeren, en voor zover hij deze verwerkt of genereert in het kader van de verstrekking van dat netwerk of van die dienst :

1° bewaart de operator, in het kader van de verstrekking van een interpersoonlijke communicatiedienst en gedurende vier maanden vanaf de datum van de communicatie, de daartoe noodzakelijke verkeersgegevens onder de volgende verkeersgegevens :

- de identifier van de bron van de communicatie;

- de identifier van de bestemming van de communicatie;

- de precieze datums en tijdstippen van het begin en het einde van de communicatie;

- de locatie van de eindapparatuur van de communicerende partijen bij de aanvang en bij het einde van de communicatie;

2° bewaart de operator gedurende twaalf maanden vanaf de datum van de communicatie de volgende verkeersgegevens betreffende de binnenkomende communicatie in het kader van de verstrekking van interpersoonlijke communicatiediensten, teneinde de persoon die de communicatie doet, te identificeren :

- het telefoonnummer aan de bron van de binnenkomende communicatie, of;

- het IP-adres dat werd gebruikt om de binnenkomende communicatie te versturen, het tijdstempel en de gebruikte poort, en;

- de precieze datums en tijdstippen van begin en einde van de binnenkomende communicatie;

3° bewaart de operator de in 1° bedoelde gegevens die betrekking hebben op een specifieke geïdentificeerde fraude of een specifiek geïdentificeerd kwaadwillig gebruik van het netwerk gedurende de periode die nodig is voor de analyse en het verhelpen ervan, in voorkomend geval langer dan de termijn van vier maanden bedoeld in 1°;

4° bewaart de operator de verkeersgegevens bedoeld in 2° en met betrekking tot een specifiek kwaadwillig gebruik van het netwerk gedurende de periode die nodig is voor de verwerking van dit kwaadwillig gebruik, in voorkomend geval langer dan de termijn van twaalf maanden bedoeld in 2°;

5° verwerkt de operator de noodzakelijke verkeersgegevens voor deze doeleinden, met inbegrip van de gegevens bedoeld in paragraaf 2 indien nodig.

In afwijking van paragraaf 1, teneinde de gepaste maatregelen bedoeld in artikel 121/8, § 1, te kunnen nemen, om fraude of kwaadwillig gebruik van het netwerk of de dienst te kunnen vaststellen of om de dader en de herkomst ervan te kunnen identificeren, mag de operator andere gegevens dan deze bedoeld in het eerste lid bewaren en verwerken, die voor deze doeleinden nodig worden geacht.

De Koning kan, bij een besluit vastgesteld na overleg in de Ministerraad en na advies van het Instituut en van de Gegevensbeschermingsautoriteit, de verkeersgegevens waarvan de bewaring als noodzakelijk moet worden beschouwd voor het nastreven van de in deze paragraaf bedoelde doeleinden, preciseren en uitbreiden.

In geval van vermeende fraude of van vermeend kwaadwillig gebruik, kunnen de operatoren aan de bevoegde autoriteiten alle wettelijk bewaarde gegevens in verband met de vermeende fraude of het vermeende kwaadwillig gebruik doorsturen.

§ 4/1. In afwijking van paragraaf 1 mogen de operatoren die verkeersgegevens bewaren en verwerken die nodig zijn om de veiligheid en correcte werking van hun elektronische-communicatienetwerken en -diensten te garanderen, en in het bijzonder om een mogelijke of werkelijke aanslag op die veiligheid op te sporen en te analyseren, inclusief om de oorsprong van die aanslag te identificeren.

De operatoren mogen deze bewaren voor een duur van twaalf maanden vanaf de datum van de communicatie.

De operatoren mogen de in het eerste lid bedoelde gegevens met betrekking tot een specifieke schending van de veiligheid van het netwerk bewaren gedurende de periode die nodig is om deze te behandelen, in voorkomend geval langer dan de termijn van twaalf maanden bedoeld in het tweede lid.

In geval van schending van de veiligheid van hun elektronische-communicatienetwerken en -diensten, kunnen de operatoren aan de bevoegde autoriteiten alle wettelijk bewaarde gegevens in verband met de schending van de veiligheid van hun elektronische-communicatienetwerken en -diensten doorsturen.

§ 4/2. In afwijking van paragraaf 1 bewaren en verwerken de operatoren de verkeersgegevens die nodig zijn om te voldoen aan een verplichting opgelegd krachtens een formele wettelijke norm, voor de daartoe benodigde duur.

§ 5. De gegevens vermeld in dit artikel mogen alleen worden verwerkt door personen die in opdracht van de operator belast zijn met de facturering of het beheer van het verkeer, de behandeling van verzoeken om inlichtingen van abonnees, de bestrijding van fraude of het

kwaadwillig gebruik van het netwerk, de veiligheid van het netwerk, de naleving van zijn wettelijke verplichtingen, de marketing van de eigen elektronische-communicatiediensten of de levering van diensten die gebruik maken van verkeersgegevens of locatiegegevens en door de leden van zijn Coördinatiecel bedoeld in artikel 127/3.

§ 6. Het Instituut, de Ombudsdienst voor telecommunicatie, de Belgische Mededingingsautoriteit, de rechtscolleges van de rechterlijke orde en de Raad van State kunnen in het kader van hun bevoegdheden in kennis worden gesteld van de relevante verkeers- en rekeninggegevens met het oog op het beslechten van geschillen, waaronder geschillen met betrekking tot interconnectie en facturering ».

B.22.1. De verzoekende partij in de zaak nr. 7930 leidt een eerste en een tweede middel af uit de schending van de artikelen 11, 12, 22 en 29 van de Grondwet, van artikel 15, lid 1, en van de artikelen 5, 6 en 9 van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8, 11, 47 en 52, lid 1, van het Handvest, van de artikelen 6, 8, 10, 11 en 18 van het Europees Verdrag voor de rechten van de mens en van de artikelen 13 en 54 van de richtlijn (EU) 2016/680, in zoverre artikel 5, 4° en 5°, van de wet van 20 juli 2022 een algemene verplichting tot bewaring van communicatiegegevens invoert, zonder dat die bewaring noodzakelijk en strikt beperkt is ten aanzien van het nagestreefde doel. De verzoekende partij formuleert geen uitdrukkelijke grief tegen artikel 5, 1° tot 3° en 6° tot 8°.

B.22.2. De verzoekende partij in de zaak nr.7931 leidt een enig middel af uit de schending van de artikelen 11, 12, 22 en 29 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 7, 8, 11, 47 en 52, lid 1, van het Handvest, met artikel 8 van het Europees Verdrag voor de rechten van de mens, met de artikelen 5, 6 en 15 van de richtlijn 2002/58/EG en met de artikelen 13 en 54 van de richtlijn (EU) 2016/680. Zij voert aan dat artikel 5, 4°, van de wet van 20 juli 2022 voorziet in een verplichting tot het systematisch en ongedifferentieerd bewaren van bepaalde gegevens om de criminaliteit in het algemeen te bestrijden, terwijl een dergelijke bewaring slechts is toegelaten in het kader van de strijd tegen zware criminaliteit, en in zoverre de bewaarplicht die het invoert in elk geval onevenredig is.

In ondergeschikte orde vraagt de verzoekende partij om een prejudiciële vraag te stellen aan het Hof van Justitie. Bovendien is artikel 5, 5°, van de wet van 20 juli 2022 volgens de verzoekende partij niet noodzakelijk ten aanzien van de andere verplichtingen die op de operatoren rusten en voorziet het in een te lange bewaartermijn.

B.22.3. De verzoekende partijen in de zaak nr. 7932 leiden een eerste middel af uit de schending van de artikelen 10, 11, 13, 15, 22, 23 en 29 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 5, 6, 8, 9, 10, 11, 14 en 18 van het Europees Verdrag voor de rechten van de mens, met de artikelen 7, 8, 11, 47 en 52 van het Handvest, met artikel 5, lid 4, van het Verdrag betreffende de Europese Unie en met artikel 6 van de richtlijn 2002/58/EG, met de richtlijn (EU) 2016/680 en met de AVG. In het eerste onderdeel van dat middel voeren de verzoekende partijen aan dat artikel 5, 4° en 5°, van de wet van 20 juli 2022 voorziet in een algemene en ongedifferentieerde bewaring van gegevens die slechts toelaatbaar is in het kader van de bescherming van de nationale veiligheid, zonder dat erin is voorzien dat de bewaarde gegevens worden verwijderd of anoniem worden gemaakt wanneer de bewaring niet meer noodzakelijk is. Bovendien voorziet artikel 5 van de wet van 20 juli 2022 in een identieke verwerking van alle gegevens, zonder een onderscheid te maken op basis van de finaliteit (strijd tegen zware criminaliteit).

Dezelfde verzoekende partijen leiden een derde middel af uit de schending van de artikelen 10, 11, 15, 22 en 29 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 5, 6, 8, 9, 10, 11, 14 en 18 van het Europees Verdrag voor de rechten van de mens, met de artikelen 7, 8, 11, 47 en 52 van het Handvest, met artikel 5, lid 4, van het Verdrag betreffende de Europese Unie, alsook met de richtlijn 2002/58/EG, met de richtlijn (EU) 2016/680 en met de AVG. In het eerste onderdeel van dat middel, stellen zij dat artikel 5, 4°, van de wet van 20 juli 2022 een verplichting tot algemene en ongedifferentieerde bewaring van gegevens creëert om te strijden tegen fraude en kwaadwillig gebruik van het netwerk of van de dienst, ten gunste van de operatoren in het kader van hun opdrachten, hetgeen te vaag en te ruim is.

B.23. Uit het voorgaande volgt dat de grieven van de verzoekende partijen betrekking hebben op artikel 5, 4° en 5°, van de wet van 20 juli 2022. Bovendien zijn die grieven hoofdzakelijk afgeleid uit de schending van het recht op eerbiediging van het privéleven en van het recht op bescherming van de persoonsgegevens, gewaarborgd bij artikel 22 van de Grondwet, bij artikel 8 van het Europees Verdrag voor de rechten van de mens, bij de artikelen 7, 8 en 52, lid 1, van het Handvest, bij de richtlijn 2002/58/EG, bij de richtlijn (EU) 2016/680 en bij de AVG.

B.24.1. Bij artikel 22 van de Grondwet wordt aan de bevoegde wetgever de bevoegdheid voorbehouden om te bepalen in welke gevallen en onder welke voorwaarden afbreuk kan worden gedaan aan het recht op eerbiediging van het privéleven. Het waarborgt aldus aan elke burger dat geen inmenging in de uitoefening van dat recht kan plaatsvinden dan krachtens regels die zijn aangenomen door een democratisch verkozen beraadslagende vergadering.

Een delegatie aan een andere macht is evenwel niet in strijd met het wettigheidsbeginsel, voor zover de machtiging voldoende nauwkeurig is omschreven en betrekking heeft op de tenuitvoerlegging van maatregelen waarvan de essentiële elementen vooraf door de wetgever zijn vastgesteld.

Bijgevolg moeten de essentiële elementen van de verwerking van persoonsgegevens in de wet, het decreet of de ordonnantie zelf worden vastgelegd. In dat verband maken de volgende elementen, ongeacht de aard van de betrokken gelegenheid, in beginsel essentiële elementen uit : (1) de categorie van verwerkte gegevens, (2) de categorie van betrokken personen, (3) de met de verwerking nagestreefde doelstelling, (4) de categorie van personen die toegang hebben tot de verwerkte gegevens en (5) de maximumtermijn voor het bewaren van de gegevens.

B.24.2. Naast het formele wettigheidsvereiste legt artikel 22 van de Grondwet, in samenhang gelezen met artikel 8 van het Europees Verdrag voor de rechten van de mens en met de artikelen 7, 8 en 52 van het Handvest, de verplichting op dat de inmenging in het recht op eerbiediging van het privéleven en in het recht op bescherming van persoonsgegevens in duidelijke en voldoende nauwkeurige bewoordingen wordt geformuleerd die het mogelijk maken de hypothesen te voorzien waarin de wetgever een dergelijke inmenging toestaat.

Inzake de bescherming van de persoonsgegevens impliceert dat vereiste van voorzienbaarheid dat voldoende precies moet worden bepaald in welke omstandigheden de verwerkingen van persoonsgegevens zijn toegelaten (EHRM, grote kamer, 4 mei 2000, *Rotaru t. Roemenië*, ECLI:CE:ECHR:2000:0504JUD002834195, § 57; grote kamer, 4 december 2008, *S. en Marper t. Verenigd Koninkrijk*, ECLI:CE:ECHR:2008:1204JUD003056204, § 99). Het vereiste dat de beperking bij wet dient te worden ingesteld, houdt met name in dat de rechtsgrond die de inmenging in die rechten toestaat, zelf de reikwijdte van de beperking van de uitoefening van het betrokken recht moet bepalen (HvJ, 6 oktober 2020, C-623/17, *Privacy International*, ECLI:EU:C:2020:790, punt 65).

Derhalve moet eenieder een voldoende duidelijk beeld kunnen hebben van de verwerkte gegevens, de bij een bepaalde gegevensverwerking betrokken personen en de voorwaarden voor en de doeleinden van de verwerking.

B.25. Uit de parlementaire voorbereiding van artikel 5, 4° en 5°, van de wet van 20 juli 2022 blijkt dat het artikel met name beoogt artikel 15 van de richtlijn 2002/58/EG om te zetten, in zoverre dat artikel 15 afwijkt van artikel 6, lid 5, van die richtlijn en het de lidstaten toelaat maatregelen te nemen om de voorkoming, het onderzoek, de opsporing en de vervolging van niet toegestaan gebruik van het elektronische-communicatiesysteem te waarborgen (*Parl. St.,* Kamer, 2021-2022, DOC 55-2572/001, pp. 28, 29, 36 en 37).

Die doelstellingen zijn legitiem in de zin van artikel 8 van het Europees Verdrag voor de rechten van de mens en artikel 52 van het Handvest.

In dat kader heeft de wetgever gepreciseerd dat het niet mogelijk was om te voorzien in een bewaring van gegevens « die reactief en doelgericht is van bij het begin » wegens de structuur zelf van de betrokken netwerken en diensten (*ibid.*, pp. 27 en 28). Hij was bovendien van oordeel dat het door artikel 5, 4° en 5°, van de wet van 20 juli 2022 bepaalde systeem voor de bewaring van verkeersgegevens bestaat « in het belang van de eindgebruikers van de diensten van de operator » (*ibid.*, p. 26) en ertoe strekt de slachtoffers van fraude of van kwaadwillig gebruik van het netwerk toe te laten de dader ervan te identificeren (*ibid.*, p. 28). Dat systeem wordt overigens voorgesteld als « [houdende] intrinsiek verband [...] met de verstrekking van de elektronische-communicatiedienst » (*ibid.*, p. 26) en als een manier om de wet van 13 juni 2005 te updaten rekening houdend met het toenemende belang van de doelstelling om fraude en kwaadwillig gebruik van het netwerk te bestrijden in het Unierecht (*ibid.*, p. 29).

B.26. Het staat aan het Hof om na te gaan of de inmenging die artikel 122, §§ 4 en 4/1, van de wet van 13 juni 2005, ingevoegd bij artikel 5, 4° en 5°, van de wet van 20 juli 2022, in het recht op eerbiediging van het privéleven en in het recht op bescherming van de persoonsgegevens met zich meebrengt, geen onevenredige gevolgen heeft voor de personen die het voorwerp uitmaken van de in die bepaling beoogde maatregelen.

B.27.1. Artikel 122, § 4, van de wet van 13 juni 2005 voorziet, ten laste van de operatoren, in een verplichting tot bewaring van verschillende verkeersgegevens « teneinde de gepaste maatregelen bedoeld in artikel 121/8, § 1, te kunnen nemen en om fraude of kwaadwillig gebruik van het netwerk of de dienst te kunnen vaststellen of om de dader en de herkomst ervan te kunnen identificeren », in zoverre de operatoren die gegevens verwerken « in het kader van de verstrekking van dat netwerk of van die dienst ».

B.27.2. De beoogde verkeersgegevens zijn « de identifier van de bron van de communicatie » « de identifier van de bestemming van de communicatie », de « precieze datums en tijdstippen van het begin en het einde van de communicatie » en « de locatie van de eindapparatuur van de communicerende partijen bij de aanvang en bij het einde van de communicatie » (eerste lid, 1°). Ook wordt erin voorzien dat de operatoren verschillende verkeersgegevens betreffende de binnenkomende communicatie bewaren om de persoon die de communicatie doet te identificeren, namelijk « het telefoonnummer aan de bron van de binnenkomende communicatie », « het IP-adres dat werd gebruikt om de binnenkomende communicatie te versturen, het tijdstempel en de gebruikte poort », alsook « de precieze datums en tijdstippen van begin en einde van de binnenkomende communicatie » (eerste lid, 2°).

Krachtens artikel 122, § 4, eerste lid, 5°, van de wet van 13 juni 2005, verwerken de operatoren de verschillende beoogde gegevens voor de voormelde doeleinden.

B.27.3. De in artikel 122, § 4, eerste lid, van de wet van 13 juni 2005 opgenomen lijst met verkeersgegevens is niet exhaustief.

Ten eerste wordt in artikel 122, § 4, tweede lid, vermeld dat « teneinde de gepaste maatregelen bedoeld in artikel 121/8, § 1, te kunnen nemen, om fraude of kwaadwillig gebruik van het netwerk of de dienst te kunnen vaststellen of om de dader en de herkomst ervan te kunnen identificeren, [...] de operator andere gegevens dan deze bedoeld in het eerste lid [mag] bewaren en verwerken, die tot deze doeleinden nodig worden geacht ». Die mogelijkheid voor de operatoren om andere gegevens dan die welke bij artikel 122, § 4, eerste lid, zijn bepaald, te bewaren en te verwerken, is niet onderworpen aan een voorafgaand advies van of een melding aan het BIPT en de Gegevensbeschermingsautoriteit. In de parlementaire voorbereiding van de bestreden bepaling wordt die mogelijkheid niet verantwoord (*Parl. St.*, Kamer, 2021-2022, DOC 55-2572/003, pp. 87-92).

Vervolgens voorziet artikel 122, § 4, derde lid, erin dat « de Koning [...], bij een besluit vastgesteld na overleg in de Ministerraad en na advies van het [BIPT] en van de Gegevensbeschermingsautoriteit, de verkeersgegevens waarvan de bewaring als noodzakelijk moet worden beschouwd voor het nastreven van de in deze paragraaf bedoelde doeleinden, [kan] preciseren en uitbreiden ». De parlementaire voorbereiding van de bestreden bepaling verantwoordt die machtiging door het feit dat fraude mettertijd aanzienlijk evolueert en dat de bewaarde gegevens kunnen verschillen afhankelijk van de verstrekte elektronische-communicatiedienst, de omvang van de operator, de tools waarover die beschikt en de gebruikers van de dienst (*Parl. St.*, Kamer, 2021-2022, DOC 55-2572/001, p. 35).

B.27.4. De in artikel 122, § 4, eerste lid, 1°, van de wet van 13 juni 2005 beoogde verkeersgegevens worden in principe gedurende vier maanden bewaard. De in artikel 122, § 4, eerste lid, 2°, beoogde gegevens worden in principe gedurende twaalf maanden bewaard.

B.27.5. Die termijnen voor de bewaring van de gegevens kunnen worden verlengd. Artikel 122, § 4, eerste lid, 3°, van de wet van 13 juni 2005 bepaalt dat de in 1° beoogde gegevens die betrekking hebben op een specifieke fraude of een specifiek kwaadwillig gebruik van een netwerk kunnen worden bewaard « gedurende de periode die nodig is voor de analyse en het verhelpen ervan, in voorkomend geval langer dan de termijn van vier maanden bedoeld in 1° ». Artikel 122, § 4, 4°, preciseert dat de in 2° beoogde gegevens die betrekking hebben op een specifiek kwaadwillig gebruik van het netwerk kunnen worden bewaard « gedurende de periode die nodig is voor de verwerking van dit kwaadwillig gebruik, in voorkomend geval langer dan een termijn van twaalf maanden bedoeld in 2° ».

B.28.1. Artikel 122, § 4/1, van de wet van 13 juni 2005 voorziet op zijn beurt in de mogelijkheid, ten laste van de operatoren, om de verkeersgegevens « die nodig zijn om de veiligheid en correcte werking van hun elektronische-communicatienetwerken en -diensten te garanderen, en in het bijzonder om een mogelijke of werkelijke aanslag op die veiligheid op te sporen en te analyseren, inclusief om de oorsprong van die aanslag te identificeren », te bewaren en te verwerken. Die mogelijkheid voor de operatoren is niet onderworpen aan een voorafgaand advies van of een melding aan het BIPT en de Gegevensbeschermingsautoriteit.

B.28.2. De verkeersgegevens waarvan sprake in artikel 122, § 4/1, eerste lid, van de wet van 13 juni 2005 kunnen voor een duur van in principe twaalf maanden worden bewaard. De gegevens met betrekking tot een « specifieke » schending van de veiligheid van het netwerk kunnen echter worden bewaard « gedurende de periode die nodig is om deze te behandelen, in voorkomend geval langer dan de termijn van twaalf maanden bedoeld in het tweede lid » (artikel 122, § 4/1, derde lid).

B.29. Artikel 122, § 4, van de wet van 13 juni 2005 voorziet, enerzijds, in een algemene en systematische bewaring van de verkeersgegevens die het beoogt en legt, anderzijds, een verplichting tot bewaring en verwerking op aan de operatoren, maar laat hen bepalen voor welke gegevens, van de in artikel 122, § 4, eerste lid, 1° en 2°, beoogde gegevens, het noodzakelijk is om ze te bewaren. Met andere woorden vormt de verplichting tot bewaring van de gegevens niet de uitzondering maar de regel in het kader van artikel 122, § 4, van de wet van 13 juni 2005.

Die vaststelling geldt des te meer daar krachtens artikel 122, § 4, vierde lid, van de wet van 13 juni 2005, de door de operatoren bewaarde verkeersgegevens die verband houden met vermeende fraude of vermeend kwaadwillig gebruik, aan de bevoegde autoriteiten kunnen worden doorgestuurd, met name de gerechtelijke autoriteiten, de politiediensten en de officieren van gerechtelijke politie van het BIPT (*Parl. St.,* Kamer, 2021-2022, DOC 55-2572/001, p. 35), zodat de bewaring en de verwerking van gegevens door de operatoren op basis van artikel 122, § 4, van de wet van 13 juni 2005 aanleiding kunnen geven tot strafrechtelijke vervolging.

B.30.1. Wat betreft artikel 122, § 4/1, van de wet van 13 juni 2005, dient te worden opgemerkt dat die bepaling niet preciseert welke gegevens kunnen worden bewaard. Daarenboven kunnen de gegevens met betrekking tot een « specifieke » schending van de veiligheid van het netwerk worden bewaard “ langer dan de termijn van twaalf maanden bedoeld in het tweede lid ”, zonder dat in de tekst van artikel 122, § 4/1, van de wet van 13 juni 2005, noch in de parlementaire voorbereiding van de wet van 20 juli 2022, wordt gepreciseerd wat de hypothese van een specifieke schending omvat.

B.30.2. Op de datum van de uitspraak van dit arrest heeft het Hof van Justitie zich nog niet moeten uitspreken over de uitlegging van artikel 15 van de richtlijn 2002/58/EG in zoverre het de lidstaten toelaat maatregelen te nemen tot bewaring van gegevens uit elektronische

communicatie om de voorkoming, het onderzoek, de opsporing en de vervolging van onbevoegd gebruik van het elektronische-communicatiesysteem te waarborgen.

B.30.3. De partijen voor het Hof verschillen van mening over de uitlegging die moet worden gegeven aan artikel 15 van de richtlijn 2002/58/EG, in zoverre het betrekking heeft op het voormelde doel en, in dat kader, in zoverre het al dan niet zo moet worden uitgelegd dat het de aanneming van nationale maatregelen zoals die welke zijn bedoeld in artikel 5, 4° en 5°, van de wet van 20 juli 2022, toelaat.

B.31. Wanneer een vraag die betrekking heeft op de uitlegging van het Unierecht wordt opgeworpen in een zaak aanhangig bij een nationale rechterlijke instantie waarvan de beslissingen volgens het nationale recht niet vatbaar zijn voor hoger beroep, is die instantie, overeenkomstig artikel 267, derde alinea, van het Verdrag betreffende de werking van de Europese Unie, ertoe gehouden die vraag te stellen aan het Hof van Justitie.

Die verwijzing is evenwel niet nodig wanneer die rechterlijke instantie heeft vastgesteld dat de opgeworpen vraag niet relevant is, dat de betrokken bepaling van het Unierecht reeds door het Hof is uitgelegd, of dat de juiste uitlegging van het Unierecht zo evident is dat redelijkerwijze geen ruimte voor twijfel kan bestaan (HvJ, 6 oktober 1982, C-283/81, *CILFIT*, ECLI:EU:C:1982:335, punt 21; grote kamer, 6 oktober 2021, C-561/19, *Consorzio Italian Management en Catania Multiservizi SpA*, ECLI:EU:C:2021:799, punt 33). Die redenen moeten, in het licht van artikel 47 van het Handvest, afdoende blijken uit de motivering van het arrest waarbij de rechterlijke instantie weigert de prejudiciële vraag te stellen (HvJ, grote kamer, 6 oktober 2021, C-561/19, voormeld, punt 51).

De uitzondering van het gebrek aan relevantie houdt in dat de nationale rechterlijke instantie van de verwijsplicht is ontheven wanneer « die vraag niet ter zake dienend is, dat wil zeggen wanneer het antwoord erop, hoe het ook luidt, geen invloed kan hebben op de oplossing van het geschil » (HvJ, 15 maart 2017, C-3/16, *Aquino*, ECLI:EU:C:2017:209, punt 43; grote kamer, 6 oktober 2021, C-561/19, voormeld, punt 34).

De uitzondering dat de juiste uitlegging van het Unierecht evident is, houdt in dat de nationale rechterlijke instantie ervan overtuigd moet zijn dat de gehanteerde oplossing even evident zou zijn voor de rechterlijke instanties van de andere lidstaten die in laatste aanleg

uitspraak doen, alsook voor het Hof van Justitie. Zij dient in dat verband rekening te houden met de specifieke kenmerken van het Unierecht, met de bijzondere moeilijkheden bij de uitlegging ervan en met het gevaar voor uiteenlopende rechtspraak binnen de Unie. Tevens dient zij acht te slaan op de verschillen tussen de taalversies van de betrokken bepaling waarvan zij op de hoogte is, met name wanneer die verschillen door de partijen naar voren zijn gebracht en onderbouwd zijn. Tot slot dient zij aandacht te hebben voor de eigen terminologie en autonome begrippen die het Unierecht bezigt, alsook voor de context van de toepasselijke bepaling in het licht van het Unierecht in zijn geheel, zijn doelstellingen en zijn ontwikkelingsstand op het ogenblik waarop de betrokken bepaling moet worden toegepast (HvJ, grote kamer, 6 oktober 2021, C-561/19, voormeld, punten 40-46).

Voorts vermag de in laatste aanleg rechtsprekende nationale rechterlijke instantie ervan af te zien het Hof van Justitie een prejudiciële vraag te stellen « om redenen van niet-ontvankelijkheid die eigen zijn aan de procedure bij die rechterlijke instantie, mits het gelijkwaardigheids- en het doeltreffendheidsbeginsel in acht worden genomen » (HvJ, 14 december 1995, C-430/93 en C-431/93, *Van Schijndel en Van Veen*, ECLI:EU:C:1995:441, punt 17; 15 maart 2017, C-3/16, voormeld, punt 56; grote kamer, 6 oktober 2021, C-561/19, voormeld, punt 61).

B.32. Aangezien de voorliggende zaak twijfel doet ontstaan over de uitlegging van artikel 15 van de richtlijn 2002/58/EG, dient aan het Hof van Justitie de eerste in het dictum geformuleerde prejudiciële vraag te worden gesteld.

4. Het bewaren van de locatiegegevens (artikel 6)

B.33.1. Het eerste en het tweede middel in de zaak nr. 7930, alsook het tweede onderdeel van het eerste middel en het eerste onderdeel van het derde middel in de zaak nr. 7932, hebben betrekking op artikel 6 van de wet van 20 juli 2022, waarbij artikel 123 van de wet van 13 juni 2005 als volgt wordt gewijzigd :

« 1° paragraaf 1 wordt vervangen als volgt :

‘ § 1. Onverminderd de toepassing van de AVG en van de wet van 30 juli 2018 mogen de operatoren van mobiele netwerken andere locatiegegevens dan verkeersgegevens die

betrekking hebben op een abonnee of een eindgebruiker slechts bewaren en verwerken in de volgende gevallen :

1° wanneer dat noodzakelijk is voor de goede werking en de veiligheid van het netwerk of van de dienst, waarbij de gegevens worden bewaard gedurende maximaal twaalf maanden vanaf de datum van de communicatie, tenzij in geval van een specifieke schending van de veiligheid van het netwerk waarvoor de gegevens in kwestie langer dienen te worden bewaard dan deze periode;

2° wanneer dat noodzakelijk is om fraude of kwaadwillig gebruik van het netwerk op te sporen of te analyseren, waarbij de gegevens worden bewaard gedurende maximaal vier maanden vanaf de datum van de communicatie, tenzij in geval van specifieke fraude of specifiek kwaadwillig gebruik waarvoor de gegevens in kwestie langer dienen te worden bewaard dan deze periode;

3° wanneer de gegevens anoniem gemaakt zijn;

4° wanneer de verwerking past in het kader van de levering van een dienst die gebruik maakt van verkeersgegevens of locatiegegevens;

5° wanneer de verwerking noodzakelijk is om te voldoen aan een verplichting opgelegd krachtens een formele wettelijke norm. ';

2° in paragraaf 2 worden in de bepaling onder 2°, de woorden ' de vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene of zijn wettelijke, vertegenwoordiger aanvaardt dat locatiegegevens die op hem betrekking hebben worden verwerkt ' vervangen door de woorden ' de toestemming in de zin van artikel 4, 11), van de AVG ';

3° in paragraaf 4 wordt het eerste lid vervangen als volgt :

' De gegevens vermeld in dit artikel mogen alleen worden verwerkt door personen die werkzaam zijn in opdracht van de operator of de derde die de dienst die gebruik maakt van verkeersgegevens of locatiegegevens levert, of door de Coördinatiecel van de operator bedoeld in artikel 127/3. ' ».

B.33.2. Ingevolge de voormelde wijziging bepaalt artikel 123 van de wet van 13 juni 2005 thans :

« § 1. Onverminderd de toepassing van de AVG en van de wet van 30 juli 2018 mogen de operatoren van mobiele netwerken andere locatiegegevens dan verkeersgegevens die betrekking hebben op een abonnee of een eindgebruiker slechts bewaren en verwerken in de volgende gevallen :

1° wanneer dat noodzakelijk is voor de goede werking en de veiligheid van het netwerk of van de dienst, waarbij de gegevens worden bewaard gedurende maximaal twaalf maanden vanaf de datum van de communicatie, tenzij in geval van een specifieke schending van de veiligheid van het netwerk waarvoor de gegevens in kwestie langer dienen te worden bewaard dan deze periode;

2° wanneer dat noodzakelijk is om fraude of kwaadwillig gebruik van het netwerk op te sporen of te analyseren, waarbij de gegevens worden bewaard gedurende maximaal vier maanden vanaf de datum van de communicatie, tenzij in geval van specifieke fraude of specifiek kwaadwillig gebruik waarvoor de gegevens in kwestie langer dienen te worden bewaard dan deze periode;

3° wanneer de gegevens anoniem gemaakt zijn;

4° wanneer de verwerking past in het kader van de levering van een dienst die gebruik maakt van verkeersgegevens of locatiegegevens;

5° wanneer de verwerking noodzakelijk is om te voldoen aan een verplichting opgelegd krachtens een formele wettelijke norm.

§ 2. De verwerking in het kader van de levering van een dienst gebaseerd op verkeersgegevens of locatiegegevens is onderworpen aan de volgende voorwaarden :

1° De operator stelt de abonnee of, in voorkomend geval, de eindgebruiker waarop de gegevens betrekking hebben, voorafgaand aan het verkrijgen van diens toestemming voor de verwerking in kennis van :

a) de soorten locatiegegevens die worden verwerkt;

b) de precieze doeleinden van de verwerking;

c) de duur van de verwerking;

d) de eventuele derden waaraan deze gegevens zullen worden doorgegeven;

e) de mogelijkheid om te allen tijde de gegeven toestemming voor de verwerking definitief of tijdelijk in te trekken.

2° De abonnee of, in voorkomend geval, de eindgebruiker, heeft voorafgaand aan de verwerking zijn toestemming gegeven voor de verwerking.

Onder toestemming voor de verwerking in de zin van dit artikel wordt verstaan de toestemming in de zin van artikel 4, 11), van de AVG.

3° De verwerking van de betrokken gegevens blijft beperkt tot de handelingen en de duur die nodig zijn voor de levering van de betrokken dienst met verkeersgegevens of locatiegegevens.

4° De betrokken operator biedt zijn abonnees of eindgebruikers gratis de mogelijkheid om te allen tijde op eenvoudige wijze de gegeven toestemming, definitief of tijdelijk, in te trekken.

§ 4. De gegevens vermeld in dit artikel mogen alleen worden verwerkt door personen die werkzaam zijn in opdracht van de operator of de derde die de dienst die gebruik maakt van verkeersgegevens of locatiegegevens levert, of door de Coördinatiecel van de operator bedoeld in artikel 127/3.

De verwerking is beperkt tot hetgeen strikt noodzakelijk is om de betrokken dienst met verkeersgegevens of locatiegegevens aan te kunnen bieden.

§ 5. In geval van een noodcommunicatie naar de beheercentrales van de nooddiensten die ter plaatse hulp bieden, heffen de operatoren in zoverre dit technisch mogelijk is, met als doel de behandeling van de noodcommunicatie door de betrokken beheercentrales mogelijk te maken, de tijdelijke weigering of het ontbreken van toestemming van de abonnee of de eindgebruiker betreffende de verwerking van lokalisatiegegevens per afzonderlijke, oproepende lijn, op.

Die opheffing is gratis ».

B.33.3.1. De verzoekende partij in de zaak nr. 7930 leidt een eerste en een tweede middel af uit de schending van de artikelen 11, 12, 22 en 29 van de Grondwet, van artikel 15, lid 1, en de artikelen 5, 6 en 9 van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8, 11, 47 en 52, lid 1, van het Handvest, van de artikelen 6, 8, 10, 11 en 18 van het Europees Verdrag voor de rechten van de mens en van de artikelen 13 en 54 van de richtlijn (EU) 2016/680, in zoverre artikel 6 van de wet van 20 juli 2022 een algemene verplichting tot bewaring van de communicatiegegevens invoert, zonder dat die bewaring noodzakelijk, noch strikt beperkt ten aanzien van het nagestreefde doel blijkt te zijn.

B.33.3.2. De verzoekende partijen in de zaak nr. 7932 leiden een eerste middel af uit de schending van de artikelen 10, 11, 13, 15, 22, 23 en 29 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 5, 6, 8, 9, 10, 11, 14 en 18 van het Europees Verdrag voor de rechten van de mens, met de artikelen 7, 8, 11, 47 en 52 van het Handvest, met artikel 5, lid 4, van het Verdrag betreffende de Europese Unie, alsook met artikel 6 van de richtlijn 2002/58/EG, met de richtlijn (EU) 2016/680 en met de AVG. In een tweede onderdeel voeren zij aan dat artikel 6 van de wet van 20 juli 2022 de bewaring toelaat gedurende twaalf maanden van de gegevens die het beoogt om de goede werking en de veiligheid van het netwerk te waarborgen, terwijl artikel 9 van de richtlijn 2002/58/EG een dergelijke verwerking uitsluit.

De verzoekende partijen leiden een derde middel af uit de schending van de artikelen 10, 11, 15, 22 en 29 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 5, 6, 8, 9, 10, 11, 14 en 18 van het Europees Verdrag voor de rechten van de mens, met de artikelen 7, 8, 11, 47 en 52 van het Handvest, met artikel 5, lid 4, van het Verdrag betreffende de Europese Unie, alsook met de richtlijn 2002/58/EG, met de richtlijn (EU) 2016/680 en met de AVG. In een eerste onderdeel voeren zij aan dat artikel 6 van de wet van 20 juli 2022 een verplichting

tot algemene en ongedifferentieerde bewaring van de gegevens creëert ten gunste van de operatoren die in het kader van hun opdrachten handelen, hetgeen te vaag en te ruim is.

B.34. Uit het voorgaande blijkt dat de grieven van de verzoekende partijen betrekking hebben op artikel 123, § 1, van de wet van 13 juni 2005, zoals vervangen door artikel 6, 1°, van de wet van 20 juli 2022. De grieven zijn hoofdzakelijk afgeleid uit de schending van het recht op eerbiediging van het privéleven en van het recht op bescherming van de persoonsgegevens, gewaarborgd bij artikel 22 van de Grondwet, bij artikel 8 van het Europees Verdrag voor de rechten van de mens, bij de artikelen 7, 8 en 52, lid 1, van het Handvest, bij de richtlijn 2002/58/EG, bij de richtlijn (EU) 2016/680 en bij de AVG.

B.35.1. Uit de parlementaire voorbereiding van artikel 6, 1°, van de wet van 20 juli 2022 blijkt dat het dient ter omzetting van artikel 9 van de richtlijn 2002/58/EG (*Parl. St.*, Kamer, 2021-2022, DOC 55-2572/001, pp. 39 en 40), dat bepaalt :

« Andere locatiegegevens dan verkeersgegevens

1. Wanneer andere locatiegegevens dan verkeersgegevens die betrekking hebben op gebruikers of abonnees van elektronische-communicatienetwerken of -diensten verwerkt kunnen worden, mogen deze gegevens slechts worden verwerkt wanneer zij anoniem zijn gemaakt of wanneer de gebruikers of abonnees daarvoor hun toestemming hebben gegeven, voorzover en voor zolang zulks nodig is voor de levering van een dienst met toegevoegde waarde. De dienstenaanbieder moet de gebruikers of abonnees, voorafgaand aan het verkrijgen van hun toestemming, in kennis stellen van de soort locatiegegevens anders dan verkeersgegevens, die zullen worden verwerkt, en van de doeleinden en de duur van die verwerking, en hun meedelen of deze gegevens aan een derde zullen worden doorgegeven ten behoeve van de levering van de dienst met toegevoegde waarde. Gebruikers of abonnees kunnen hun toestemming voor de verwerking van andere locatiegegevens dan verkeersgegevens te allen tijde intrekken.

2. Wanneer de gebruikers of abonnees toestemming hebben gegeven voor de verwerking van andere locatiegegevens dan verkeersgegevens, moet de gebruiker of abonnee de mogelijkheid behouden om op eenvoudige en kosteloze wijze tijdelijk de verwerking van dergelijke gegevens te weigeren voor elke verbinding met het netwerk of voor elke transmissie van communicatie.

3. De verwerking van locatiegegevens anders dan verkeersgegevens in overeenstemming met de leden 1 en 2, moet worden beperkt tot personen die werkzaam zijn onder het gezag van de aanbieder van het openbare elektronische-communicatienetwerk of de openbare elektronische-communicatiedienst of de derde die de dienst met toegevoegde waarde levert, en moet beperkt blijven tot hetgeen noodzakelijk is om de dienst met toegevoegde waarde te kunnen aanbieden ».

B.35.2. In zoverre artikel 123, § 1, van de wet van 13 juni 2005 voorziet in de bewaring van de andere locatiegegevens dan verkeersgegevens die betrekking hebben op een abonnee of een eindgebruiker wanneer de gegevens anoniem zijn gemaakt (3°) en wanneer de verwerking past in het kader van de levering van een dienst die gebruik maakt van verkeersgegevens of locatiegegevens (4°) – op voorwaarde dat, in dat laatste geval, de abonnee of de eindgebruiker krachtens artikel 123, § 2, vooraf zijn toestemming heeft gegeven –, past die bepaling in de door artikel 9, lid 1, van de richtlijn 2002/58/EG beoogde gevallen.

B.35.3. Artikel 123, § 1, van de wet van 13 juni 2005 beoogt daarentegen ook andere hypotheses van bewaring van de andere locatiegegevens dan de verkeersgegevens, dan die welke zijn toegelaten bij artikel 9 van de richtlijn 2002/58/EG, zoals de afdeling wetgeving van de Raad van State en de Gegevensbeschermingsautoriteit hebben opgemerkt in hun advies over het voorontwerp van wet dat aan de basis ligt van de wet van 20 juli 2022 (*ibid.*, pp. 306 tot 308 en 677 tot 678).

Wat die andere hypotheses betreft, dient te worden verwezen naar artikel 15, lid 1, van de richtlijn 2002/58/EG, dat toelaat de reikwijdte van de met name in artikel 9 ervan bepaalde rechten te beperken, « indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale [veiligheid], d.w.z. de staatsveiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronische-communicatiesysteem ».

B.36. De grieven van de verzoekende partijen hebben meer in het bijzonder betrekking op de hypotheses van bewaring van de andere locatiegegevens dan de verkeersgegevens, die onder de bij artikel 15, lid 1, van de richtlijn 2002/58/EG bepaalde beperkingsregeling vallen en die worden beoogd door artikel 123, § 1, 1°, 2° en 5°, van de wet van 13 juni 2005, zoals vervangen bij artikel 6 van de wet van 20 juli 2022.

B.37.1. Artikel 123, § 1, van de wet van 13 juni 2005 voorziet erin dat de operatoren van mobiele netwerken de voormelde locatiegegevens die betrekking hebben op een abonnee of een eindgebruiker slechts mogen bewaren en verwerken « wanneer dat noodzakelijk is voor de

goede werking en de veiligheid van het netwerk of van de dienst » (1°) en « wanneer dat noodzakelijk is om fraude of kwaadwillig gebruik van het netwerk op te sporen of te analyseren » (2°).

De in artikel 123, § 1, 1°, van de wet van 13 juni 2005 beoogde gegevens worden in principe gedurende twaalf maanden bewaard, te rekenen vanaf de datum van de communicatie. De in artikel 123, § 1, 2°, van de wet van 13 juni 2005 beoogde gegevens worden in principe gedurende vier maanden bewaard.

B.37.2. De door artikel 123, § 1, 1° en 2°, van de wet van 13 juni 2005 beoogde hypotheses laten toe onbevoegd gebruik van het elektronische-communicatiesysteem in de zin van artikel 15, lid 1, van de richtlijn 2002/58/EG te voorkomen, te onderzoeken, op te sporen en te vervolgen.

B.38. Het staat aan het Hof om na te gaan of de inmenging die artikel 123, § 1, 1° en 2°, van de wet van 13 juni 2005, vervangen bij artikel 6, 1°, van de wet van 20 juli 2022, in het recht op eerbiediging van het privéleven en in het recht op bescherming van de persoonsgegevens veroorzaakt, in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter voorkoming van onbevoegd gebruik van het elektronische-communicatiesysteem.

B.39.1. De operatoren bepalen welke andere locatiegegevens dan de verkeersgegevens kunnen worden bewaard en verwerkt. Zij beoordelen ook in elk concreet geval de noodzaak van die bewaring en van die verwerking.

Wat betreft de bewaringstermijn van de in artikel 123, § 1, 1° en 2°, van de wet van 13 juni 2005 beoogde gegevens, is bovendien erin voorzien dat de voormelde duur van twaalf maanden kan worden verlengd « in geval van een specifieke schending van de veiligheid van het netwerk waarvoor de gegevens in kwestie langer dienen te worden bewaard dan deze periode » en dat de voormelde duur van vier maanden kan worden verlengd « in geval van specifieke fraude of specifiek kwaadwillig gebruik waarvoor de gegevens in kwestie langer dienen te worden bewaard dan deze periode ».

B.39.2. Artikel 123, § 1, 1° en 2°, van de wet van 13 juni 2005 laat de operatoren bepalen voor welke van die locatiegegevens het noodzakelijk is ze te bewaren en te verwerken, en de bewaringstermijn van de gegevens in kwestie verlengen in geval van, enerzijds, een specifieke schending van de veiligheid van het netwerk en, anderzijds, specifieke fraude of specifiek kwaadwillig gebruik.

B.39.3. Om dezelfde redenen als die welke zijn vermeld in B.30 en B.31, is het, aangezien de voorliggende zaak twijfels doet rijzen over de uitlegging van artikel 15, lid 1, van de richtlijn 2002/58/EG, aangewezen om aan het Hof van Justitie de tweede in het dictum geformuleerde prejudiciële vraag te stellen.

Het is daarnaast aangewezen de derde in het dictum vermelde prejudiciële vraag te stellen.

B.40.1. Ten slotte laat artikel 123, § 1, 5°, van de wet van 13 juni 2005 de bewaring toe van de andere locatiegegevens dan verkeersgegevens die betrekking hebben op een abonnee of een eindgebruiker, « wanneer de verwerking noodzakelijk is om te voldoen aan een verplichting opgelegd krachtens een formele wettelijke norm ».

In die hypothese kunnen de grieven van de verzoekende partijen op zich niet te wijten zijn aan artikel 123 van de wet van 13 juni 2005, maar, in voorkomend geval, aan de verplichtingen opgelegd bij een formele wetskrachtige norm waarnaar wordt verwezen.

B.40.2. Het eerste en tweede middel in de zaak nr. 7930, alsook het tweede onderdeel van het eerste middel en het eerste onderdeel van het derde middel in de zaak nr. 7932, met betrekking tot artikel 123, § 1, 5°, van de wet van 13 juni 2005, zijn niet gegrond in zoverre zij zijn afgeleid uit de schending van de in B.34 vermelde bepalingen. De toetsing aan de andere in B.33.3.1 en B.33.3.2 vermelde referentienormen, in de veronderstelling dat de schending ervan op geldige wijze door de verzoekende partijen wordt aangevoerd, kan in geen geval tot een andere conclusie leiden.

5. Het bewaren van de inschrijvings- en identificatiegegevens (artikel 8)

B.41.1. Het eerste en het tweede middel in de zaak nr. 7930, het enige middel in de zaak nr. 7931 en het eerste, tweede en vijfde onderdeel van het tweede middel in de zaak nr. 7932 hebben betrekking op artikel 8 van de wet van 20 juli 2022, dat bepaalt :

« Artikel 126 van [de wet van 13 juni 2005], vervangen bij artikel 5 van de wet van 30 juli 2013, zelf vernietigd bij arrest nr. 84/2015 van het Grondwettelijk Hof, en bij artikel 4 van de wet van 29 mei 2016, zelf vernietigd bij arrest nr. 57/2021 van het Grondwettelijk Hof, wordt vervangen als volgt :

‘ Art. 126. § 1. Onverminderd de AVG en de wet van 30 juli 2018, bewaren de operatoren die aan de eindgebruikers elektronische-communicatiediensten aanbieden, alsook de operatoren die de onderliggende elektronische-communicatienetwerken aanbieden waarmee deze diensten verstrekt kunnen worden, de volgende gegevens, voor zover ze die verwerken of genereren in het kader van de verstrekking van die netwerken of diensten :

1° het Rijksregisternummer of een equivalent nummer, de naam en voornaam van de eindgebruiker die een natuurlijke persoon is of de naam van de abonnee die een rechtspersoon is;

2° de eventuele alias gekozen door de eindgebruiker bij de inschrijving op of de activering van de dienst;

3° de contactgegevens van de abonnee die verstrekt zijn bij de inschrijving op de dienst, met name zijn telefoonnummer, zijn e-mailadres en zijn postadres;

4° de datum en het tijdstip van inschrijving op de dienst en van de activering van de dienst en de elementen aan de hand waarvan de plaats kan bepaald worden waarvandaan die inschrijving en die activering zijn uitgevoerd, met name :

- het fysieke adres van het verkooppunt waar de inschrijving of activering heeft plaatsgevonden, of;

- het fysieke adres van het netwerkaansluitpunt dat gediend heeft voor de inschrijving of de activering, of;

- het IP-adres dat gediend heeft voor de inschrijving of de activering, alsook de bronpoort van de verbinding en het tijdstempel, of;

- in het kader van een mobiel telefoonnetwerk, de geografische locatie van de eindapparatuur die de inschrijving of de activering aan de hand van een telefoonnummer mogelijk heeft gemaakt;

5° het fysieke leveringsadres van de dienst;

6° het facturatieadres van de dienst en de gegevens betreffende de betalingswijze en het betaalmiddel, het tijdstip van de betalingen en de referentie van de betalingstransactie in geval van onlinebetaling;

7° de hoofddienst en de aanvullende diensten die de abonnee kan gebruiken;

8° de datum vanaf wanneer die diensten gebruikt kunnen worden, de datum van het eerste gebruik van die diensten en de datum van beëindiging van die diensten;

9° in geval van overdracht van de identifier van de abonnee, zoals zijn telefoonnummer, de identiteit van de operator die de identifier overdraagt en de identiteit van de operator naar wie de identifier wordt overgedragen en de datum waarop de overdracht wordt uitgevoerd;

10° het toegewezen telefoonnummer;

11° het voornaamste e-mailadres en de e-mailadressen die als alias gebruikt worden;

12° de internationale identiteit van de mobiele abonnee, “ International Mobile Subscriber Identity ”, afgekort “ IMSI ”;

13° de permanente identifier van het abonnement, “ Subscription Permanent Identifier ”, afgekort “ SUPI ”;

14° de verdoken identifier van het abonnement, “ Subscription Concealed Identifier ”, afgekort “ SUCI ”;

15° het IP-adres aan de bron van de verbinding, het tijdstempel van de toewijzing alsook, in geval van gedeeld gebruik van een IP-adres van de eindgebruiker, de poorten die daaraan zijn toegewezen;

16° de identifier van de eindapparatuur van de eindgebruiker, of indien de operator dit niet verwerkt of genereert, de identifier van de apparatuur die zich het dichtste bij die eindapparatuur bevindt, met name :

- de internationale identiteit van de mobiele apparatuur, “ International Mobile Equipment Identity ”, afgekort “ IMEI ”;

- de permanente identifier van de apparatuur, “ Permanent Equipment Identifier ”, afgekort “ PEI ”;

- het adres van de controller van de toegang tot het netwerk, “ Media Access Control address ”, afgekort “ MAC ”;

17° de andere identifiers met betrekking tot de eindgebruiker, tot de eindapparatuur of tot de apparatuur het dichtst bij die eindapparatuur, die uit de technologische evolutie resulteren en die door de Koning bepaald worden, op voorwaarde dat dit besluit bij wet wordt bekrachtigd binnen zes maanden na de bekendmaking van dit besluit.

De operatoren hoeven de MAC-adressen bedoeld in het eerste lid, 16°, derde streepje, niet te bewaren voor de elektronische-communicatiediensten die ze enkel aan ondernemingen of rechtspersonen aanbieden.

Het koninklijk besluit bedoeld in het eerste lid, 17°, slaat niet op de inhoud van de elektronische communicatie, noch op de elektronische-communicatiemetagegevens die informatie geven over de geadresseerde van de communicatie, zoals het IP-adres van de geadresseerde van de communicatie, of over de locatie van de eindapparatuur.

De Koning :

1° kan de gegevens bedoeld in het eerste lid preciseren;

2° bepaalt de vereisten inzake nauwkeurigheid en betrouwbaarheid waaraan deze gegevens moeten beantwoorden.

§ 2. De operatoren bewaren de in paragraaf 1, eerste lid, 1° tot 14°, bedoelde gegevens tot zolang de elektronische-communicatiedienst gebruikt wordt en tot twaalf maanden na het einde van de dienst.

De operatoren bewaren de in paragraaf 1, eerste lid, 15° en 16°, bedoelde gegevens gedurende een periode van twaalf maanden na het einde van de sessie.

In afwijking van het tweede lid wordt de bewaringstermijn van de in paragraaf 1, eerste lid, 16°, derde streepje, bedoelde gegevens, teruggebracht tot zes maanden na het einde van de sessie indien de operator een ander gegeven zoals bedoeld in paragraaf 1, eerste lid, 16°, bewaart.

De operatoren bewaren de gegevens bedoeld in paragraaf 1, eerste lid, 17°, gedurende de door de Koning bepaalde periode. Die periode mag niet langer zijn dan de in het eerste lid bedoelde bewaringstermijn.

Het koninklijk besluit bedoeld in paragraaf 1, eerste lid, 17°, en vierde lid, en in paragraaf 2, vierde lid, wordt voorgesteld door de minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie en de minister, maakt het voorwerp uit van een advies van de Gegevensbeschermingsautoriteit en van het Instituut en daarover wordt beraadslaagd in de Ministerraad. ’».

B.41.2.1. De verzoekende partij in de zaak nr. 7930 leidt een eerste en een tweede middel af uit de schending van de artikelen 11, 12, 22 en 29 van de Grondwet, van artikel 15, lid 1, en de artikelen 5, 6 en 9 van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8, 11, 47 en 52, lid 1, van het Handvest, van de artikelen 6, 8, 10, 11 en 18 van het Europees Verdrag voor de rechten van de mens en van de artikelen 13 en 54 van de richtlijn (EU) 2016/680, in zoverre artikel 8 van de wet van 20 juli 2022 een algemene verplichting tot bewaring van de communicatiegegevens invoert, zonder dat die bewaring noodzakelijk of strikt beperkt lijkt ten aanzien van het nagestreefde doel.

B.41.2.2. De verzoekende partij in de zaak nr. 7931 leidt een enig middel af uit de schending van de artikelen 11, 12, 22 en 29 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 7, 8, 11, 47 en 52, lid 1, van het Handvest, met artikel 8 van het Europees Verdrag voor de rechten van de mens, met de artikelen 5, 6 en 15 van de richtlijn 2002/58/EG en met de artikelen 13 en 54 van de richtlijn (EU) 2016/680. Zij betoogt dat artikel 8 van de wet van 20 juli 2022 in een verplichting voorziet tot het systematisch en ongedifferentieerd bewaren van de identificatiegegevens, die niet noodzakelijk is ten aanzien van het nagestreefde doel. In ondergeschikte orde vraagt de verzoekende partij om een prejudiciële vraag te stellen aan het Hof van Justitie.

B.41.2.3. De verzoekende partijen in de zaak nr. 7932 leiden een tweede middel af uit de schending van de artikelen 10, 11, 15, 22 en 29 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 5, 6, 8, 9, 10, 11, 14 en 18 van het Europees Verdrag voor de rechten van de mens, met de artikelen 7, 8, 11, 47 en 52 van het Handvest, met artikel 5, lid 4, van het Verdrag betreffende de Europese Unie, met de richtlijn 2002/58/EG, met de richtlijn (EU) 2016/680 en met de AVG. In het eerste en het derde onderdeel voeren zij aan dat artikel 8 van de wet van 20 juli 2022 voorziet in een gegevensbewaring die niet noodzakelijk is, alsook in een te lange bewaringstermijn, zodat het niet bestaanbaar is met het recht op eerbiediging van het privéleven en met artikel 5, lid 1, *c)* en *d),* van de AVG. In een tweede onderdeel voeren zij aan dat, in zoverre artikel 8 van de wet van 20 juli 2022 van toepassing is op « *over-the-top* » elektronische-communicatiediensten (hierna : OTT-diensten), zoals WhatsApp en Skype, het een identieke behandeling doet ontstaan die strijdig is met het beginsel van gelijkheid en niet-discriminatie en met het wettigheidsbeginsel.

B.42. Het eerste en het tweede middel in de zaak nr. 7930, het enige middel in de zaak nr. 7931, alsook het eerste en het derde onderdeel van het tweede middel in de zaak nr. 7932 zijn in hoofdzaak afgeleid uit de schending van het recht op eerbiediging van het privéleven en van het recht op bescherming van de persoonsgegevens, die zijn gewaarborgd bij artikel 22 van de Grondwet, bij artikel 8 van het Europees Verdrag voor de rechten van de mens, bij de artikelen 7, 8 en 52, lid 1, van het Handvest, bij de richtlijn 2002/58/EG, bij de richtlijn (EU) 2016/680 en bij de AVG.

B.43.1. Uit de parlementaire voorbereiding van artikel 8 van de wet van 20 juli 2022 blijkt dat de wetgever, met die bepaling, een antwoord heeft willen bieden op het voormelde arrest van het Hof nr. 158/2021, door zelf de verschillende te bewaren identificatiegegevens op te sommen (*Parl. St.*, Kamer, 2021-2022, DOC 55-2572/002, pp. 5 tot 7).

B.43.2. Daarnaast blijkt uit die parlementaire voorbereiding dat de wetgever, voor de operatoren bedoeld in artikel 126, § 1, eerste lid, ook de verplichting heeft willen invoeren om de voormelde identificatiegegevens te bewaren (*ibid.*, pp. 7 tot 10).

In dat verband heeft de Gegevensbeschermingsautoriteit, in haar advies over het amendement dat aan artikel 8 van de wet van 20 juli 2022 ten grondslag ligt, opgemerkt :

« 23. Door de omzetting van het Europees Wetboek voor elektronische communicatie (hierna ‘ EWEC ’) in de telecomwet, heeft de wetgever onder meer de begrippen ‘ operator ’ en ‘ elektronische-communicatiediensten ’ geherdefinieerd, die worden gebruikt om het persoonlijke toepassingsgebied te bepalen van de aan operatoren opgelegde verplichtingen om verkeers- en locatiegegevens van abonnees te bewaren en de verplichting om abonnees en eindgebruikers van elektronische-communicatiediensten te identificeren. Zoals de Autoriteit reeds in haar advies nr. 108/2021 heeft opgemerkt, leiden deze nieuwe definities tot een aanzienlijke uitbreiding van de reikwijdte van de verplichtingen om gegevens te bewaren en abonnees en eindgebruikers te identificeren. Met de omzetting van het EWEC in de telecomwet zijn bedrijven die over-the-top elektronische communicatiediensten aanbieden, zoals Voice over IP-diensten, berichtendiensten (bv. : WhatsApp, Signal, Telegram, Facebook Messenger), of online e-maildiensten (bv. : Gmail of Hotmail), onderworpen aan gegevensbewaringsverplichtingen en moeten zij hun abonnees of eindgebruikers identificeren. Ook de ondernemingen die instaan voor het aanbieden van ‘ diensten die geheel of hoofdzakelijk bestaan in het overbrengen van signalen zoals transmissiediensten die voor het verlenen van intermachinale diensten worden gebruikt ’ - het gaat om diensten in verband met het internet van de dingen - moeten nu worden beschouwd als operatoren die onderworpen zijn aan gegevensbewaringsverplichtingen en de verplichting om hun abonnees en eindgebruikers te identificeren.

24. De nieuwe definities van ‘ operator ’ en ‘ elektronische communicatiedienst ’, in het bijzonder gekoppeld aan de identificatieplicht die wordt opgelegd door de nieuwe artikelen 126 en 127 van de telecomwet (ingevoerd bij Amendementen nrs. 1 en 6), maken het onmogelijk - of op zijn minst zeer moeilijk - om anoniem te corresponderen op het internet. Bovendien merkt de Autoriteit op met betrekking tot de ‘ OTT ’-berichtendiensten (zoals Signal of WhatsApp) dat het verzamelen en bewaren van IP-adressen die aan de bron van de verbinding worden toegewezen, niet alleen indirect de gebruiker identificeert, maar ook (potentieel) de gebruiker lokaliseert. Het is immers vaak mogelijk eindapparatuur (en dus de persoon die er gebruik van maakt) te lokaliseren aan de hand van het IP-adres dat eraan is toegekend. De systematische verzameling van aan de bron van de verbinding toegewezen IP-adressen en de tijdsregistratie ervan maken het dus mogelijk de bewegingen van de gebruikers van deze

diensten te volgen; dit vormt een bijzonder belangrijke inmenging in het recht op privacy van deze gebruikers.

25. Dit betekent een radicale verandering ten opzichte van het paradigma van, en de privacyregels die zijn opgelegd door, de e-privacyrichtlijn. De Autoriteit benadrukt de noodzaak van een grondig parlementair debat over de gevolgen van deze wijziging, met name wat betreft het recht op privacy en het recht op vrijheid van meningsuiting. In ieder geval herinnert de Autoriteit eraan dat inmenging in de rechten en vrijheden van de betrokken personen alleen toelaatbaar is indien zij noodzakelijk is en in verhouding staat tot de nagestreefde doelstelling van algemeen belang » (Gegevensbeschermingsautoriteit, advies nr. 66/2022 van 1 april 2022, punten 23 tot 25).

B.44.1. In het dictum van zijn voormelde arrest van 6 oktober 2020 heeft het Hof van Justitie voor recht verklaard dat artikel 15, lid 1, van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8 en 11, alsook van artikel 52, lid 1, van het Handvest, zich niet verzet tegen, onder meer, wettelijke maatregelen « die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de IP-adressen die zijn toegewezen aan de bron van een verbinding, voor een periode die niet langer is dan strikt noodzakelijk », enerzijds, en « die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van criminaliteit en de bescherming van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronische communicatiemiddelen », anderzijds.

B.44.2. Zoals de afdeling wetgeving van de Raad van State opmerkte in haar advies over het voorontwerp van wet dat ten grondslag ligt aan de wet van 20 juli 2022, maakt het Hof van Justitie dus een onderscheid tussen, enerzijds, een algemene en ongedifferentieerde bewaring van de IP-adressen die zijn toegewezen aan een bron van een verbinding, die enkel aan de operatoren kan worden opgelegd ten behoeve van de vrijwaring van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid, en dat voor een periode die niet langer is dan strikt noodzakelijk, en, anderzijds, een algemene en ongedifferentieerde bewaring van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronische-communicatiemiddelen, die voor ruimere doelstellingen aan de operatoren kan worden opgelegd, te weten de bescherming van de nationale veiligheid, de bestrijding van criminaliteit, ongeacht of die zwaar is of niet, en de bescherming van de openbare veiligheid, zelfs wanneer die veiligheid niet ernstig wordt

bedreigd, en dat zonder dat die gegevens moeten worden bewaard voor een periode die niet langer is dan strikt noodzakelijk (*Parl. St.,* Kamer, 2021-2022, DOC 55-2572/001, p. 296).

B.44.3. Overigens is het Hof van Justitie van oordeel dat voor de IP-adressen die zijn toegewezen aan de bron van een verbinding, een bijzondere regeling moet worden uitgewerkt, aangezien die adressen « onder meer kunnen worden gebruikt om de volledige zoekgeschiedenis van een internetgebruiker te traceren en dus om een volledig beeld te krijgen van diens online activiteit[;] [...] aan de hand van die gegevens [kan] een gedetailleerd profiel van de betrokkene worden opgesteld. De voor een dergelijke tracking noodzakelijke bewaring en analyse van IP-adressen vormen dan ook ernstige inmengingen in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten van de internetgebruiker » (HvJ, 6 oktober 2020, C-511/18, C-512/18 en C-520/18, voormeld, punt 153).

B.45. Bij zijn in voltallige zitting gewezen arrest van 30 april 2024 in zake *La Quadrature du Net e.a.* (Persoonsgegevens en bestrijding van namaak) (C-470/21, ECLI:EU:C:2024:370, voorlopige editie) heeft het Hof van Justitie zulks als volgt gepreciseerd :

« 75. [Er] moet worden opgemerkt dat volgens vaste rechtspraak van het Hof de IP-adressen weliswaar [...] verkeersgegevens in de zin van richtlijn 2002/58 vormen, maar zich onderscheiden van de andere categorieën verkeers- en locatiegegevens.

76. In dit verband heeft het Hof erop gewezen dat IP-adressen los van een bepaalde communicatie worden gegenereerd en primair dienen om via de aanbieders van elektronische-communicatiediensten de eigenaar te identificeren van een eindapparaat waarvandaan via het internet wordt gecommuniceerd. Voor zover bij e-mailverkeer en internettelefonie uitsluitend de IP-adressen van de bron van de communicatie en niet die van de ontvanger ervan worden bewaard, geven die adressen als zodanig geen enkele informatie prijs over de derden die in contact zijn geweest met de persoon die aan de basis ligt van de communicatie. In dat opzicht is deze categorie gegevens van minder gevoelige aard dan de andere verkeersgegevens (zie in die zin arrest van 6 oktober 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punt 152).

77. In punt 156 van het arrest van 6 oktober 2020, *La Quadrature du Net e.a.* (C-511/18, C-512/18 en C-520/18, EU:C:2020:791), heeft het Hof - ook al heeft het vastgesteld dat IP-adressen minder gevoelig zijn wanneer zij uitsluitend dienen om de gebruiker van een elektronische-communicatiedienst te identificeren - weliswaar geoordeeld dat artikel 15, lid 1, van richtlijn 2002/58 zich verzet tegen de algemene en ongedifferentieerde bewaring van uitsluitend de aan de bron van een verbinding toegewezen IP-adressen voor andere doeleinden dan de bestrijding van zware criminaliteit, het voorkomen van ernstige bedreigingen van de openbare veiligheid of de bescherming van de nationale veiligheid. Om tot die slotsom te komen, heeft het Hof zich evenwel uitdrukkelijk gebaseerd op het feit dat een dergelijke

bewaring van IP-adressen een ernstige inmenging inhoudt in de door de artikelen 7, 8 en 11 van het Handvest gewaarborgde grondrechten.

78. Het Hof heeft namelijk in punt 153 van dat arrest geoordeeld dat IP-adressen - onder meer wanneer zij worden gebruikt om de ‘ volledige zoekgeschiedenis van een internetgebruiker te traceren ’ en dus om een volledig beeld te krijgen van diens online activiteit - het mogelijk maken om een ‘ gedetailleerd profiel ’ van de betrokkene op te stellen, waardoor de voor een dergelijke tracking noodzakelijke bewaring en analyse van IP-adressen ernstige inmengingen in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten van de betrokkene vormen, die de gebruikers van elektronische communicatiemiddelen ook kunnen ontmoedigen om hun door artikel 11 van het Handvest gewaarborgde vrijheid van meningsuiting uit te oefenen.

79. Niettemin moet worden benadrukt dat niet elke algemene en ongedifferentieerde bewaring van een eventueel uitgebreide verzameling statische en dynamische IP-adressen die een persoon gedurende een bepaalde periode gebruikt, noodzakelijkerwijs een ernstige inmenging in de door de artikelen 7, 8 en 11 van het Handvest gewaarborgde grondrechten vormt.

80. In dat verband hadden de zaken die hebben geleid tot het arrest van 6 oktober 2020, *La Quadrature du Net e.a.* (C-511/18, C-512/18 en C-520/18, EU:C:2020:791), betrekking op nationale regelingen die een bewaarplicht inhielden voor een verzameling gegevens die nodig waren om de datum, het tijdstip, de duur en de aard van die communicatie te bepalen, het gebruikte communicatiemateriaal te identificeren en de eindapparatuur en de communicatie te lokaliseren. Tot die gegevens behoorden in het bijzonder de naam en het adres van de gebruiker, het telefoonnummer van de beller en het gebelde nummer, en het IP-adres voor de internetdiensten. Bovendien leken de betrokken nationale regelingen in twee van die zaken ook te gelden voor de gegevens betreffende het overbrengen van elektronische communicatie via netwerken, die het ook mogelijk maakten om de aard van de online geraadpleegde informatie te bepalen (zie in die zin arrest van 6 oktober 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punten 82 en 83).

81. De bewaring van IP-adressen in het kader van dergelijke nationale regelingen maakte het dus - gelet op de andere gegevens die volgens deze regelingen moesten worden bewaard en de mogelijkheid om deze verschillende gegevens te combineren - mogelijk om nauwkeurige gevolgtrekkingen te maken over het privéleven van de personen van wie de gegevens waren bewaard, en kon dus leiden tot een ernstige inmenging in de grondrechten die zijn verankerd in de artikelen 7 en 8 van het Handvest, die betrekking hebben op de bescherming van het privéleven en de persoonsgegevens van die personen, en in de grondrechten die zijn verankerd in artikel 11 van het Handvest, dat betrekking heeft op de vrijheid van meningsuiting van die personen.

82. De bij een wettelijke maatregel krachtens artikel 15, lid 1, van richtlijn 2002/58 aan aanbieders van elektronische-communicatiediensten opgelegde verplichting om te zorgen voor een algemene en ongedifferentieerde bewaring van IP-adressen kan daarentegen in voorkomend geval worden gerechtvaardigd door de doelstelling van bestrijding van strafbare feiten in het algemeen, wanneer daadwerkelijk is uitgesloten dat die bewaring kan leiden tot ernstige inmenging in het privéleven van de betrokkene doordat daarover nauwkeurige gevolgtrekkingen kunnen worden gemaakt, onder meer door die IP-adressen te koppelen aan een verzameling verkeers- of locatiegegevens die ook door deze aanbieders zijn bewaard.

83. Bijgevolg moet een lidstaat die aanbieders van elektronische-communicatiediensten wil verplichten tot de algemene en ongedifferentieerde bewaring van IP-adressen teneinde een doel te bereiken dat verband houdt met de bestrijding van strafbare feiten in het algemeen, zich ervan vergewissen dat die gegevens zodanig worden bewaard dat met inachtneming van richtlijn 2002/58 elke combinatie van die IP-adressen met andere bewaarde gegevens wordt uitgesloten, zodat het niet mogelijk is om nauwkeurige gevolgtrekkingen te maken over het privéleven van de personen van wie de gegevens aldus worden bewaard.

84. Om ervoor te zorgen dat een dergelijke combinatie van gegevens op basis waarvan nauwkeurige gevolgtrekkingen kunnen worden gemaakt over het privéleven van de betrokkene, wordt uitgesloten, moet de wijze van bewaring betrekking hebben op de structuur zelf van de bewaring, die in wezen zodanig moet worden ingericht dat een daadwerkelijk volledige scheiding van de verschillende categorieën bewaarde gegevens wordt gegarandeerd.

85. In dit verband staat het weliswaar aan de lidstaat die aanbieders van elektronische-communicatiediensten wil verplichten tot de algemene en ongedifferentieerde bewaring van IP-adressen teneinde een doel te bereiken dat verband houdt met de bestrijding van strafbare feiten in het algemeen, om in zijn wetgeving te voorzien in duidelijke en nauwkeurige regels inzake genoemde wijzen van bewaring, die moeten voldoen aan strikte vereisten, maar kan het Hof deze wijzen nader toelichten.

86. In de eerste plaats moeten de in het vorige punt genoemde nationale regels garanderen dat elke categorie gegevens, met inbegrip van de gegevens betreffende de burgerlijke identiteit en de IP-adressen, volledig gescheiden van de andere categorieën bewaarde gegevens wordt bewaard.

87. In de tweede plaats moeten deze regels waarborgen dat de verschillende categorieën bewaarde gegevens, met name de gegevens betreffende de burgerlijke identiteit, de IP-adressen, de verschillende verkeersgegevens – anders dan IP-adressen – en de verschillende locatiegegevens, technisch volledig van elkaar gescheiden zijn doordat een beveiligd en betrouwbaar IT-instrument wordt gebruikt.

88. In de derde plaats mogen die regels, voor zover zij voorzien in de mogelijkheid om de bewaarde IP-adressen te koppelen aan de burgerlijke identiteit van de betrokkene met inachtneming van de vereisten van artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 van het Handvest, een dergelijke koppeling slechts mogelijk maken met behulp van een efficiënt technisch procedé dat geen afbreuk doet aan de doeltreffendheid van de volledige scheiding van deze categorieën gegevens.

89. In de vierde plaats moet de betrouwbaarheid van deze volledige scheiding regelmatig worden getoetst door een andere overheidsinstantie dan die welke toegang wenst te verkrijgen tot de door de aanbieders van elektronische-communicatiediensten bewaarde persoonsgegevens.

90. Voor zover in de toepasselijke nationale wetgeving is voorzien in dergelijke strikte vereisten met betrekking tot de wijzen van algemene en ongedifferentieerde bewaring van IP-adressen en andere door de aanbieders van elektronische-communicatiediensten bewaarde gegevens, kan de uit deze bewaring van IP-adressen voortvloeiende inmenging niet wegens de structuur zelf van die bewaring als ‘ ernstig ’ worden aangemerkt.

91. Wanneer een dergelijke wetgeving wordt ingevoerd, sluiten de aldus voorgeschreven wijzen van bewaring van IP-adressen namelijk uit dat deze gegevens kunnen worden gekoppeld aan andere gegevens die met inachtneming van richtlijn 2002/58 worden bewaard, zodat het niet mogelijk is om nauwkeurige gevolgtrekkingen over het privéleven van de betrokkene te maken.

92. Wanneer er sprake is van wetgeving die voldoet aan de in de punten 86 tot en met 89 van dit arrest uiteengezette vereisten, zodat het gegarandeerd wordt uitgesloten dat er nauwkeurige gevolgtrekkingen over het privéleven van de betrokkene kunnen worden gemaakt door gegevens te koppelen, verzet artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 van het Handvest, zich er dus niet tegen dat de betrokken lidstaat een verplichting tot algemene en ongedifferentieerde bewaring van IP-adressen oplegt met het oog op de bestrijding van strafbare feiten in het algemeen.

93. Ten slotte moet dergelijke wetgeving, zoals blijkt uit punt 168 van het arrest van 6 oktober 2020, *La Quadrature du Net e.a.* (C-511/18, C-512/18 en C-520/18, EU:C:2020:791), bepalen dat de bewaringstermijn tot het strikt noodzakelijke wordt beperkt en, door het gebruik van duidelijke en nauwkeurige regels, verzekeren dat de betrokken gegevens slechts worden bewaard indien aan de daarvoor geldende materiële en procedurele voorwaarden wordt voldaan, en dat de betrokken personen beschikken over effectieve waarborgen tegen het risico van misbruik en tegen onrechtmatige toegang tot en onrechtmatig gebruik van die gegevens ».

B.46.1. Artikel 126, § 1, eerste lid, van de wet van 13 juni 2005 heeft betrekking op zeventien identificatiegegevens die de voormelde operatoren moeten bewaren wanneer zij die gegevens verwerken of genereren in het kader van de diensten en netwerken die zij verstrekken. Het gaat om het Rijksregisternummer of een equivalent nummer, de naam en voornaam van de eindgebruiker die een natuurlijke persoon is of de naam van de abonnee die een rechtspersoon is (1°); de eventuele alias gekozen door de eindgebruiker bij de inschrijving op of de activering van de dienst (2°); de contactgegevens van de abonnee die verstrekt zijn bij de inschrijving op de dienst, met name zijn telefoonnummer, zijn e-mailadres en zijn postadres (3°); de datum en het tijdstip van inschrijving op de dienst en van activering van de dienst, alsook de elementen aan de hand waarvan de plaats kan worden bepaald waarvandaan die inschrijving en die activering zijn uitgevoerd, met name het fysieke adres van het verkooppunt waar de inschrijving of activering heeft plaatsgevonden, of het fysieke adres van het netwerkaansluitpunt dat gediend heeft voor de inschrijving of de activering, of het IP-adres dat gediend heeft voor de inschrijving of de activering, alsook de bronpoort van de verbinding en het tijdstempel, of in het kader van een mobiel telefoonnetwerk, de geografische locatie van de eindapparatuur die de inschrijving of de activering aan de hand van een telefoonnummer mogelijk heeft gemaakt (4°); het fysieke leveringsadres van de dienst (5°); het facturatieadres van de dienst en de gegevens betreffende de betalingswijze en het betaalmiddel, het tijdstip van de betalingen en de referentie van de

betalingstransactie in geval van onlinebetaling (6°); de hoofddienst en de aanvullende diensten die de abonnee kan gebruiken (7°); de datum vanaf wanneer die diensten gebruikt kunnen worden, de datum van het eerste gebruik van die diensten en de datum van beëindiging van die diensten (8°); in geval van overdracht van de *identifier* van de abonnee, zoals zijn telefoonnummer, de identiteit van de operator die de *identifier* overdraagt en de identiteit van de operator naar wie de *identifier* wordt overgedragen en de datum waarop de overdracht wordt uitgevoerd (9°); het toegewezen telefoonnummer (10°); het voornaamste e-mailadres en de e-mailadressen die als alias gebruikt worden (11°); de internationale identiteit van de mobiele abonnee, « International Mobile Subscriber Identity » (afgekort « IMSI » (12°); de permanente *identifier* van het abonnement, « Subscription Permanent Identifier » (afgekort « SUPI ») (13°); de verdoken *identifier* van het abonnement, « Subscription Concealed Identifier » (afgekort « SUCI ») (14°); het IP-adres aan de bron van de verbinding, het tijdstempel van de toewijzing, alsook, in geval van gedeeld gebruik van een IP-adres van de eindgebruiker, de poorten die daaraan zijn toegewezen (15°); de *identifier* van de eindapparatuur van de eindgebruiker, of indien de operator dit niet verwerkt of genereert, de *identifier* van de apparatuur die zich het dichtst bij die eindapparatuur bevindt, met name de internationale identiteit van de mobiele apparatuur, « International Mobile Equipment Identity » (afgekort « IMEI »), de permanente identifier van de apparatuur, « Permanent Equipment Identifier » (afgekort « PEI »), het adres van de controller van de toegang tot het netwerk, « Media Access Control address » (afgekort « MAC ») (16°); de andere *identifiers* met betrekking tot de eindgebruiker, de eindapparatuur of de apparatuur het dichtst bij die eindapparatuur, die uit de technologische evolutie resulteren en die door de Koning worden bepaald, voor zover dat besluit bij wet wordt bekrachtigd binnen zes maanden na de bekendmaking van dat besluit, en op voorwaarde dat die andere *identifiers* niet op de inhoud van de elektronische communicatie slaan, noch op de elektronische-communicatiemetagegevens die informatie geven over de geadresseerde van de communicatie, zoals het IP-adres van de geadresseerde van de communicatie, of over de locatie van de eindapparatuur (17°).

B.46.2. Krachtens artikel 126, § 1, vierde lid, kan de Koning de voormelde gegevens preciseren en de vereisten inzake nauwkeurigheid en betrouwbaarheid waaraan die gegevens moeten beantwoorden, bepalen.

B.46.3. Artikel 126 preciseert niet zelf de doeleinden waarvoor die gegevens moeten worden bewaard. In dat verband wordt verwezen naar artikel 127/1, § 3, van de wet van 13 juni 2005, ingevoegd bij artikel 13 van de wet van 20 juli 2022, dat bepaalt :

« De gegevens die worden bewaard krachtens de artikelen 126 en 127, worden bewaard voor de autoriteiten en de doeleinden bedoeld in paragraaf 2, 1° tot 8°.

Enkel de autoriteiten bedoeld in paragraaf 2 mogen van een operator gegevens ontvangen die worden bewaard krachtens de artikelen 126 en 127, voor de doeleinden waarin dezelfde paragraaf voorziet, voor zover dit bepaald is door en onder de voorwaarden die vastgesteld zijn in een formele wettelijke norm.

In afwijking van het tweede lid, mogen de in paragraaf 2, 10°, bedoelde autoriteiten van een operator geen aan de bron van de verbinding toegewezen IP-adressen krijgen.

In afwijking van het tweede lid, is een verzoek van een autoriteit om van een operator een IP-adres te krijgen dat is toegewezen aan de bron van een verbinding, enkel toegestaan voor de doeleinden van de vrijwaring van de nationale veiligheid, de bestrijding van zware criminaliteit, de preventies van ernstige dreigingen tegen de openbare veiligheid en de vrijwaring van de vitale belangen van een fysieke persoon, wanneer die autoriteit in staat zou zijn om, met behulp van de informatie in haar bezit en de aan de bron van de verbinding toegewezen IP-adressen die ze van de operator heeft verkregen, het traject van een eindgebruiker op internet te achterhalen ».

Artikel 127/1, § 2, van de wet van 13 juni 2005 luidt :

« Enkel de volgende autoriteiten mogen van een operator gegevens krijgen die worden bewaard krachtens de artikelen 122 en 123, voor de doeleinden hieronder voor zover dit bepaald is door en onder de voorwaarden die vastgesteld zijn in een formele wettelijke norm :

1° de inlichtingen- en veiligheidsdiensten, teneinde de opdrachten te volbrengen die hen worden toegewezen krachtens de organieke wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten;

2° de bevoegde autoriteiten met het oog op de voorkoming van ernstige bedreigingen voor de openbare veiligheid;

3° de autoriteiten belast met het vrijwaren van de vitale belangen van natuurlijke personen;

4° de autoriteiten bevoegd voor het onderzoek van een veiligheidslek in het elektronische-communicatienetwerk of in de elektronische-communicatiedienst of in informatiesystemen;

5° de administratieve of gerechtelijke autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing of de vervolging van een online gepleegde inbreuk of een inbreuk gepleegd via een elektronische-communicatienetwerk of -dienst;

6° de administratieve of gerechtelijke autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing of de vervolging van een feit dat onder de zware criminaliteit valt;

7° de administratieve autoriteiten belast met het vrijwaren van een belangrijk economisch of financieel belang van de Europese Unie of van België, met inbegrip van de monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid;

8° de administratieve of gerechtelijke autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing of de vervolging van een feit dat een strafrechtelijke inbreuk vormt, maar niet onder de zware criminaliteit valt;

9° het [BIPT] in het kader van de controle van deze wet en de autoriteiten bevoegd voor de bescherming van de gegevens in het kader van hun controleopdrachten;

10° de autoriteiten die wettelijk gemachtigd zijn om data te hergebruiken voor doeleinden van wetenschappelijk of historisch onderzoek of voor statistische doeleinden ».

B.46.4. Wat de bewaringstermijn van de voormelde gegevens betreft, bepaalt artikel 126, § 2, van de wet van 13 juni 2005 dat de gegevens bedoeld in paragraaf 1, eerste lid, 1° tot 14°, worden bewaard zolang de elektronische-communicatiedienst wordt gebruikt en tot twaalf maanden na het einde van die dienst. De gegevens bedoeld in paragraaf 1, eerste lid, 15° en 16°, worden bewaard gedurende twaalf maanden na het einde van de sessie. Het adres van de controller van de toegang tot het netwerk (MAC) wordt evenwel bewaard gedurende zes maanden na het einde van de sessie indien de operator andere gegevens, zoals bedoeld in paragraaf 1, eerste lid, 16°, bewaart. De gegevens bedoeld in paragraaf 1, eerste lid, 17°, worden ten slotte bewaard gedurende de door de Koning bepaalde periode, die niet langer mag zijn dan twaalf maanden na het einde van de dienst.

B.47.1. Alle gegevens bedoeld in artikel 126, § 1, eerste lid, van de wet van 13 juni 2005, waaronder het « IP-adres aan de bron van de verbinding » (4° en 15°), mogen worden bewaard voor de doeleinden die zijn opgesomd in artikel 127/1, § 2, 1° tot 8°, van die wet. Die doeleinden zijn ruim omschreven en hebben onder meer betrekking op het onderzoek van een veiligheidslek in het elektronische-communicatienetwerk of in de elektronische-communicatiedienst of in informatiesystemen (4°), de preventie, het onderzoek, de opsporing of de vervolging van een online gepleegde inbreuk of een inbreuk gepleegd via een elektronische communicatiedienst of -netwerk (5°) en de preventie, het onderzoek, de opsporing of de vervolging van een feit dat een strafrechtelijke inbreuk vormt maar niet onder de zware criminaliteit valt (8°).

B.47.2. Artikel 126, § 1, eerste lid, van de wet van 13 juni 2005 beoogt bepaalde gegevens die betrekking hebben op de burgerlijke identiteit van de gebruikers van elektronische-communicatiemiddelen. Zoals in B.44.2 is vermeld, mogen die gegevens op algemene en ongedifferentieerde wijze worden bewaard ten behoeve van de vrijwaring van de nationale veiligheid, de bestrijding van al dan niet zware criminaliteit en de vrijwaring van de openbare veiligheid. De doeleinden die zijn opgesomd in artikel 127/1, § 2, 1° tot 8°, kunnen worden beschouwd als zijnde in overeenstemming met die vereiste.

B.47.3. Zoals in B.44.3 is vermeld, dient te worden vermeden dat de in het geding zijnde gegevens kunnen worden gecombineerd met andere bewaarde gegevens zodat precieze conclusies kunnen worden getrokken over het privéleven van de betrokken personen.

B.48.1. De Ministerraad voert in zijn aanvullende memorie van 30 mei 2024 dienaangaande aan dat de eis van een volledige scheiding tussen de betrokken gegevenscategorieën, zoals vermeld in het voormelde arrest van het Hof van Justitie van 30 april 2024, noodzakelijk is in het kader van de toegang van een autoriteit tot de door de operatoren van elektronische communicatie bewaarde databanken, wegens het risico dat die autoriteit die gegevens analyseert en de door die databank geboden mogelijkheden benut om die gegevens te combineren, teneinde precieze conclusies te trekken over het privéleven van de betrokkenen.

Overeenkomstig artikel 127/1, § 2, van de wet van 13 juni 2005 hebben de autoriteiten die gegevens kunnen krijgen die door de operatoren moeten worden bewaard krachtens de artikelen 122 en 123 van dezelfde wet, evenwel zelf geen toegang tot de databanken van de operatoren van elektronische communicatie, met de mogelijkheid om die gegevens te analyseren en te combineren (gegevensextractie, « pull »). Die autoriteiten moeten onder de voorwaarden van de bestreden wet en de op hen van toepassing zijnde organieke wetten een gericht verzoek richten opdat de operator van elektronische communicatie hen bepaalde bewaarde gegevens verstrekt (gegevensverstrekking, « push »), zonder dat die laatstgenoemde die autoriteiten toegang verleent tot de databank.

B.48.2. Artikel 124 van de wet van 13 juni 2005 bepaalt in dit verband :

« Indien men daartoe geen toestemming heeft gekregen van alle andere, direct of indirect betrokken personen, mag niemand :

1° met opzet kennis nemen van het bestaan van informatie van alle aard die via elektronische weg is verstuurd en die niet persoonlijk voor hem bestemd is;

2° met opzet de personen identificeren die bij de overzending van de informatie en de inhoud ervan betrokken zijn;

3° onverminderd de toepassing van de artikelen 122 en 123, met opzet kennis nemen van gegevens inzake elektronische communicatie en met betrekking tot een andere persoon;

4° de informatie, identificatie of gegevens die met of zonder opzet werden verkregen, wijzigen, schrappen, kenbaar maken, opslaan of er enig gebruik van maken ».

De artikelen 127/2 en 127/3 bepalen :

« Art. 127/2. § 1. De operatoren garanderen de kwaliteit van de bewaarde metagegevens van elektronische communicatie en, in het geval van de gegevens bewaard voor de autoriteiten, zorgen ze ervoor dat ze dezelfde kwaliteit hebben als de gegevens die worden verwerkt in het kader van de verstrekking van het elektronische-communicatienetwerk of van de elektronische-communicatiedienst.

De operatoren stellen alles in het werk om de technische verbanden te leggen tussen de gegevens bewaard voor de autoriteiten die nodig zijn om op hun vragen te antwoorden.

§ 2. Wat betreft de identiteitsgegevens van de abonnee en de metagegevens van elektronische communicatie, bewaard voor de autoriteiten :

1° garanderen de operatoren dat de bewaarde gegevens onderworpen worden aan dezelfde beveiligings- en beschermingsmaatregelen als de gegevens in het netwerk of verwerkt door de dienst;

2° nemen de operatoren maatregelen van technologische beveiliging die de bewaarde gegevens, vanaf hun registratie, onleesbaar en onbruikbaar maken voor elke persoon die niet gemachtigd is om er toegang toe te hebben;

3° mogen de operatoren de bewaarde gegevens niet gebruiken voor andere doeleinden dan de verstrekking van deze gegevens aan de autoriteiten, tenzij wanneer ze de toestemming krijgen van de betrokken abonnees, conform artikel 4, 11), van de AVG en onverminderd andere wettelijke bepalingen.

§ 3. Wat betreft de identiteitsgegevens van de abonnee en de metagegevens van elektronische communicatie dienen de operatoren :

1° de gegevens op het grondgebied van de Europese Unie te bewaren en in België de door een Belgische autoriteit gevraagde gegevens te verstrekken;

2° ervoor te zorgen dat de bewaarde gegevens na afloop van de bewaringstermijn die voor die gegevens geldt van elke drager worden verwijderd of dat deze gegevens worden geanonimiseerd;

3° ervoor te zorgen dat de bewaarde gegevens worden onderworpen aan passende technische en organisatorische maatregelen om de gegevens te beveiligen tegen vernietiging, hetzij onbedoeld hetzij onrechtmatig, tegen een onbedoeld verlies of onbedoelde wijziging of tegen niet-toegelaten of onrechtmatige opslag, verwerking, toegang of openbaarmaking, conform artikel 107/2;

4° te garanderen dat de toegang tot de bewaarde gegevens om te antwoorden op de verzoeken van de autoriteiten, enkel gebeurt door een of meer leden van de Coördinatiecel bedoeld in artikel 127/3, § 1, op manuele of op geautomatiseerde wijze;

5° ervoor te zorgen dat het gebruik van de bewaarde gegevens kan worden opgespoord.

§ 4. De in de paragraaf 3, 5°, bedoelde opspoorbaarheid wordt verwezenlijkt aan de hand van een logboek.

De operator neemt de nodige maatregelen opdat elke raadpleging van de gegevens die hij bewaart voor de autoriteiten, automatisch in het logboek een registratie van de volgende gegevens genereert : de identiteit van de persoon die de gegevens heeft geraadpleegd, het moment van de raadpleging en de geraadpleegde gegevens.

Dit logboek bevat eveneens de volgende informatie en documenten, die eventueel manueel daarin worden ingevoerd :

1° de identiteit van de vragende autoriteit, het voorwerp, de datum en het tijdstip van het verzoek, een kopie van het verzoek of een link naar dit laatste;

2° wat betreft het antwoord van de operator op het verzoek van de autoriteit : de identiteit van zijn geadresseerde, de datum en het tijdstip van de verzending ervan alsook het communicatiemiddel dat werd gebruikt voor de verzending.

Het logboek mag andere documenten of informatie bevatten, op voorwaarde dat die informatie en documenten geen vertrouwelijke informatie over het door de autoriteit gevoerde onderzoek onthullen, zoals het doel of de context ervan.

De gegevens van dit logboek worden bewaard gedurende een periode van tien jaar. Nadat deze bewaringstermijn is verstreken, worden de logboekgegevens vernietigd.

De operator neemt de passende maatregelen om de veiligheid van het logboek te garanderen. Elke wijziging van de in het logboek opgenomen gegevens is verboden. Elke raadpleging van het logboek wordt geregistreerd.

De Koning kan, na advies van de Gegevensbeschermingsautoriteit en van het Instituut, de eisen bepalen die de operatoren in acht moeten nemen wat betreft het logboek.

In het kader van de controle van de operator mogen het Instituut alsook de inspecteur-generaal en de door de inspecteur-generaal aangewezen inspecteurs binnen de Gegevensbeschermingsautoriteit, bedoeld in artikel 66, § 1, van de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit, dat logboek raadplegen of een kopie van een deel of van het geheel van dat logboek eisen.

§ 5. Indien het Instituut over aanwijzingen beschikt die zouden kunnen duiden op een inbreuk van een operator op paragraaf 2, 3 of 4, dan kan het de operator verplichten om zich te onderwerpen aan een veiligheidscontrole door een gekwalificeerde onafhankelijke instantie die de operator ter goedkeuring voorlegt aan het Instituut.

Die instantie neemt geen kennis van de verzoeken van de autoriteiten jegens de operatoren, inclusief het logboek bedoeld in paragraaf 4.

Het rapport en de resultaten van deze veiligheidscontrole worden bezorgd aan het Instituut. De kosten van de controle worden door de operator gedragen.

Art. 127/3. § 1. Bij elke operator wordt een Coördinatiecel opgericht, belast met het verstrekken aan de wettelijk bevoegde autoriteiten, op hun verzoek, van de elektronische-communicatiegegevens.

Enkel de leden van de Coördinatiecel mogen antwoorden op de verzoeken van de autoriteiten met betrekking tot de gegevens bedoeld in het eerste lid. Ze mogen echter, onder hun toezicht en binnen de grenzen van het strikt noodzakelijke, technische hulp krijgen van aangestelden van de operator.

Deze autoriteiten richten hun verzoeken tot deze cel.

In voorkomend geval kunnen verscheidene operatoren een gemeenschappelijke Coördinatiecel oprichten. In dergelijk geval neemt elke operator de nodige maatregelen opdat deze gemeenschappelijke Coördinatiecel in staat is om te antwoorden op de verzoeken die eraan worden gericht.

De Koning bepaalt, na advies van de autoriteiten bevoegd voor de bescherming van de gegevens en van het Instituut, de vereisten waaraan de Coördinatiecel moet beantwoorden, in het bijzonder op het vlak van beschikbaarheid en bereikbaarheid.

§ 2. De leden van de Coördinatiecel en de aangestelden die technische bijstand verlenen, zijn onderworpen aan het beroepsgeheim. Deze leden delen aan de aangestelden enkel de gegevens mee die strikt noodzakelijk zijn om die bijstand te krijgen.

Elke operator waakt over de vertrouwelijkheid van de gegevens die worden behandeld door de Coördinatiecel.

De leden van de Coördinatiecel beschikken over een positief en niet-achterhaald veiligheidsadvies bedoeld in artikel 22*quinquies*/1 van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.

De administratieve instantie die bevoegd is voor de behandeling van de adviezen is de minister van Justitie.

De Koning bepaalt alternatieve veiligheidsmaatregelen die passend zijn voor de personen voor wie een veiligheidsadvies niet kan worden verstrekt wegens gebrek aan voldoende informatie.

In afwijking van het derde lid kan een in het vijfde lid bedoelde persoon deel uitmaken van de Coördinatiecel, wanneer deze alternatieve veiligheidsmaatregelen in acht worden genomen en zonder over een veiligheidsadvies te beschikken.

De Koning bepaalt, na advies van de autoriteiten bevoegd voor de bescherming van de gegevens en van het Instituut, het volgende :

1° voor de andere operatoren dan diegene die reeds over een veiligheidsofficier beschikken wegens andere activiteiten dan de Coördinatiecel, de categorieën van operatoren die vrijgesteld zijn van de verplichting om een dergelijke officier aan te stellen in functie van het aantal verzoeken ontvangen vanwege de gerechtelijke autoriteiten, alsook de regels die van toepassing zijn bij gebrek aan een dergelijke officier;

2° de vereisten waaraan een lid van de Coördinatiecel moet beantwoorden, inzonderheid wat het gebruik van de talen betreft;

3° de regels voor de toegang van de gemachtigde Belgische autoriteiten tot de contactgegevens van de Coördinatiecel en zijn leden.

§ 3. Elke operator stelt een interne procedure vast voor het beantwoorden van de verzoeken vanwege de autoriteiten om toegang tot de persoonsgegevens van eindgebruikers. Hij verstrekt aan het Instituut, op verzoek, gegevens over deze procedures, het aantal ontvangen verzoeken, de aangevoerde wettelijke grondslag en zijn antwoord.

Elke operator wordt beschouwd als verwerkingsverantwoordelijke in de zin van de AVG, voor de gegevens verwerkt op basis van de artikelen 122, 123, 126, 126/1, 126/2, 126/3 en 127.

§ 4. De Koning bepaalt, na advies van de autoriteiten bevoegd voor de bescherming van de gegevens en van het Instituut, de regels voor de samenwerking van de operatoren met de Belgische autoriteiten of met sommige van hen. Zo worden onder andere, in voorkomend geval en per betrokken autoriteit, de volgende zaken geregeld :

a) de overdrachtsmodus, de vorm en de inhoud van de verzoeken en antwoorden;

b) het dringendheidsniveau voor de behandeling van de verzoeken;

c) de antwoordtermijn;

d) de vereiste beschikbaarheid van de dienst;

e) de nadere regels voor het testen van de samenwerking;

f) de tarieven voor de vergoeding van die samenwerking.

Indien nodig en voor de toepassing van dit artikel, kan de Koning verschillende regels bepalen voor verschillende categorieën van operatoren, met name in functie van het aantal vorderingen dat zij ontvangen van de gerechtelijke autoriteiten en de inlichtingen- en veiligheidsdiensten, de plaats van vestiging en of zij al dan niet een elektronische-communicatienetwerk aanbieden in België ».

B.48.3. Zoals de Ministerraad aanvoert in zijn aanvullende memorie van 30 mei 2024 stelt de bestreden wet zodoende strenge eisen die verhinderen dat zowel de operatoren als de bevoegde autoriteiten de IP-adressen kunnen gebruiken om de volledige zoekgeschiedenis van een internetgebruiker te traceren en dus om een volledig beeld te krijgen van diens onlineactiviteit evenals om aan de hand van die gegevens een gedetailleerd profiel van de betrokkene op te stellen.

B.48.4. Overigens blijkt niet in welk opzicht de toepasselijkheid van artikel 8 van de wet van 20 juli 2022 op OTT-diensten strijdig zou zijn met het beginsel van gelijkheid en niet-discriminatie en met het wettigheidsbeginsel.

B.49. Het eerste en het tweede middel in de zaak nr. 7930, het enige middel in de zaak nr. 7931, alsook het eerste en het derde onderdeel van het tweede middel in de zaak nr. 7932 zijn niet gegrond in zoverre zij zijn afgeleid uit de schending van artikel 22 van de Grondwet, in samenhang gelezen met artikel 8 van het Europees Verdrag voor de rechten van de mens, met de artikelen 7, 8 en 52, lid 1, van het Handvest en met artikel 15, lid 1, van de richtlijn 2002/58/EG.

6. De verplichting tot identificatie van de abonnees en eindgebruikers van elektronische-communicatiediensten (artikel 12)

B.50. Het eerste en het tweede middel in de zaak nr. 7930, alsook het derde, het vierde en het zesde onderdeel van het tweede middel in de zaak nr. 7932 hebben betrekking op artikel 12 van de wet van 20 juli 2022, waarbij artikel 127 van de wet van 13 juni 2005 als volgt wordt vervangen :

« § 1. Dit artikel is van toepassing op de operatoren die in België een elektronische-communicatiedienst aanbieden aan eindgebruikers.

Het is verboden om in België, inclusief via het internet, zonder het akkoord van de buitenlandse onderneming die de voor het publiek beschikbare elektronische-communicatiedienst verstrekt, het volgende aan te bieden aan de eindgebruikers :

- voorafbetaalde kaarten of abonnementen van die onderneming die hen in staat stellen om er een elektronische-communicatiedienst te gebruiken;

- geconnecteerde voorwerpen waarin een product van die onderneming is geïntegreerd en die hen in staat stellen om er een internettoegangsdienst of een interpersoonlijke communicatiedienst van een operator te gebruiken.

De persoon die deze voorafbetaalde kaarten, deze abonnementen of deze geconnecteerde voorwerpen aanbiedt in België, verstrekt aan de officieren van gerechtelijke politie van het Instituut, wanneer zij daarom verzoeken, het bewijs van dat akkoord.

Indien de onderneming akkoord gaat, is zij de operator en schikt zij zich naar artikel 9, § 1.

§ 2. Voor de toepassing van dit artikel wordt verstaan onder :

1° ‘ elektronische-communicatiebetaaldienst ’ : een elektronische-communicatiedienst waarbij de abonnee moet betalen aan de operator om de dienst te gebruiken of te blijven gebruiken, evenals elke elektronische-communicatiedienst die samen met deze dienst zonder meerkosten door de operator wordt aangeboden aan de abonnee;

2° ‘ gratis elektronische-communicatiedienst ’ : de elektronische-communicatiedienst aangeboden door de operator aan de abonnee die geen elektronische-communicatiebetaaldienst is;

3° ‘ directe identificatiemethode ’ : de methode waarbij de operator voor de behoeften van de autoriteiten bedoeld in artikel 127/1, § 3, eerste lid :

- betrouwbare gegevens verzamelt en bewaart met betrekking tot de burgerlijke identiteit van een natuurlijke persoon, die zijn abonnee is of die optreedt voor rekening van een rechtspersoon die abonnee is van de operator om de verplichtingen inzake identificatie van de rechtspersoon te vervullen en, in voorkomend geval;

- een kopie van het identificatiedocument van deze natuurlijke persoon verzamelt en bewaart;

4° ‘ indirecte identificatiemethode ’ : de methode waarbij de operator gegevens verzamelt en bewaart aan de hand waarvan de in artikel 127/1, § 3, eerste lid, bedoelde autoriteiten van een derde de identiteit van zijn abonnees kunnen krijgen;

5° ‘ verkooppunt ’ : het fysiek verkooppunt van voorafbetaalde kaarten of abonnementen van een operator.

§ 3. De operator die een elektronische-communicatiebetaaldienst verstrekt, identificeert zijn abonnees door middel van een directe of indirecte identificatiemethode, met uitzondering van de indirecte identificatiemethodes bedoeld in paragraaf 10, eerste lid, 1° en 2°.

In afwijking van het tweede lid mag de in dat lid bedoelde operator de abonnee ook identificeren aan de hand van de indirecte identificatiemethode bedoeld in paragraaf 10, eerste lid, 2°, wanneer hij elektronische-communicatiediensten aanbiedt waarvoor de directe en indirecte identificatiemethodes bedoeld in het tweede lid belangrijke lasten met zich meebrengen voor de abonnees en de operator, namelijk :

- de vaste internettoegangsdiensten die worden gebruikt door natuurlijke personen buiten hun verblijfplaats en de plaats waar ze een beroepsactiviteit uitoefenen, zoals de elektronische-communicatiediensten die worden verstrekt door middel van WiFi hotspots van de operatoren;

- de andere diensten bepaald door de Koning.

Een operator die een gratis elektronische-communicatiedienst verstrekt, identificeert zijn abonnees aan de hand van een indirecte identificatiemethode zoals bedoeld in paragraaf 10.

§ 4. Het is verboden voor de verkooppunten om identificatiegegevens of kopieën van identiteitsdocumenten te bewaren, of deze voor enig ander doeleinde te gebruiken dan de identificatie van de abonnee.

De operatoren nemen de gepaste en evenredige technische en organisatorische maatregelen voor de tenuitvoerlegging van het in het eerste lid bedoelde verbod, door onder andere de verkooppunten toe te staan om de identificatiegegevens en de kopieën van identificatiedocumenten rechtstreeks in te voeren in hun computersystemen.

Indien een rechtstreekse invoer in de computersystemen van de operator tijdelijk niet mogelijk is door een storing in deze systemen, worden de identificatiegegevens en de kopieën van identificatiedocumenten die het verkooppunt op het moment van de storing heeft bewaard, vernietigd, uiterlijk na de activering van de elektronische-communicatiedienst.

Behoudens andersluidende wettelijke bepaling, worden de identificatiegegevens en de kopieën van identificatiedocumenten vergaard krachtens dit artikel bewaard vanaf de datum van activering van de dienst tot twaalf maanden na de stopzetting van de elektronische-communicatiedienst.

§ 5. De operator stelt alles in het werk om de betrouwbaarheid van de identificatie van de abonnee die een natuurlijke persoon is te garanderen.

Wanneer de operator de abonnee identificeert aan de hand van een identificatiedocument, vergewist hij zich ervan :

- dat de vergaarde identificatiegegevens overeenstemmen met de gegevens op het document;

- dat de geldigheidsdatum van dat document niet overschreden is op het ogenblik van de identificatie van de abonnee.

Wanneer de operator de abonnee identificeert aan de hand van een identificatiedocument, stelt hij alles in het werk om te controleren :

- of het document het origineel is, leesbaar is en de indruk geeft van authenticiteit;

- dat dit document betrekking heeft op de geïdentificeerde persoon.

Teneinde de betrouwbaarheid bedoeld in het eerste lid te garanderen en identiteitsfraudes te vermijden, kan de operator of het verkooppunt automatisch een vergelijking uitvoeren tussen de biometrische gegevens op de foto van het identificatiedocument van de abonnee en deze van zijn gezicht, volgens deze voorwaarden :

1° de vergelijkingstool werd toegestaan door de minister en de minister van Justitie, na verificatie dat deze tool de betrouwbaarheid van de identificatie van de abonnee voor de behoeften van de autoriteiten garandeert, in het bijzonder rekening houdende met het risico van identiteitsfraude vanwege de persoon die zich identificeert;

2° de operator biedt de abonnee minstens een alternatieve manier aan om zich te identificeren;

3° de abonnee heeft zijn uitdrukkelijke instemming gegeven in de zin van artikel 4, 11), van de AVG, wat met name inhoudt dat de abonnee op de hoogte is van de doeleinden waarvoor deze gegevens zullen worden verzameld, te weten de tenuitvoerbrenging van de wettelijke verplichting tot identificatie van de abonnee op betrouwbare wijze en de strijd tegen identiteitsfraude;

4° de operator en het verkooppunt mogen deze biometrische gegevens niet meedelen aan een derde als bedoeld in artikel 4, 10), van de AVG en zij mogen deze maar verwerken binnen de grenzen van wat nodig is om de in dit lid beoogde doeleinden van gezichtsvergelijking te verwezenlijken;

5° het is verboden om deze biometrische gegevens te bewaren na die vergelijking.

Wanneer de abonnee zich aan de hand van een Belgische elektronische identiteitskaart identificeert en de operator de in het vierde lid bedoelde methode van gezichtsvergelijking niet heeft toegepast, kan de operator aan de abonnee vragen om de pincode in te tikken.

§ 6. De toegestane identificatiedocumenten ter identificatie van de abonnee die een natuurlijke persoon is, zijn de volgende :

1° de Belgische elektronische identiteitskaart;

2° het Belgisch paspoort;

3° het bewijs van inschrijving in het vreemdelingenregister - tijdelijk verblijf, afgeleverd voor 11 oktober 2021, op voorwaarde dat deze nog steeds geldig is (A-kaart);

4° de beperkte verblijfstitel (A-kaart);

5° het bewijs van inschrijving in het vreemdelingenregister, afgeleverd voor 11 oktober 2021, op voorwaarde dat deze nog steeds geldig is (B-kaart);

6° de onbeperkte verblijfstitel (B-kaart);

7° de identiteitskaart voor vreemdelingen, afgeleverd voor 11 oktober 2021, op voorwaarde dat deze nog steeds geldig is (C-kaart);

8° de vestigingsvergunning (K-kaart);

9° de EU-verblijfstitel voor langdurig ingezetenen, afgeleverd voor 11 oktober 2021, op voorwaarde dat deze nog steeds geldig is (D-kaart);

10° de EU-verblijfstitel voor langdurig ingezetenen (L-kaart);

11° de verklaring van inschrijving, afgeleverd voor 10 mei 2021, op voorwaarde dat deze nog steeds geldig is (E-kaart);

12° het document van inschrijving ‘ Art. 8 RL 2004/38/EG ’ E (EU-kaart);

13° het document ter staving van duurzaam verblijf, afgeleverd voor 10 mei 2021, op voorwaarde dat deze nog steeds geldig is (E+-kaart);

14° het document van duurzaam verblijf ‘ Art. 19 RL 2004/38/EG ’ (EU+-kaart);

15° de verblijfskaart van een familielid van een burger van de Unie, afgeleverd voor 11 oktober 2021, op voorwaarde dat deze nog steeds geldig is (F-kaart);

16° de verblijfskaart van een familielid van een burger van de Unie ‘ familielid EU - Art. 10 RL 2004/38/EG ’ (F-kaart);

17° de duurzame verblijfskaart van een familielid van een burger van de Unie, afgeleverd voor 11 oktober 2021, op voorwaarde dat deze nog steeds geldig is (F+-kaart);

18° de duurzame verblijfskaart van een familielid van een burger van de Unie ‘ Familielid EU -Art. 20 RL 2004/38/EG ’ (F+-kaart);

19° de Europese blauwe kaart (H-kaart);

20° de vergunning voor een binnen een onderneming overgeplaatste persoon ‘ ICT ’ (I-kaart);

21° de vergunning voor lange-termijnmobiliteit ‘ mobiele ICT ’ (J-kaart);

22° de verblijfskaart voor begunstigden van het terugtrekkingsakkoord ‘ Artikel 50 VEU ’ (M-kaart);

23° de duurzame verblijfskaart voor begunstigden van het terugtrekkingsakkoord ‘ Artikel 50 VEU ’ (M-kaart);

24° de kaart voor klein grensverkeer voor begunstigden van het terugtrekkingsakkoord ‘ Artikel 50 VEU – grensarbeider ’ (N-kaart);

25° de akte van bekendheid;

26° de bijlage 12 verstrekt krachtens artikel 6 van het koninklijk besluit van 25 maart 2003 betreffende de identiteitskaarten of krachtens artikel 36*bis* van het koninklijk besluit van 8 oktober 1981 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen;

27° het attest van immatriculatie (oranje kaart);

28° de buitenlandse identiteitskaart, wanneer een internationaal paspoort niet nodig is om in België te verblijven;

29° de bijzondere identiteitskaarten verstrekt aan de categorieën van personeel dat actief is in diplomatieke en consulaire zendingen en aan hun familieleden, krachtens de Verdragen van Wenen van 1961 en 1963 en het koninklijk besluit van 30 oktober 1991 betreffende de documenten voor het verblijf in België van bepaalde vreemdelingen;

30° de identiteitskaart verstrekt conform de Conventies van Genève van 12 augustus 1949 inzake de bescherming van de slachtoffers van internationale gewapende conflicten;

31° het buitenlands paspoort;

32° elk ander document bepaald door de Koning, op voorwaarde dat het koninklijk besluit bij wet wordt bekrachtigd binnen zes maanden na de bekendmaking van dit besluit.

De operatoren die over verkooppunten beschikken, maken het voor hun abonnees mogelijk om zich te identificeren aan de hand van om het even welke van de in het eerste lid bedoelde identificatiedocumenten, in het kader van minstens één identificatiemethode van hun keuze.

In afwijking van het tweede lid kan een operator weigeren om een abonnee te identificeren op basis van een ander identificatiedocument dat is vermeld in het eerste lid dan de Belgische elektronische identiteitskaart indien hij hem de mogelijkheid biedt zich te identificeren op een van de alternatieve wijzen vermeld in het koninklijk besluit van 27 november 2016 betreffende de identificatie van de eindgebruiker van mobiele openbare elektronische-communicatiediensten die worden geleverd op basis van een voorafbetaalde kaart en voor zover de abonnee in staat is die alternatieve wijze te gebruiken.

Wanneer de operator een abonnee identificeert uitgaande van een identificatiedocument, bewaart hij een kopie van dat document, behalve als het gaat om de Belgische elektronische identiteitskaart.

De operatoren nemen de passende en evenredige maatregelen van technische en organisatorische aard teneinde te verhinderen dat de verkooppunten of derden een kopie nemen van de Belgische elektronische identiteitskaart, zulks onverminderd paragraaf 4, derde lid.

§ 7. Onverminderd artikel 126 bewaart de operator het rijksregisternummer, de naam en voornaam van zijn abonnee die een natuurlijke persoon is, wanneer hij die abonnee identificeert aan de hand van zijn Belgische elektronische identiteitskaart.

Onverminderd artikel 126 bewaart de operator, bij het identificeren van de abonnee via een ander document dan de Belgische elektronische identiteitskaart of aan de hand van een andere

directe identificatiemethode dan de overlegging van een identificatiedocument, tussen de volgende gegevens diegene die op het voorgelegde identificatiedocument staan of diegene die worden verwerkt tijdens de toepassing van de directe identificatiemethode :

1° de naam en voornaam;

2° de nationaliteit;

3° de geboortedatum;

4° het adres van de woonplaats, het e-mailadres en het telefoonnummer;

5° het nummer van het identificatiedocument en het land van uitgifte van het document wanneer het een buitenlands document betreft;

6° het verband tussen de nieuwe elektronische-communicatiedienst waarop de abonnee intekent en de dienst waarvoor hij reeds werd geïdentificeerd.

§ 8. Wanneer een operator op basis van een voorafbetaalde kaart een mobiele elektronische-communicatiedienst aanbiedt aan een abonnee die een rechtspersoon is en die hij identificeert aan de hand van een directe identificatiemethode, vergaart en bewaart hij de burgerlijke identiteit van een natuurlijke persoon die handelt voor rekening van de rechtspersoon, conform de vereisten bedoeld in de paragrafen 4 tot 7.

§ 9. Wat de directe identificatiemethodes betreft, kan de Koning :

1° de enige methodes vastleggen die de operatoren mogen gebruiken;

2° per methode bepalen aan welke voorwaarden moet worden voldaan, onder meer door een door een onderneming voorgestelde identificatiemethode te onderwerpen aan een voorafgaande machtiging van de minister en van de minister van Justitie;

3° verplichtingen opleggen aan de operatoren, aan de verkooppunten, aan de ondernemingen die een identificatiedienst verstrekken en aan de abonnees, met het oog op de identificatie van deze laatsten.

§ 10. De operator maakt het voor de autoriteiten bedoeld in artikel 127/1, § 3, eerste lid, mogelijk om zijn abonnees te identificeren via een indirecte identificatiemethode :

1° door de bewaring, overeenkomstig artikel 126 en gedurende de in dat artikel bepaalde termijnen, van het IP-adres dat werd gebruikt om zich op de elektronische-communicatiedienst in te tekenen of om deze dienst te activeren, het IP-adres aan de bron van de verbinding en de gegevens die daarbij bewaard moeten worden, of;

2° door de vergaring en bewaring van het telefoonnummer van de abonnee dat werd toegewezen in het kader van een elektronische-communicatiebetaaldienst waarvoor een operator de abonnee moet identificeren krachtens dit artikel, of;

3° in geval van een onlinebetaling specifiek voor de intekening op een elektronische-communicatiedienst, door de vergaring en bewaring van :

- het kenmerk van de betalingsverrichting, en;

- de naam, de voornaam, het verblijfadres en de geboortedatum opgegeven door de natuurlijke persoon die de abonnee van de operator is of die handelt voor rekening van een rechtspersoon die de abonnee van de operator is, teneinde zijn verplichtingen inzake identificatie te vervullen, of;

4° in geval van een simkaart (‘ subscriber identity/identification module ’) of andere gelijkwaardige kaart die in een voertuig wordt ingebouwd, door de vergaring en bewaring van het chassisnummer van het voertuig en van de link tussen het chassisnummer en het nummer van de kaart;

5° in geval van een intekening van een abonnee die in een gesloten centrum of woonunit verblijft in de zin van de artikelen 74/8 en 74/9 van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen, op een mobiele elektronische-communicatiedienst verstrekt door middel van een voorafbetaalde kaart, door de vergaring en bewaring van de naam en de voornaam van de abonnee, zijn openbaar veiligheidsnummer, zijnde het door de Dienst Vreemdelingenzaken toegekende dossiernummer, en de contactgegevens van het centrum of de woonunit waar de intekening heeft plaatsgevonden, of :

6° in geval van intekening op een elektronische-communicatiedienst door een rechtspersoon namens en voor rekening van een natuurlijke persoon die moeilijkheden heeft om die intekening te verrichten, door de vergaring en bewaring van de precieze benaming van de rechtspersoon en, wat de natuurlijke persoon in kwestie betreft, minimaal zijn naam, zijn voornaam, zijn verblijfadres als hij dat heeft, zijn geboortedatum en het nummer op basis waarvan hij is geïdentificeerd, zoals een rijksregisternummer, welke hem wordt meegedeeld door de rechtspersoon.

Voor de toepassing van het eerste lid, 6° :

1° moet de rechtspersoon, alvorens te kunnen intekenen op een elektronische-communicatiedienst voor de natuurlijke persoon, een erkenning verkrijgen, verstrekt door de minister en de minister van Justitie, en met als voorwerp om na te gaan dat de persoon de democratische waarden vastgelegd in de Grondwet alsook dit artikel nakomt;

2° identificeert de rechtspersoon zich bij de operator overeenkomstig dit artikel;

3° identificeert de rechtspersoon de abonnees aan de hand van een van de identificatiedocumenten bedoeld in paragraaf 6, conform de vereisten inzake betrouwbaarheid bedoeld in paragraaf 5, of aan de hand van een andere methode die toegestaan is in de in de bepaling onder 1° bedoelde erkenning;

4° bewaart de rechtspersoon een kopie van het andere identificatiedocument van de abonnees dan de Belgische elektronische identiteitskaart, behoudens afwijking toegestaan in de in de bepaling onder 1° bedoelde erkenning;

5° bewaart de rechtspersoon een geactualiseerde lijst aan de hand waarvan het verband kan worden vastgesteld tussen de elektronische-communicatiedienst en de abonnees, met daarin

ten minste de naam, de voornaam, het verblijfadres als de persoon dat heeft, de geboortedatum en het nummer op basis waarvan hij is geïdentificeerd, zoals het rijksregisternummer.

De Koning kan :

1° per in het eerste lid vermelde methode de voorwaarden vastleggen die moeten worden nageleefd, waarbij een voorwaarde het verkrijgen van een voorafgaande machtiging van de minister en van de minister van Justitie kan zijn;

2° verplichtingen opleggen aan de operatoren, aan de in het eerste lid bedoelde rechtspersonen, aan de ondernemingen die een identificatiedienst verstrekken en aan de abonnees, met het oog op de identificatie van deze laatsten.

§ 11. Behoudens tegenbewijs wordt de geïdentificeerde persoon geacht zelf de elektronische-communicatiedienst te gebruiken.

De Koning, voor de mobiele elektronische-communicatiediensten verstrekt op basis van een voorafbetaalde kaart:

1° beperkt de mogelijkheid voor de abonnee om derden gebruik te laten maken van de dienst;

2° legt verplichtingen op aan de abonnees die rechtspersonen zijn om de gewoonlijke gebruikers van de dienst te identificeren.

De operator die een simkaart of een gelijkwaardige kaart aanbiedt die bestemd is om in een voertuig te worden ingebouwd, bewaart het chassisnummer van dat voertuig, evenals de link tussen het chassisnummer en het nummer van deze kaart. Op verzoek van een autoriteit deelt de operator haar enkel dat chassisnummer of het nummer van deze kaart mee.

De Koning kan de nadere regels van de verplichting bedoeld in het derde lid vastleggen en kan de ondernemingen die over het chassisnummer beschikken, verplichten om dat door te geven aan de operatoren.

§ 12. Indien een operator niet voldoet aan de hem door dit artikel of door de Koning opgelegde maatregelen, is het hem verboden de dienst waarvoor de betrokken maatregelen niet genomen zijn, aan te bieden.

De operatoren sluiten de abonnees die niet voldoen aan de hen door dit artikel of door de Koning opgelegde maatregelen af van de netwerken en diensten waarop de opgelegde maatregelen van toepassing zijn. Die abonnees worden op geen enkele wijze vergoed voor de afsluiting.

Het koninklijk besluit bedoeld in dit artikel wordt voorgesteld door de minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie en de minister, maakt het voorwerp uit van een advies van de Gegevensbeschermingsautoriteit en van het Instituut en wordt vastgesteld na overleg in de Ministerraad. ’ ».

B.51.1. De verzoekende partij in de zaak nr. 7930 leidt een eerste en een tweede middel af uit de schending van de artikelen 11, 12, 22 en 29 van de Grondwet, van artikel 15, lid 1, en van de artikelen 5, 6 en 9 van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8, 11, 47 en 52, lid 1, van het Handvest, van de artikelen 6, 8, 10, 11 en 18 van het Europees Verdrag voor de rechten van de mens en van de artikelen 13 en 54 van de richtlijn (EU) 2016/680, in zoverre artikel 12 van de wet van 20 juli 2022 een algemene verplichting invoert om identificatiegegevens te bewaren, zonder dat die bewaring noodzakelijk noch strikt beperkt blijkt ten opzichte van het nagestreefde doel. Zij voert in het bijzonder aan dat dit systeem niet in overeenstemming is met de rechtspraak van het Hof van Justitie betreffende artikel 15 van de richtlijn 2002/58/EG en de artikelen 7, 8 en 52 van het Handvest, die een dergelijke bewaring enkel toestaat met het oog op de vrijwaring van de nationale veiligheid, de strijd tegen zware criminaliteit en het voorkomen van ernstige bedreigingen van de openbare veiligheid.

Uit de uiteenzettingen van het eerste en het tweede middel betreffende artikel 12 van de wet van 20 juli 2022 blijkt dat de grieven van die verzoekende partij moeten worden geïnterpreteerd in die zin dat zij in dat kader uitsluitend betrekking hebben op de lijst van de in die bepaling beoogde identificatiegegevens en de bewaringstermijn ervan, in zoverre die maatregelen niet bestaanbaar zouden zijn met het recht op eerbiediging van het privéleven en het recht op bescherming van de persoonsgegevens, die zijn gewaarborgd bij de in B.11.2 geciteerde bepalingen.

De verzoekende partij formuleert geen grief die is afgeleid uit de schending van de andere referentienormen die in het eerste en het tweede middel worden aangehaald in het kader van artikel 12 van de wet van 20 juli 2022.

B.51.2. De verzoekende partijen in de zaak nr. 7932 leiden een tweede middel af uit de schending van de artikelen 10, 11, 15, 22 en 29 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 5, 6, 8, 9, 10, 11, 14 en 18 van het Europees Verdrag voor de rechten van de mens, met de artikelen 7, 8, 11, 47 en 52 van het Handvest, met artikel 5, lid 4, van het Verdrag betreffende de Europese Unie, alsook met de richtlijn 2002/58/EG, met de richtlijn (EU) 2016/980 en met de AVG.

De grieven van de verzoekende partijen hebben in eerste instantie betrekking op artikel 127, § 5, derde lid, van de wet van 13 juni 2005 in zoverre het het gebruik van de

technologie van gezichtsherkenning zou toestaan, wat strijdig zou zijn met het recht op eerbiediging van het privéleven en met het recht op bescherming van de persoonsgegevens (derde onderdeel). Vervolgens bekritiseren de verzoekende partijen de maatregel waarin artikel 127, § 10, 4°, van de wet van 13 juni 2005 voorziet en die bepaalt, in geval van een in een voertuig ingebouwde simkaart of gelijkwaardige kaart, dat het chassisnummer van het voertuig en de link tussen het chassisnummer en het nummer van de kaart moeten worden verzameld en bewaard. Volgens hen zou die maatregel onevenredig zijn, met name door de combinatie ervan met de verplichte bewaring van de locatiegegevens op de autosnelwegen. Die grief moet zo worden geïnterpreteerd dat zij betrekking heeft op de bestaanbaarheid van de voormelde maatregel met het recht op eerbiediging van het privéleven (vierde onderdeel). Tot slot betogen de verzoekende partijen dat artikel 127, § 11, van de wet van 13 juni 2005 niet bestaanbaar is met het recht op een eerlijk proces, dat is gewaarborgd bij artikel 6 van het Europees Verdrag voor de rechten van de mens, in zoverre het een vermoeden zou invoeren dat de op grond van die bepaling geïdentificeerde persoon een elektronische-communicatiedienst gebruikt (zesde onderdeel).

B.52. Het Hof onderzoekt eerst de lijst van de gegevens die worden bewaard krachtens artikel 12 van de wet van 20 juli 2022 – waaronder de maatregel betreffende de simkaarten of andere gelijkwaardige kaarten – en de bewaringstermijn ervan (eerste en tweede middel in de zaak nr. 7930, tweede middel, vierde onderdeel, in de zaak nr. 7932), vervolgens het vermoeden van gebruik van de elektronische-communicatiedienst (tweede middel, zesde onderdeel, in de zaak nr. 7932) en, tot slot, het gebruik van de technologie van gezichtsherkenning (tweede middel, derde onderdeel, in de zaak nr. 7932).

B.53.1. Krachtens artikel 127 van de wet van 13 juni 2005, zoals vervangen bij artikel 12 van de wet van 20 juli 2022, moeten de « operatoren die in België een elektronische-communicatiedienst aanbieden aan eindgebruikers » de abonnees van die dienst identificeren (artikel 127, § 3), aan de hand van een directe of indirecte identificatiemethode (artikel 127, § 10).

De directe identificatiemethode is de methode waarbij de operator, enerzijds, « betrouwbare gegevens verzamelt en bewaart met betrekking tot de burgerlijke identiteit van een natuurlijke persoon, die zijn abonnee is of die optreedt voor rekening van een rechtspersoon die abonnee is van de operator om de verplichtingen inzake identificatie van de rechtspersoon

te vervullen » en, anderzijds, « een kopie van het identificatiedocument van deze natuurlijke persoon », ten behoeve van de autoriteiten bedoeld in artikel 127/1, § 3, eerste lid, van de wet van 13 juni 2005 (artikel 127, § 2, 3°).

De indirecte identificatiemethode is « de methode waarbij de operator gegevens verzamelt en bewaart aan de hand waarvan de in artikel 127/1, § 3, eerste lid, bedoelde autoriteiten van een derde de identiteit van zijn abonnees kunnen krijgen » (artikel 127, § 2, 4°).

B.53.2.1. De documenten die zijn toegestaan ter identificatie van de abonnee zijn die welke zijn vermeld in artikel 127, § 6, eerste lid, van de wet van 13 juni 2005. Het gaat om de Belgische elektronische identiteitskaart (1°), het Belgisch paspoort (2°), het bewijs van inschrijving in het vreemdelingenregister - tijdelijk verblijf, afgeleverd vóór 11 oktober 2021, op voorwaarde dat die nog steeds geldig is (A-kaart) (3°), de beperkte verblijfstitel (A-kaart) (4°), het bewijs van inschrijving in het vreemdelingenregister, afgeleverd vóór 11 oktober 2021, op voorwaarde dat die nog steeds geldig is (B-kaart) (5°), de onbeperkte verblijfstitel (B-kaart) (6°), de identiteitskaart voor vreemdelingen, afgeleverd vóór 11 oktober 2021, op voorwaarde dat die nog steeds geldig is (C-kaart) (7°), de vestigingsvergunning (K-kaart) (8°), de EU-verblijfstitel voor langdurig ingezetenen, afgeleverd vóór 11 oktober 2021, op voorwaarde dat die nog steeds geldig is (D-kaart) (9°), de EU-verblijfstitel voor langdurig ingezetenen (L-kaart) (10°), de verklaring van inschrijving, afgeleverd vóór 10 mei 2021, op voorwaarde dat die nog steeds geldig is (E-kaart) (11°), het document van inschrijving « Art. 8 RL 2004/38/EG » E (EU-kaart) (12°), het document ter staving van duurzaam verblijf, afgeleverd vóór 10 mei 2021, op voorwaarde dat het nog steeds geldig is (E+-kaart) (13°), het document van duurzaam verblijf « Art. 19 RL 2004/38/EG » (EU+-kaart) (14°), de verblijfskaart van een familielid van een burger van de Unie, afgeleverd vóór 11 oktober 2021, op voorwaarde dat die nog steeds geldig is (F-kaart) (15°), de verblijfskaart van een familielid van een burger van de Unie « familielid EU – Art. 10 RL 2004/38/EG » (F-kaart) (16°), de duurzame verblijfskaart van een familielid van een burger van de Unie, afgeleverd vóór 11 oktober 2021, op voorwaarde dat die nog steeds geldig is (F+-kaart) (17°), de duurzame verblijfskaart van een familielid van een burger van de Unie « Familielid EU – Art. 20 RL 2004/38/EG » (F+-kaart) (18°), de Europese blauwe kaart (H-kaart) (19°), de vergunning voor een binnen een onderneming overgeplaatste persoon « ICT » (I-kaart) (20°), de vergunning voor langetermijnmobiliteit « mobiele ICT » (J-kaart) (21°), de verblijfskaart voor begunstigden van het terugtrekkingsakkoord « Art. 50 VEU » (M-kaart) (22°), de duurzame verblijfskaart voor begunstigden van het

terugtrekkingsakkoord « Art. 50 VEU » (M-kaart) (23°), de kaart voor klein grensverkeer voor begunstigden van het terugtrekkingsakkoord « Art. 50 VEU – grensarbeider » (N-kaart) (24°), de akte van bekendheid (25°), de bijlage 12 verstrekt krachtens artikel 6 van het koninklijk besluit van 25 maart 2003 « betreffende de identiteitskaarten » of krachtens artikel 36*bis* van het koninklijk besluit van 8 oktober 1981 « betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen » (26°), het attest van immatriculatie (oranje kaart) (27°), de buitenlandse identiteitskaart, wanneer een internationaal paspoort niet nodig is om in België te verblijven (28°), de bijzondere identiteitskaarten verstrekt aan de categorieën van personeel dat actief is in diplomatieke en consulaire zendingen en aan hun familieleden, krachtens de Verdragen van Wenen van 1961 en 1963 en het koninklijk besluit van 30 oktober 1991 « betreffende de documenten voor het verblijf in België van bepaalde vreemdelingen » (29°), de identiteitskaart verstrekt conform de Conventies van Genève van 12 augustus 1949 inzake de bescherming van de slachtoffers van internationale gewapende conflicten (30°), het buitenlands paspoort (31°) en, ten slotte, elk ander document bepaald door de Koning, op voorwaarde dat het koninklijk besluit bij wet wordt bekrachtigd binnen zes maanden na de bekendmaking van dat besluit (32°).

B.53.2.2. Krachtens artikel 127, § 6, tweede lid, van de wet van 13 juni 2005, maakt de operator die over verkooppunten beschikt het voor zijn abonnee mogelijk om zich te identificeren aan de hand van om het even welk van de in het eerste lid opgesomde identificatiedocumenten. Krachtens het derde lid kan een operator evenwel weigeren om een abonnee te identificeren aan de hand van een van de voormelde identificatiedocumenten indien de abonnee de mogelijkheid heeft om zich te identificeren op een van de andere wijzen bedoeld in het koninklijk besluit van 27 november 2016 « betreffende de identificatie van de eindgebruiker van mobiele voor het publiek beschikbare elektronische-communicatiediensten die worden geleverd op basis van een voorafbetaalde kaart ». Die oplossing is niet mogelijk wanneer de abonnee wil worden geïdentificeerd aan de hand van zijn Belgische elektronische identiteitskaart.

B.53.2.3. Wanneer een abonnee wordt geïdentificeerd aan de hand van een van de voormelde identificatiedocumenten, bewaart de operator een kopie van dat document, behalve wanneer het gaat om de Belgische elektronische identiteitskaart (artikel 127, § 6, vierde lid).

B.53.3.1. Na de identificatie van een abonnee moet de operator bepaalde persoonsgegevens bewaren met toepassing van artikel 127, §§ 7 en 8, van de wet van 13 juni 2005.

B.53.3.2. Wanneer de abonnee een natuurlijke persoon is en geïdentificeerd wordt aan de hand van zijn Belgische elektronische identiteitskaart, bewaart de operator het rijksregisternummer, de naam en de voornaam van de abonnee (artikel 127, § 7, eerste lid).

B.53.3.3. Wanneer de abonnee een natuurlijke persoon is en geïdentificeerd wordt aan de hand van een ander document dan de Belgische elektronische identiteitskaart, bedoeld in artikel 127, § 6, eerste lid, 2° tot 32°, of aan de hand van een andere directe identificatiemethode dan de overlegging van een identificatiedocument, bewaart de operator, van de gegevens die op het identificatiedocument staan of die worden verwerkt tijdens de toepassing van de directe identificatiemethode, de naam en voornaam, de nationaliteit, de geboortedatum, het adres van de woonplaats, het e-mailadres, het telefoonnummer, het nummer van het identificatiedocument en het land van uitgifte van het document wanneer het een buitenlands document betreft en, ten slotte, het verband tussen de nieuwe elektronische-communicatiedienst waarop de abonnee intekent en de dienst waarvoor hij reeds werd geïdentificeerd (artikel 127, § 7, tweede lid).

B.53.3.4. Wanneer de abonnee een rechtspersoon is, de elektronische communicatiedienst wordt aangeboden op basis van een vooraf betaalde kaart en de abonnee geïdentificeerd wordt aan de hand van een directe identificatiemethode, verzamelt en bewaart de operator de gegevens bedoeld in artikel 127, §§ 4 tot 7, van de wet van 13 juni 2005, die betrekking hebben op de burgerlijke identiteit van een natuurlijke persoon die handelt voor rekening van de rechtspersoon (artikel 127, § 8).

B.53.4. Tot slot moeten de operatoren, krachtens artikel 127, § 10, van de wet van 13 juni 2005, het voor de autoriteiten bedoeld in artikel 127/1, § 3, eerste lid, van dezelfde wet mogelijk maken om hun abonnees te identificeren aan de hand van een indirecte identificatiemethode.

Daartoe bepaalt artikel 127, § 10, eerste lid, dat de operatoren, overeenkomstig artikel 126 van de wet van 13 juni 2005 en gedurende de in dat artikel bepaalde termijnen, het IP-adres bewaren dat werd gebruikt om op de elektronische-communicatiedienst in te tekenen of om die dienst te activeren, het IP-adres aan de bron van de verbinding en de gegevens die daarbij

bewaard moeten worden (1°) of het telefoonnummer van de abonnee dat werd toegewezen in het kader van een elektronische-communicatiebetaaldienst waarvoor een operator de abonnee moet identificeren overeenkomstig artikel 127 van de wet van 13 juni 2005 (2°); dat de operatoren, in geval van een onlinebetaling specifiek voor de intekening op een elektronische-communicatiedienst, het kenmerk van de betalingsverrichting en de naam, de voornaam, het verblijfadres en de geboortedatum opgegeven door de natuurlijke persoon die abonnee van de operator is of die handelt voor rekening van een rechtspersoon die abonnee van de operator is, verzamelen en bewaren om hun verplichtingen inzake identificatie te vervullen (3°) of, in geval van een in een voertuig ingebouwde simkaart of andere gelijkwaardige kaart, het chassisnummer van het voertuig en de link tussen het chassisnummer en het nummer van de kaart (4°); dat de operatoren, in geval van een intekening van een abonnee die in een gesloten centrum of woonunit verblijft in de zin van de artikelen 74/8 en 74/9 van de wet van 15 december 1980 « betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen » op een mobiele elektronische-communicatiedienst verstrekt door middel van een vooraf betaalde kaart, de naam en voornaam van de abonnee en het openbaar veiligheidsnummer verzamelen en bewaren (5°) of, in geval van intekening op een elektronische-communicatiedienst door een rechtspersoon namens en voor rekening van een natuurlijke persoon die moeilijkheden heeft om die intekening te verrichten, de precieze benaming van die rechtspersoon en, wat de natuurlijke persoon in kwestie betreft, minimaal zijn naam, zijn voornaam, zijn verblijfadres als hij dat heeft, zijn geboortedatum en het nummer op basis waarvan hij is geïdentificeerd, zoals een rijksregisternummer, waarbij die inlichtingen hun worden meegedeeld door die rechtspersoon (6°).

B.53.5. De in B.53.2.1 tot B.53.4 bedoelde gegevens worden, behoudens andersluidende wettelijke bepaling, bewaard « vanaf de datum van activering van de dienst tot twaalf maanden na de stopzetting van de elektronische-communicatiedienst » (artikel 127, § 4, vierde lid).

B.54.1. De gegevens opgesomd bij artikel 127 van de wet van 13 juni 2005 hebben tot doel de abonnees van de in die bepaling beoogde operatoren te identificeren. In de parlementaire voorbereiding van de wet van 20 juli 2022 wordt in dat verband verduidelijkt :

« Het is een wezenlijk beginsel dat een persoon rekenschap moet afleggen van zijn daden, zowel op burgerrechtelijk als op strafrechtelijk vlak. De anonimiteit brengt dat beginsel in gevaar. De mogelijkheid om de abonnee te identificeren staat toe om het ten uitvoer te leggen. Het is ook van essentieel belang dat het voor de autoriteiten (gerechtelijke autoriteiten,

inlichtingen- en veiligheidsdiensten en andere autoriteiten die bij de operatoren verkeers- of identificatiegegevens kunnen opvragen) mogelijk is om de identiteit van de abonnee te kunnen achterhalen » (*Parl. St.,* Kamer, 2021-2022, DOC 55-2572/002, p. 71).

In dat kader is het ook de bedoeling identiteitsfraude te bestrijden (*ibid.*, pp. 96 en 97).

B.54.2. Zoals in B.44.2 is vermeld, dient een onderscheid te worden gemaakt, wat de identificatiegegevens betreft, tussen de IP-adressen aan de bron, enerzijds, en de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronische-communicatiemiddelen, anderzijds.

B.55.1. Artikel 127, § 10, eerste lid, 1°, van de wet van 13 juni 2005 herinnert aan de in artikel 126, § 1, eerste lid, 4° en 15°, neergelegde verplichting, voor de operatoren, om « het IP-adres dat werd gebruikt om op de elektronische-communicatiedienst in te tekenen of om deze dienst te activeren, het IP-adres aan de bron van de verbinding en de gegevens die daarbij bewaard moeten worden » te bewaren.

B.55.2. Aangezien, om de redenen vermeld in B.48.1 tot B.48.4, artikel 126 van de wet van 13 juni 2005, ingevoegd bij artikel 8 van de wet van 20 juli 2022, de in B.49 aangehaalde referentienormen niet schendt en de thans onderzochte grieven in hoofdzaak zijn afgeleid uit de schending van dezelfde referentienormen, geldt hetzelfde wat artikel 127, § 10, eerste lid, 1°, van de wet van 13 juni 2005 betreft.

B.55.3. Het eerste en het tweede middel in de zaak nr. 7930 zijn niet gegrond in zoverre zij betrekking hebben op de in B.55.1 vermelde maatregel van gegevensbewaring.

B.56. De andere identificatiegegevens bedoeld in artikel 127, §§ 4, 6 tot 8, en 10, van de wet van 13 juni 2005 kunnen worden gelijkgesteld met gegevens betreffende de burgerlijke identiteit van de gebruikers van elektronische communicatiemiddelen omdat met enkel die gegevens noch de datum, het tijdstip, de duur en de ontvangers van een communicatie kunnen worden achterhaald, noch de plaats waar die communicatie heeft plaatsgevonden of het aantal malen dat in een specifieke periode met bepaalde personen is gecommuniceerd. Het Europees Hof voor de Rechten van de Mens en het Hof van Justitie zijn immers van oordeel dat die gegevens geen informatie verschaffen over wat die personen hebben gecommuniceerd, noch over hun privéleven. Aan de hand van die gegevens alleen kan geen profiel van de gebruiker

worden opgesteld of kunnen zijn bewegingen niet worden gevolgd (EHRM, 30 januari 2020, *Breyer t. Duitsland*, ECLI:CE:ECHR:2020:0130JUD005000112, §§ 92-95; HvJ, grote kamer, 2 oktober 2018, C-207/16, *Ministerio Fiscal*, ECLI:EU:C:2018:788, punt 62; grote kamer, 6 oktober 2020, C-511/18, C-512/18 en C-520/18, *La Quadrature du Net e.a.*, voormeld, punt 157).

Het Hof van Justitie leidt daaruit af dat het recht op eerbiediging van het privéleven zich niet verzet tegen een algemene en ongedifferentieerde verzameling, verwerking en bewaring van identificatiegegevens van gebruikers van elektronische-communicatienetwerken ten behoeve van het onderzoeken, opsporen en vervolgen van strafbare feiten en het waarborgen van de openbare veiligheid. Het hoeft daarbij niet te gaan om ernstige strafbare feiten of om ernstige bedreigingen en verstoringen van de openbare veiligheid (HvJ, grote kamer, 6 oktober 2020, C-511/18, C-512/18 en C-520/18, voormeld). Wel dient te worden aangetoond dat « die maatregelen, door het gebruik van duidelijke en nauwkeurige regels, verzekeren dat de betrokken gegevens slechts worden bewaard indien aan de daarvoor geldende materiële en procedurele voorwaarden wordt voldaan, en dat de betrokken personen beschikken over effectieve waarborgen tegen het risico van misbruik » (*ibid.*, punt 168).

Het Europees Hof voor de Rechten van de Mens toetst de algemene en ongedifferentieerde verzameling, verwerking en bewaring van die identificatiegegevens op minder intensieve wijze dan de verzameling, verwerking en bewaring van verkeers- en locatiegegevens. Het gaat na of de bewaartermijn redelijk is, rekening houdend met de gebruikelijke duur van een strafrechtelijk onderzoek. Het Europees Hof voor de Rechten van de Mens vereist niet dat er voor de verzameling en bewaring van loutere identificatiegegevens een toezicht *a priori* wordt ingesteld : een toegang *a posteriori* tot een onafhankelijke rechterlijke of bestuurlijke instantie, in samenhang met de gemeenrechtelijke rechtsmiddelen waarover de beklaagde tijdens een strafproces beschikt, volstaat (EHRM, 30 januari 2020, *Breyer t. Duitsland*, voormeld, §§ 96-107).

B.57.1. De verzoekende partijen in de zaak nr. 7932 voeren aan dat de maatregel waarin artikel 127, § 10, eerste lid, 4°, van de wet van 13 juni 2005 voorziet in geval van een in een voertuig ingebouwde simkaart of gelijkwaardige kaart, die toestaat dat het chassisnummer van het voertuig en de link tussen het chassisnummer en het nummer van de kaart worden verzameld en bewaard, een permanente tracking van dat voertuig mogelijk maakt via de

internetverbinding, meer bepaald door het combineren van dat identificatiegegeven met het locatiegegeven op de autosnelwegen waarvan de bewaring is toegestaan krachtens artikel 126/3, § 4, *c)*, van de wet van 13 juni 2005.

B.57.2. Artikel 127, § 10, eerste lid, 4°, van de wet van 13 juni 2005 staat niet toe dat de gegevens inzake de internetverbinding van de in die bepaling bedoelde voertuigen worden bewaard en verzameld.

Bovendien, is het niet mogelijk om aan de hand van het chassisnummer van het voertuig, het nummer van de simkaart of van de gelijkwaardige kaart die in het voertuig is ingebouwd, en de link tussen de voormelde nummers, iemands verplaatsingen, communicaties, activiteiten of sociale relaties te volgen, noch om een persoonlijk profiel op te stellen dat toelaat precieze conclusies te trekken over iemands seksuele geaardheid, overtuigingen en gezondheid. De voormelde gegevens geven op zich dus geen gevoelige informatie over het privéleven prijs.

Hoewel die identificatiegegevens vervolgens kunnen worden gekoppeld aan andere gegevens en op die manier kunnen bijdragen aan het vrijgeven van dergelijke gevoelige informatie over iemands privéleven, zijn die andere gegevens op een andere manier verzameld, en ook die verzameling dient te geschieden met inachtneming van de toepasselijke wetgeving en van de grondrechten van de betrokkene.

B.57.3. Het vierde onderdeel van het tweede middel in de zaak nr. 7932 is niet gegrond.

B.58.1. Wat betreft de grieven die de verzoekende partijen in de zaak nr. 7930 in hun eerste en tweede middel hebben uiteengezet, dient de bestaanbaarheid van de maatregelen inzake het verzamelen en bewaren van gegevens die zijn vastgelegd bij artikel 127, §§ 6 tot 8 en 10, eerste lid, 2° tot 6°, van de wet van 13 juni 2005, met het recht op eerbiediging van het privéleven, te worden beoordeeld aan de hand van de in B.56 vermelde criteria.

B.58.2. Uit de in B.54.1 geciteerde parlementaire voorbereiding blijkt dat de wetgever, met artikel 127 van de wet van 13 juni 2005, doelstellingen nastreefde op het gebied van het onderzoeken, opsporen en vervolgen van strafbare feiten, alsook het vrijwaren van de openbare veiligheid in de zin van artikel 15 van de richtlijn 2002/58/EG.

B.58.3.1. De materiële en procedurele voorwaarden voor de verzameling, verwerking en bewaring van de identificatiegegevens van abonnees van een elektronische-communicatienetwerk worden geregeld in de artikelen 127 en 127/3 van de wet van 13 juni 2005.

B.58.3.2. Artikel 127, § 1, eerste lid, van de wet van 13 juni 2005 bepaalt aan welke personen in dit kader verplichtingen worden opgelegd, namelijk aan de operatoren die in België een elektronische-communicatiedienst aanbieden aan eindgebruikers. Bij artikel 127/3, § 3, tweede lid, van de wet van 13 juni 2005 worden bovendien de voormelde operatoren aangewezen als verwerkingsverantwoordelijken voor de gegevens. Artikel 127 van de wet van 13 juni 2005 legt overigens het beginsel vast dat alle abonnees identificeerbaar moeten zijn en bepaalt dat de identificatie dient te gebeuren aan de hand van een directe of indirecte identificatiemethode.

B.58.3.3. Artikel 127 bepaalt de voorwaarden voor de bewaring van de verzamelde gegevens. In paragraaf 6 van die bepaling worden de documenten opgesomd die zijn toegelaten voor de identificatie van een natuurlijke persoon, die in voorkomend geval handelt voor een rechtspersoon.

De paragrafen 7 en 8 preciseren welke identificatiegegevens door de operatoren moeten worden bewaard. In paragraaf 10 worden tot slot de identificatiegegevens opgesomd die kunnen worden verzameld en bewaard om het voor de autoriteiten bedoeld in artikel 127/1, § 3, eerste lid, mogelijk te maken abonnees te identificeren aan de hand van een indirecte identificatiemethode.

B.58.3.4. Artikel 127 stelt de maximale bewaringstermijn vast voor de erin beoogde identificatiegegevens. Paragraaf 4, vierde lid, van die bepaling voorziet erin dat die gegevens worden bewaard tot twaalf maanden na de stopzetting van de elektronische-communicatiedienst, tenzij een wettelijke bepaling een andere termijn vaststelt.

B.58.3.5. Artikel 127 verbiedt overigens de verkooppunten expliciet om identificatiegegevens of kopieën van identiteitsdocumenten te bewaren, maar zij moeten die gegevens en kopieën rechtstreeks invoeren in hun computersystemen, met dien verstande dat de operatoren de gepaste en evenredige technische en organisatorische maatregelen moeten

nemen voor de tenuitvoerlegging van het voormelde verbod, door onder andere de verkooppunten toe te staan om de gegevens en de kopieën rechtstreeks in te voeren in de computersystemen (§ 4, eerste en tweede lid). Er is in een uitzondering voorzien in geval van een storing in het computersysteem waardoor de voormelde rechtstreekse invoer onmogelijk wordt. In dat geval mogen de verkooppunten de gegevens en de kopieën tijdelijk bewaren op voorwaarde dat zij uiterlijk na de activering van de elektronische-communicatiedienst worden vernietigd (§ 4, derde lid).

B.58.3.6. Tot slot is bepaald dat, indien een operator niet voldoet aan de krachtens artikel 127 van de wet van 13 juni 2005 opgelegde maatregelen, het hem verboden is de dienst waarvoor de betrokken maatregelen niet zijn genomen, aan te bieden (artikel 127, § 12, eerste lid).

B.58.3.7. Voor het overige, hoewel artikel 127 van de wet van 13 juni 2005 niet voorziet in een specifiek rechterlijk toezicht op de verwerking van de krachtens die bepaling verzamelde en bewaarde identificatiegegevens, dient evenwel in herinnering te worden gebracht, zoals in B.56 werd uiteengezet, dat inzake de verwerking van loutere identificatiegegevens de gemeenrechtelijke rechtsmiddelen volstaan (EHRM, 30 januari 2020, *Breyer t. Duitsland*, voormeld, § 106).

In het kader van de strafprocedure beschikt de beklaagde in dat verband over het recht om voor de onderzoeksgerechten of voor de vonnisrechter de nietigheid van een onderzoekshandeling aan te voeren die zijn recht op eerbiediging van het privéleven of zijn recht op een eerlijk proces schendt.

In het kader van de werking van de inlichtingen- en veiligheidsdiensten beschikt de betrokkene overigens, krachtens artikel 79 van de wet van 30 juli 2018 « betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens », over het recht om aan het Vast Comité I te vragen zijn onjuiste persoonsgegevens te laten verbeteren of verwijderen en de naleving van de toepasselijke bepalingen te verifiëren.

Daarnaast beschikt elke abonnee van een elektronische-communicatiedienst wiens identificatiegegevens in strijd met artikel 127 van de wet van 13 juni 2005 zijn verwerkt, over

een gemeenrechtelijke aansprakelijkheidsvordering tegen de persoon die die wetsbepaling heeft overtreden.

Tot slot kan de betrokkene krachtens artikel 58 van de wet van 3 december 2017 « tot oprichting van de Gegevensbeschermingsautoriteit » kosteloos een klacht indienen bij de Gegevensbeschermingsautoriteit in geval van een onrechtmatige verwerking van zijn persoonsgegevens.

B.59. Het eerste en het tweede middel in de zaak nr. 7930 zijn niet gegrond in zoverre zij betrekking hebben op de gegevens bedoeld in artikel 127, §§ 6 tot 8 en 10, eerste lid, 2° tot 6°, van de wet van 13 juni 2005.

B.60. Artikel 127, § 11, eerste lid, van de wet van 13 juni 2005 bepaalt dat « behoudens tegenbewijs [...] de geïdentificeerde persoon geacht [wordt] zelf de elektronische-communicatiedienst te gebruiken ».

Volgens de verzoekende partijen in de zaak nr. 7932 schendt die bepaling het recht op een eerlijk proces, in het bijzonder het vermoeden van onschuld, dat is gewaarborgd bij artikel 6 van het Europees Verdrag voor de rechten van de mens, in zoverre het voor de vermoedelijke eindgebruiker onmogelijk zou zijn om het tegenbewijs te leveren, inzonderheid wanneer die gebruiker publieke toegang tot zijn wifinetwerk toestaat of in geval van ongeoorloofde toegang tot dat netwerk.

B.61.1. Krachtens artikel 6, lid 2, van het Europees Verdrag voor de rechten van de mens wordt eenieder die wegens een strafbaar feit wordt vervolgd voor onschuldig gehouden totdat zijn schuld volgens de wet wordt bewezen.

B.61.2. Als procedurele waarborg in strafzaken stelt het vermoeden van onschuld eisen aan onder meer de bewijslast, wettelijke vermoedens van feitelijke en juridische aard, het recht om zichzelf niet te beschuldigen, publiciteit voorafgaand aan het proces en voorbarige uitingen door rechters of andere overheidsfunctionarissen over de schuld van een verdachte (EHRM, grote kamer, 12 juli 2013, *Allen t. Verenigd Koninkrijk,* ECLI:CE:ECHR:2013:0712JUD002542409, § 93).

B.61.3. Het recht van eenieder die wegens een strafbaar feit wordt vervolgd om voor onschuldig te worden gehouden en om te vereisen dat het openbaar ministerie de bewijslast draagt, is echter niet absoluut. In elk strafrechtelijk systeem bestaan er immers wettelijke vermoedens van feitelijke of juridische aard. Dergelijke vermoedens zijn in beginsel niet verboden, zolang zij binnen redelijke grenzen blijven, rekening houdend met de ernst van de zaak en de eerbiediging van de rechten van verdediging. Bij het gebruik van vermoedens in strafzaken moet dus een billijk evenwicht worden gevonden tussen het belang van de zaak en de rechten van verdediging. De gebruikte middelen moeten met andere woorden in verhouding staan tot het nagestreefde legitieme doel (EHRM, beslissing, 19 oktober 2004, *Falk t. Nederland*, ECLI:CE:ECHR:2004:1019DEC006627301; 23 juli 2002, *Västberga Taxi Aktiebolag en Vulic t. Zweden*, ECLI:CE:ECHR:2002:0723JUD003698597, § 113).

B.62.1. Artikel 127, § 11, eerste lid, van de wet van 13 juni 2005 vestigt geen automatische strafrechtelijke verantwoordelijkheid of objectieve aansprakelijkheid van de geïdentificeerde eindgebruiker van een vooraf betaalde belkaart voor het gebruik dat een derde daarvan maakt. Het heeft voornamelijk een waarschuwingsfunctie, aangezien het het uitgangspunt van elk strafrechtelijk onderzoek en van elk onderzoek door de inlichtingen- en veiligheidsdiensten in herinnering brengt, namelijk het uitgangspunt dat de eigenaar of gewoonlijke gebruiker van een voorwerp vermoedelijk diegene is die het heeft gebruikt om een misdrijf te plegen of om de nationale veiligheid te bedreigen. De onderzoekers verlaten dat uitgangspunt zodra het wordt ontkracht door de verzamelde bewijselementen.

B.62.2. De bestreden bepaling houdt aldus verband met de in B.54 vermelde doelstellingen die de wetgever met artikel 127 van de wet van 13 juni 2005 nastreeft.

B.62.3. Bovendien beschikt de vermoedelijke eindgebruiker over verschillende mogelijkheden om zich te verdedigen tegen strafrechtelijke vervolgingen die zouden kunnen voortvloeien uit het gebruik dat een derde van de elektronische-communicatiedienst heeft gemaakt. Indien hij aan de onderzoekers meldt wie van die dienst gebruik heeft gemaakt, dienen zij diens betrokkenheid te onderzoeken. Indien de elektronische-communicatiedienst toegankelijk wordt gemaakt voor derden, dient de vermoedelijke eindgebruiker dat mee te delen aan de onderzoekers, die moeten trachten de persoon die de dienst daadwerkelijk heeft gebruikt alsook diens betrokkenheid te identificeren.

Artikel 127, § 11, eerste lid, van de wet van 13 juni 2005 stelt overigens slechts een weerlegbaar vermoeden in, dat door de beklaagde met alle middelen van recht kan worden weerlegd. Het verbiedt hem niet om alle feitelijke elementen aan te dragen die zijn betrokkenheid bij de gepleegde misdrijven of bij de onderzochte bedreigingen voor de nationale veiligheid ontkrachten.

Daarnaast doet de voormelde bepaling geen afbreuk aan het beginsel dat het in een strafproces aan het openbaar ministerie toekomt de schuld van de beklaagde te bewijzen. Het staat aan de strafrechter de bewijswaarde van alle bewijselementen, met inbegrip van de uitleg van de beklaagde, te onderzoeken en daarbij diens recht op een eerlijk proces te eerbiedigen.

B.62.4. Artikel 127, § 11, eerste lid, van de wet van 13 juni 2005 doet geen afbreuk aan het vermoeden van onschuld.

B.63. Het zesde onderdeel van het tweede middel in de zaak nr. 7932 is niet gegrond.

B.64. Artikel 127, § 5, vierde lid, van de wet van 13 juni 2005 bepaalt dat, om een betrouwbare identificatie van de abonnee die een natuurlijke persoon is, te garanderen en identiteitsfraude te vermijden, de operator of het verkooppunt automatisch een vergelijking kan uitvoeren tussen de biometrische gegevens op de foto van het identificatiedocument van de abonnee, enerzijds, en die van zijn gezicht, anderzijds.

Volgens de verzoekende partijen in de zaak nr. 7932 wordt bij die bepaling het gebruik van gezichtsherkenningstechnologie toegestaan die het recht op eerbiediging van het privéleven en op bescherming van de persoonsgegevens, zoals het onder meer wordt gewaarborgd door de AVG, schendt in zoverre die maatregel niet noodzakelijk, noch evenredig zou zijn en evenmin het vereiste van de uitdrukkelijke en geïnformeerde toestemming van de betrokken abonnee in acht zou nemen.

B.65.1. Het recht op eerbiediging van het privéleven is niet absoluut. Artikel 22 van de Grondwet en artikel 8 van het Europees Verdrag voor de rechten van de mens sluiten een overheidsinmenging in de uitoefening van dat recht niet uit, voor zover zij wordt toegestaan door een voldoende precieze wettelijke bepaling, beantwoordt aan een dwingende

maatschappelijke behoefte in een democratische samenleving en evenredig is met de daarmee nagestreefde wettige doelstelling.

De wetgever beschikt ter zake over een beoordelingsvrijheid. Die vrijheid is evenwel niet onbegrensd : opdat een wettelijke regeling verenigbaar is met het recht op eerbiediging van het privéleven, is vereist dat de wetgever een billijk evenwicht heeft ingesteld tussen alle rechten en belangen die in het geding zijn.

B.65.2. Zoals in B.11.2 is vermeld, hebben de artikelen 7 en 8 van het Handvest bovendien, wat de verwerking van persoonsgegevens betreft, een draagwijdte die analoog is aan die van artikel 8 van het Europees Verdrag voor de rechten van de mens.

B.66.1. Artikel 5 van de AVG stelt de beginselen vast inzake de verwerking van persoonsgegevens :

« 1. Persoonsgegevens moeten :

a) worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is (‘ rechtmatigheid, behoorlijkheid en transparantie ’);

b) voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeenkomstig artikel 89, lid 1, niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd (‘ doelbinding ’);

c) toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (‘ minimale gegevensverwerking ’);

d) juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren (‘ juistheid ’);

e) worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is; persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt overeenkomstig artikel 89, lid 1, mits de bij deze verordening vereiste passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen (‘ opslagbeperking ’);

f) door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (‘ integriteit en vertrouwelijkheid ’).

2. De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van lid 1 en kan deze aantonen (‘ verantwoordingsplicht ’) ».

Artikel 9 van de AVG betreft de verwerking van bijzondere categorieën van persoonsgegevens :

« 1. Verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn verboden.

2. Lid 1 is niet van toepassing wanneer aan een van de onderstaande voorwaarden is voldaan :

a) de betrokkene heeft uitdrukkelijke toestemming gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden, behalve indien in Unierecht of lidstatelijk recht is bepaald dat het in lid 1 genoemde verbod niet door de betrokkene kan worden opgeheven;

[...]

g) de verwerking is noodzakelijk om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene;

[...] ».

Artikel 9 van de AVG moet in samenhang worden gelezen met artikel 4, punt 14), van de AVG, dat bepaalt :

« Voor de toepassing van deze verordening wordt verstaan onder :

[...]

14) ‘ biometrische gegevens ’ : persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde

kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens ».

B.66.2. Artikel 9, lid 2, *g)*, van de AVG maakt de verwerking van gevoelige persoonsgegevens, zoals biometrische gegevens, mogelijk wanneer zij « noodzakelijk [is] om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene ».

B.67.1. Uit de parlementaire voorbereiding van artikel 127, § 5, vierde lid, van de wet van 13 juni 2005 blijkt dat die bepaling ertoe strekt personen zo doeltreffend mogelijk te kunnen identificeren, met name om de strijd tegen identiteitsfraude vanwege zowel de abonnees als de verkooppunten zelf te versterken (*Parl. St.,* Kamer, 2021-2022, DOC 55-2572/002, pp. 90 en 91).

B.67.2. Bij zijn arrest nr. 2/2021 van 14 januari 2021 (ECLI:BE:GHCC:2021:ARR.002) heeft het Hof geoordeeld dat de voormelde doelstellingen legitiem zijn, aangezien zij ertoe strekken de rechten en de vrijheden van anderen te beschermen, daarenboven door de Europese Unie erkende doelstellingen van algemeen belang vormen en eveneens kunnen worden beschouwd als redenen van zwaarwegend algemeen belang, in de zin van artikel 9, lid 2, *g)*, van de AVG (B.20.2).

B.68. Artikel 127, § 5, vierde lid, van de wet van 13 juni 2005 is relevant met het oog op het verwezenlijken van de nagestreefde doelstellingen, aangezien de vergelijking van de biometrische gegevens van de foto van het identificatiedocument en die van het gezicht van de abonnee, enerzijds, de taak van de operatoren kan vergemakkelijken om alles in het werk te stellen teneinde een betrouwbare identificatie te garanderen van de abonnee die een natuurlijke persoon is en, anderzijds, het frauduleuze gebruik van de bedoelde identificatiedocumenten kan voorkomen.

Het eventuele gebrek aan volledige betrouwbaarheid van het procedé en de daarmee samenhangende onmogelijkheid dat het niet-opsporen van bepaalde gevallen van *lookalike*-fraude wordt uitgesloten, leiden niet tot een andere conclusie.

B.69. De bestreden maatregel van gezichtsvergelijking is overigens vastgelegd in een voldoende precieze wettelijke bepaling, aangezien artikel 127, § 5, vierde lid, van de wet van 13 juni 2005 de gegevens bepaalt waarop de in het geding zijnde maatregel betrekking heeft, namelijk de biometrische gegevens op de foto van de identificatiedocumenten bedoeld in artikel 127, § 6, van die wet en die van het gezicht van de abonnee, het verboden is de voormelde biometrische gegevens langer te bewaren dan nodig is voor het vergelijkingsprocedé, de gegevens uitsluitend elektronisch leesbaar zijn en alleen de operatoren en de verkooppunten in de zin van het voormelde artikel 127 gemachtigd zijn om die gegevens te lezen.

Op die manier kunnen de in die bepaling bedoelde abonnees op voldoende nauwkeurige wijze de voorwaarden kennen waaronder de voormelde biometrische gegevens worden verwerkt.

B.70. Het Hof onderzoekt thans de noodzaak en de evenredigheid van de inmenging.

B.71.1. In het kader van het onderzoek van de noodzaak dient te worden nagegaan of de inmenging niet verder gaat dan hetgeen nodig is voor het verwezenlijken van de nagestreefde doelstellingen en, in het bijzonder, of er maatregelen bestaan die minder afbreuk doen aan de betrokken rechten, terwijl ze op doeltreffende wijze bijdragen tot het doel van de in het geding zijnde regelgeving (HvJ, 17 oktober 2013, C-291/12, *Schwarz t. Stadt Bochum*, ECLI:EU:C:2013:670, punten 46 en 47).

B.71.2. Uit de parlementaire voorbereiding van de bestreden bepaling blijkt dat de wetgever de maatregel van gezichtsvergelijking bedoeld in artikel 127, § 5, vierde lid, van de wet van 13 juni 2005 noodzakelijk achtte om de in B.67.1 vermelde doelstellingen te bereiken :

« De gezichtsvergelijkingsmethode is ook een goede methode om de door de regering beoogde doelstellingen te bereiken.

Met deze methode van gezichtsvergelijking kunnen operatoren identiteitsfraude verminderen. Dankzij deze methode is het ook niet langer nodig om een beroep te doen op de verkooppunten, die de ‘ zwakke schakels ’ zijn wanneer het gaat om de betrouwbaarheid van de identificatie van de abonnee. Dat de betrouwbaarheid van de identificatie daardoor toeneemt, komt niet alleen de autoriteiten ten goede, maar ook de operatoren, die het slachtoffer zijn van fraude (vandaar het belang van verschillende operatoren om van deze methode gebruik te maken) en de abonnee (die zo misbruik van zijn identiteit voorkomt). Zelfs als een persoon erin slaagt om zich te identificeren met een vals identiteitsdocument, zal op de kopie van dat identiteitsdocument dat geen Belgische elektronische identiteitskaart is, een correcte foto van de abonnee staan, waardoor de autoriteiten een onderzoek zouden kunnen opstarten.

Dankzij de gezichtsvergelijkingsmethode kunnen de operatoren voldoen aan hun verplichting om een betrouwbare identificatie van de abonnee uit te voeren en zich aan te passen aan de behoeften van de abonnees (cf. *infra*).

Het gaat om een aanvaardbare methode vanuit privacyoogpunt aangezien de biometrische gegevens van het gezicht niet worden bewaard. Zoals reeds werd aangegeven, is het daardoor niet langer nodig om een beroep te doen op de verkooppunten, die soms zelf aan de basis liggen van fraude (bijvoorbeeld frauduleus hergebruik van identificatiegegevens van een persoon om een andere persoon te identificeren).

Daardoor is het ook mogelijk om een abonnee meer mogelijkheden te bieden om zich te identificeren en zijn identificatie te vergemakkelijken, in het bijzonder voor online identificaties. Voor vele gebruikers die mee zijn met de technologie is dit een dagelijkse gewoonte geworden. De vergelijking van de biometrische parameters van een selfie en de foto op een identiteitsdocument geeft nieuwe mogelijkheden om een betrouwbare identificatie uit te voeren. Deze oplossing kan specifiek de online identificatie voor de klant sterk vergemakkelijken vooral in geval van identificatie via smartphone waar het gebruik van de Belgische eID lezer niet mogelijk is » (*Parl. St.,* Kamer, 2021-2022, DOC 55-2572/002, pp. 90 en 91).

B.71.3. In dat verband wilde de wetgever een systeem opzetten waarmee gepast kan worden ingespeeld op elk specifiek geval, onder meer dat van niet-Belgische inwoners zonder elektronische identiteitskaart, dat van buitenlanders op bezoek in België of dat van personen die minder vertrouwd zijn met de digitale wereld. In dat opzicht preciseert de parlementaire voorbereiding van de wet van 20 juli 2022 dat « de identificatie op basis van gezichtsvergelijking [...] complementair [is] en [...] een noodzakelijke aanvulling [is] voor de reeds bestaande methodes » (*Parl. St.,* Kamer, 2021-2022, DOC 55-2572/002, p. 84).

B.72.1. Wat de evenredigheid van de maatregel betreft, legt artikel 127, § 5, vierde lid, van de wet van 13 juni 2005 zelf meerdere waarborgen vast ten gunste van de abonnee die te maken krijgt met de maatregel van gezichtsvergelijking.

De vergelijkingstool moet zijn toegestaan door de minister die bevoegd is voor elektronische communicatie en door de minister van Justitie, na verificatie dat de tool een betrouwbare identificatie garandeert, rekening houdend met het risico van identiteitsfraude (1°).

Daarenboven biedt de operator de abonnee minstens één andere manier aan om zich te identificeren (2°), zodat de abonnee nooit kan worden gedwongen om de gezichtsherkenningsmethode te gebruiken teneinde in te tekenen op een elektronische communicatiedienst.

Vervolgens moet de abonnee zijn uitdrukkelijke toestemming geven in de zin van artikel 4, punt 11), van de AVG (3°), met dien verstande dat, in tegenstelling tot hetgeen de verzoekende partijen beweren, artikel 9, lid 2, *a)*, van de AVG niet vereist dat die toestemming schriftelijk is.

Tot slot mogen de operatoren en de verkooppunten de verwerkte biometrische gegevens niet meedelen aan een derde, noch ze verwerken voor andere doeleinden dan de identificatie van abonnees (4°).

B.72.2. Voor het overige blijkt niet dat de bestreden maatregel de essentiële inhoud van het recht op eerbiediging van het privéleven en van het recht op bescherming van persoonsgegevens zou raken.

B.73. Het derde onderdeel van het tweede middel in de zaak nr. 7932 is niet gegrond.

7. De gerichte bewaring van de gegevens op basis van een geografisch criterium (artikelen 9 tot 11)

B.74.1. Het eerste, het tweede en het derde middel in de zaak nr. 7930, het enige middel in de zaak nr. 7931 en het derde onderdeel van het eerste middel in de zaak nr. 7932 hebben betrekking op de maatregel van gerichte bewaring van de verkeers- en locatiegegevens bepaald bij de artikelen 9, 10 en 11 van de wet van 20 juli 2022.

B.74.2. Artikel 9 van de wet van 20 juli 2022 voegt een artikel 126/1 in de wet van 13 juni 2005 in, dat bepaalt :

« § 1. Onverminderd de AVG en de wet van 30 juli 2018, bewaren de operatoren die aan de eindgebruikers elektronische-communicatiediensten aanbieden, alsook de operatoren die onderliggende en elektronische-communicatienetwerken aanbieden, de in artikel 126/2, § 2, bedoelde gegevens voor de geografische zones bedoeld in artikel 126/3, gedurende twaalf maanden te rekenen vanaf de datum van de communicatie, tenzij een andere termijn bepaald is in artikel 126/3.

Elke operator bewaart de gegevens die door hem gegenereerd of verwerkt zijn in het kader van de verstrekking van de betrokken [...] elektronische-communicatiediensten en -netwerken.

Deze gegevens worden bewaard ten behoeve van de vrijwaring van de nationale veiligheid, de strijd tegen zware criminaliteit, de preventie van ernstige dreigingen van de openbare veiligheid, en de bescherming van de vitale belangen van een natuurlijke persoon.

§ 2. De elektronische-communicatiemetagegevens, met inbegrip van de metagegevens voor de oproeppogingen zonder resultaat, waarop de in paragraaf 1 bedoelde bewaarplicht van toepassing is, worden opgesomd in artikel 126/2, § 2.

§ 3. De operatoren bewaren de verkeersgegevens voor iedere communicatie of alle oproeppogingen zonder resultaat die vanuit of naar een geografisch gebied als bedoeld in artikel 126/3 worden gevoerd.

Indien de operator, als gevolg van de door hem gebruikte technologie, niet in staat is de eindapparatuur die betrokken is bij de communicatie, met inbegrip van de oproeppoging zonder resultaat, nauwkeuriger te lokaliseren dan de lokalisatie ervan op het nationale grondgebied, bewaart de operator de in artikel 126/2, § 2, bedoelde gegevens gedurende de kortste overeenkomstig dit artikel en artikel 126/3 bepaalde termijn, op voorwaarde dat overeenkomstig dit artikel en artikel 126/3 het gehele nationale grondgebied gedekt is door een bewaarplicht. Indien niet aan deze voorwaarde is voldaan, bewaart de operator op wie dit lid van toepassing is deze gegevens niet.

Wanneer de eindgebruiker zich tijdens een elektronische communicatie verplaatst, bewaart de operator de verkeersgegevens voor zover de eindgebruiker zich op een bepaald moment van de communicatie bevindt in een zone bedoeld in artikel 126/3.

De operatoren bewaren de gegevens met betrekking tot de verbinding van de eindapparatuur met het netwerk en met de dienst en met betrekking tot de plaats van die apparatuur, inclusief het netwerkaansluitpunt, die opgesomd zijn in artikel 126/2, § 2, wanneer die apparatuur zich bevindt in een in artikel 126/3 bedoelde zone.

Om te bepalen of eindapparatuur zich in een geografische zone als bedoeld in artikel 126/3 bevindt, maken de operatoren gebruik van de meest betrouwbare en nauwkeurige gegevens als mogelijk is. Zij maken hiervoor, indien beschikbaar, gebruik van de satellietlocatie van eindapparatuur.

Indien de door de operator gebruikte technologie niet toelaat de bewaring van gegevens te beperken tot een in artikel 126/3 bedoelde zone, bewaart hij de gegevens die nodig zijn om de hele betrokken zone te bestrijken en beperkt hij de bewaring van gegevens buiten die zone tot wat strikt noodzakelijk is in het licht van de technische mogelijkheden.

Wanneer een aggregatiepunt van de operator, zoals een antenne, verschillende in artikel 126/3 bedoelde geografische zones dekt die onderworpen zijn aan een verschillende bewaringstermijn, bewaart de operator de gegevens voor dat aggregatiepunt gedurende de kortste bewaringstermijn.

Wanneer op grond van dit artikel en van artikel 126/3 verschillende bewaringstermijnen van toepassing zijn op dezelfde gegevens, bewaren de operatoren de gegevens gedurende de kortste termijn.

§ 4. De Koning kan, bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie, en van de minister, na raadpleging van de autoriteiten bevoegd voor de bescherming van de gegevens en van het Instituut, het volgende bepalen :

- de technische parameters en gegevens die de operatoren gebruiken om de gegevensopslag te beperken tot de in artikel 126/3 bedoelde zones;

- de lijst van de verschillende autoriteiten die bevoegd zijn voor de in artikel 126/3, §§ 2 tot 5, bedoelde aangelegenheden;

- de nadere regels voor de mededeling van informatie door de bevoegde autoriteiten aan de door de Koning aangewezen dienst, de nadere regels voor de mededeling van informatie door deze dienst aan de betrokken operatoren en de termijn waarbinnen de operatoren jaarlijks de in paragraaf 1 bedoelde bewaring ten uitvoer leggen;

- in voorkomend geval, de bijkomende geografische zones bedoeld in artikel 126/3, § 3, *m)*, § 4, *g)*, en § 5, *f)*.

Het koninklijk besluit bedoeld in het eerste lid, vierde streepje, wordt elke drie jaar hernieuwd. Bij ontstentenis van een hernieuwing vervalt de verplichting tot bewaring bedoeld in paragraaf 1 wat deze bijkomende geografische zones betreft, en dit tot een nieuw koninklijk besluit van kracht wordt.

§ 5. De minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie en de minister brengen, na voorafgaand advies van het Coördinatiecomité Inlichtingen en Veiligheid, van het Instituut en de autoriteiten bevoegd voor de bescherming van de gegevens, jaarlijks een evaluatieverslag uit aan de Kamer van volksvertegenwoordigers over de toepassing van dit artikel en, in voorkomend geval, van het in paragraaf 4 bedoelde koninklijk besluit, teneinde na te gaan of het nodig is bepalingen aan te passen.

In dit evaluatieverslag wordt in het bijzonder nagegaan of de categorieën van geografische zones opgenomen in de wet en het in paragraaf 4 bedoelde koninklijk besluit nog steeds voldoen aan de criteria bedoeld in artikel 126/3, §§ 3 tot 5, en of het nog nodig is deze te handhaven dan wel of andere categorieën opgenomen moeten worden.

Categorieën van geografische zones kunnen enkel opgenomen worden ter vrijwaring van de nationale veiligheid, of indien er in deze zones op basis van objectieve en niet-discriminerende elementen kan worden vastgesteld dat er een situatie bestaat die wordt gekenmerkt door een hoog risico op het voorbereiden of plegen van daden van zware criminaliteit.

Het evaluatieverslag bevat ook het percentage van het nationale grondgebied waarvoor de verplichting tot gegevensbewaring op basis van dit artikel en artikel 126/3 van toepassing is.

Dit evaluatieverslag wordt gestuurd naar het Controleorgaan op de politionele informatie en naar het Vast Comité I ».

B.74.3. Artikel 10 van de wet van 20 juli 2022 voegt een artikel 126/2 in de wet van 13 juni 2005 in, dat bepaalt :

« § 1. Voor de toepassing van dit artikel wordt verstaan onder ‘ communicatie ’, informatie die wordt uitgewisseld of overgebracht tussen een eindig aantal partijen door middel van een publiek beschikbare elektronische-communicatiedienst, met uitsluiting van de informatie die via een openbare omroepdienst over een elektronische-communicatienetwerk wordt overgebracht, behalve in de mate waarin de informatie kan worden gelinkt aan de identificeerbare abonnee of gebruiker die deze informatie ontvangt.

§ 2. De gegevens bedoeld in artikel 126/1, § 2, die in uitvoering van de artikelen 126/1 en 126/3 bewaard moeten worden door de operatoren die aan de eindgebruikers elektronische-communicatiediensten aanbieden, alsook door de operatoren die de onderliggende elektronische-communicatienetwerken aanbieden die het aanbieden van die diensten mogelijk maken, zijn de volgende :

1° de beschrijving en de technische karakteristieken van de elektronische-communicatiedienst die werd aangewend tijdens de communicatie;

2° de identificatiegegevens bedoeld in artikel 126, § 1, 2°, 10° tot 14°, en 16°, van de geadresseerde van de communicatie;

3° voor de elektronische-communicatiediensten met uitzondering van de internettoegangsdiensten, het IP-adres dat gebruikt is door de geadresseerde van de communicatie, het tijdstempel alsook, in geval van gedeeld gebruik van een IP-adres van de geadresseerde, de poorten die aan hem zijn toegewezen;

4° in geval van een groepsgesprek, oproepdoorschakeling of -doorverbinding, de identificatie van alle lijnen waaronder ook diegene waarnaar de oproep is doorgeleid;

5° de datum en het exacte tijdstip van de aanvang en het einde van de sessie van de betrokken elektronische-communicatiedienst, waaronder de datum en het exacte tijdstip van de aanvang en het einde van de oproep;

6° de gegevens die de identificatie en de lokalisatie van de cellen of andere netwerkaansluitpunten van het mobiele netwerk mogelijk maken, die werden gebruikt voor de

communicatie, van de start tot het einde van de communicatie, alsook de exacte data en tijdstippen van deze verschillende locaties;

7° het tijdens de duur van de sessie geüploade en gedownloade volume van gegevens;

8° voor wat betreft de mobiele elektronische-communicatiediensten, de datum en het tijdstip van de verbinding van de eindapparatuur met het netwerk wegens het opstarten van die apparatuur, en het moment waarop de verbinding van deze eindapparatuur met het netwerk wordt verbroken wegens het uitschakelen van die apparatuur;

9° voor wat betreft de mobiele elektronische-communicatiediensten, de locatie van de eindapparatuur en de datum en het tijdstip van deze locatie telkens wanneer de operator wil weten welke eindapparatuur is verbonden met zijn netwerk;

10° de andere identifiers met betrekking tot de geadresseerde van de elektronische communicatie, tot zijn eindapparatuur of tot de apparatuur het dichtst bij die eindapparatuur, die uit de technologische evolutie resulteren en die door de Koning bepaald worden, na advies van de Gegevensbeschermingsautoriteit en het Instituut, op voorwaarde dat dit besluit bij wet wordt bekrachtigd binnen zes maanden na de bekendmaking van dit besluit.

In afwijking van de artikelen 126/1 en 126/3 bedraagt de bewaartermijn van het gegeven bedoeld in het eerste lid, 8°, zes maanden nadat het is gegenereerd of verwerkt.

Het koninklijk besluit bedoeld in het eerste lid, 10°, slaat niet op de inhoud van de elektronische communicatie.

De Koning kan, na advies van de Gegevens-beschermingsautoriteit en het Instituut, de gegevens bedoeld in eerste lid, preciseren.

§ 3. De combinatie van de gegevens bewaard in uitvoering van artikel 126 en van dit artikel moet het mogelijk maken om de relatie te leggen tussen de bron en de bestemming van de communicatie.

De Koning kan, bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van Justitie, de minister van Binnenlandse Zaken, de minister van Defensie en de minister, en na advies van de autoriteiten bevoegd voor de bescherming van de gegevens en van het Instituut, de vereisten inzake nauwkeurigheid en betrouwbaarheid bepalen waaraan de gegevens bedoeld in dit artikel moeten beantwoorden ».

B.74.4. Artikel 11 van de wet van 20 juli 2022 voegt een artikel 126/3 in de wet van 13 juni 2005 in, dat bepaalt :

« § 1. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de geografische zones bestaande uit :

- de gerechtelijke arrondissementen waar minstens drie strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per 1 000 inwoners per jaar zijn vastgesteld, over een gemiddelde van de drie voorbije kalenderjaren;

- de politiezones waar minstens drie strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per 1 000 inwoners per jaar, zijn vastgesteld, over een gemiddelde van de drie voorbije kalenderjaren, en die deel uitmaken van een gerechtelijk arrondissement waar, in het kalenderjaar voorafgaand aan het lopende kalenderjaar minder dan drie strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per 1 000 inwoners per jaar, zijn vastgesteld, over een gemiddelde van de drie voorbije kalenderjaren.

In het geval bedoeld in het eerste lid, eerste streepje, bedraagt de bewaringstermijn van de gegevens bedoeld in artikel 126/2, § 2 :

a) zes maanden, indien er drie of vier strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren;

b) negen maanden, indien er vijf of zes strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren;

c) twaalf maanden, indien er zeven of meer dan zeven strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren.

In het geval bedoeld in het eerste lid, tweede streepje, bedraagt de bewaringstermijn van de gegevens bedoeld in artikel 126/2, § 2 :

a) zes maanden, indien er drie of vier strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren;

b) negen maanden, indien er vijf of zes strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren;

c) twaalf maanden, indien er zeven of meer dan zeven strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld zijn over een gemiddelde van de drie voorbije kalenderjaren.

Het aldus vastgestelde aantal strafbare feiten wordt naar boven of naar beneden afgerond op het dichtstbijzijnde gehele getal, al naargelang het eerste cijfer achter de komma al dan niet vijf bereikt.

De statistieken betreffende het aantal strafbare feiten zoals bedoeld in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering per jaar per 1 000 inwoners vastgesteld over een gemiddelde van de drie voorbije kalenderjaren zijn afkomstig uit de Algemene Nationale Gegevensbank zoals bedoeld in artikel 44/7 van de wet van 5 augustus 1992 op het politieambt.

De grenzen van de gerechtelijke arrondissementen bedoeld in het eerste lid, eerste streepje, zijn vastgesteld in artikel 4 van de bijlage bij het Gerechtelijk Wetboek.

De grenzen van de politiezones bedoeld in het eerste lid, tweede streepje, zijn die welke zijn vermeld in de bijlage bij het koninklijk besluit van 24 oktober 2001 houdende de benaming van de politiezones.

De directie, bedoeld in artikel 44/11 van de wet van 5 augustus 1992 op het politieambt, stuurt de statistieken met betrekking tot het aantal strafbare feiten en de bewaringstermijn voor elk gerechtelijk arrondissement en elke politiezone naar het Controleorgaan op de politionele informatie, dat binnen een maand na ontvangst van alle daartoe vereiste gegevens, deze valideert. Het Controleorgaan kan, met het oog op deze validatie, al de bevoegdheden uitoefenen die hem zijn toegekend bij titel 7 van de wet van 30 juli 2018.

De statistieken en de bewaringstermijnen worden door de directie bedoeld in artikel 44/11 van de wet van 5 augustus 1992 op het politieambt aan de door de Koning aangewezen dienst toegezonden, enkel nadat deze op de hoogte is gebracht van hun validatie door het Controleorgaan.

Op voorstel van de door de Koning aangewezen dienst stellen de ministers van Justitie en van Binnenlandse Zaken jaarlijks de lijst vast van de gerechtelijke arrondissementen en de politiezones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaartermijn.

Na deze vaststelling, zendt de door de Koning aangewezen dienst de lijst van de gerechtelijke arrondissementen en politiezones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaartermijn, naar de operatoren.

§ 2. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de geografische zones die bepaald worden door het Coördinatieorgaan voor de Dreigingsanalyse, waar het dreigingsniveau, vastgesteld op basis van de evaluatie bedoeld in artikel 8, 1° en 2°, van de wet van 10 juli 2006 betreffende de analyse van de dreiging, ten minste niveau 3 bedraagt, overeenkomstig artikel 11 van het koninklijk besluit van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging, en zolang het dreigingsniveau van tenminste niveau 3 blijft bestaan voor deze zones.

Wanneer het dreigingsniveau ten minste niveau 3 bedraagt en deze het hele grondgebied bestrijkt, deelt het Coördinatieorgaan voor de Dreigingsanalyse dit onmiddellijk mee aan de dienst aangewezen door de Koning, zodat deze dienst de nodige maatregelen kan nemen om de operatoren in te lichten en tot een algemene en ongedifferentieerde bewaring van de gegevens bedoeld in artikel 126/2, § 2, over te gaan voor het gehele grondgebied.

De bewaarplicht bedoeld in het tweede lid wordt bevestigd bij koninklijk besluit, op gezamenlijk voorstel van de minister van Binnenlandse Zaken en de minister van Justitie. Bij ontstentenis van bevestiging bij koninklijk besluit, bekendgemaakt binnen de maand na de in het tweede lid bedoelde beslissing, wordt de gegevensbewaring opgeheven en worden de operatoren daarvan zo spoedig mogelijk in kennis gesteld door de dienst aangewezen door de Koning. Na deze kennisgeving vernietigen de operatoren de tot dan toe en voor dit doel bewaarde gegevens.

§ 3. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de gebieden die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit, met name :

a) de havenfaciliteiten, de havens en de havenbeveiligingszones bedoeld in artikel 2.5.2.2, 3° tot 5°, van het Belgisch Scheepvaartwetboek;

b) de spoorwegstations in de zin van artikel 2, 5°, van de wet van 27 april 2018 op de politie van de spoorwegen;

c) de metro- en de pre-metrostations;

d) de luchthavens in de zin van artikel 2, punt 1), van Richtlijn 2009/12/EG van het Europees Parlement en de Raad van 11 maart 2009 inzake luchthavengelden, met inbegrip van de luchthavens die tot het kernnetwerk behoren, opgesomd in bijlage II, afdeling 2, van Verordening (EU) nr. 1315/2013 van het Europees Parlement en de Raad van 11 december 2013 betreffende richtsnoeren van de Unie voor de ontwikkeling van het trans-Europees vervoersnetwerk en tot intrekking van Besluit nr. 661/2010/EU, alsook de entiteiten die de bijbehorende installaties bedienen welke zich op de luchthavens bevinden;

e) de gebouwen bestemd voor de administratie van douane en accijnzen;

f) de gevangenissen in de zin van artikel 2, 15°, van de basiswet van 12 januari 2005 betreffende het gevangeniswezen en de rechtspositie van de gedetineerden, de gemeenschapscentra voor minderjarigen die een als misdrijf omschreven feit hebben gepleegd, bedoeld in artikel 606 van het Wetboek van strafvordering, en de forensisch psychiatrische centra, bedoeld in artikel 3, 4°, *c)*, van de wet van 5 mei 2014 betreffende de internering;

g) de wapenhandelaars en schietstanden zoals bedoeld in artikel 2, 1° en 19°, van de wet van 8 juni 2006 houdende regeling van economische en individuele activiteiten met wapens;

h) de inrichtingen bedoeld in artikel 3.1.*a)*, van het koninklijk besluit van 20 juli 2001 houdende algemeen reglement op de bescherming van de bevolking, van de werknemers en het leefmilieu tegen het gevaar van de ioniserende stralingen;

i) de inrichtingen bedoeld in artikel 2, 1°, van het samenwerkingsakkoord van 16 februari 2016 tussen de Federale Staat, het Vlaams Gewest, het Waals Gewest en het Brussels Hoofdstedelijk Gewest betreffende de beheersing van de gevaren van zware ongevallen waarbij gevaarlijke stoffen zijn betrokken;

j) de gemeenten waar zich een of meerdere kritieke netwerkelementen of een of meerdere kritieke infrastructuren bevinden als bedoeld in de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren en de uitvoeringsbesluiten ervan; indien het gehele netwerk als kritieke infrastructuur is aangemerkt, worden voor de toepassing van dit artikel alleen de kritieke netwerkelementen in aanmerking genomen;

k) de zetel van de NV Astrid en de gebouwen waarin haar centrale en provinciale datacentra zijn ondergebracht, alsmede de gebouwen waarin zich de centrale datacentra en de communicatieknooppunten van het beveiligde en gecodeerde communicatie- en

informatiesysteem bevinden bedoeld in artikel 11, § 7, van het koninklijk besluit van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging;

l) de netwerk- en informatiesystemen die de verlening van essentiële diensten van aanbieders van essentiële diensten ondersteunen aangeduid op basis van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;

m) in voorkomend geval, en onverminderd artikel 126/1, § 5, derde lid, de andere zones die in het bijzonder blootgesteld zijn aan bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit, vastgesteld bij koninklijk besluit.

§ 4. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de zones waar er een mogelijke ernstige bedreiging is voor de vitale belangen van het land of de essentiële behoeften van de bevolking, dit wil zeggen :

a) voor de openbare orde, de neutrale zones bedoeld in artikel 3 van de wet van 2 maart 1954 tot voorkoming en beteugeling der aanslagen op de vrije uitoefening van de door de Grondwet ingestelde soevereine machten, en de ministeriële beleidscellen;

b) voor het wetenschappelijk en economisch potentieel, de gebouwen bestemd voor rechtspersonen waarvan het economisch en/of wetenschappelijk potentieel beschermd moet worden en die zijn opgenomen in een lijst die jaarlijks door de Veiligheid van de Staat en de Algemene Dienst lnlichting en Veiligheid wordt opgesteld op voorstel van de minister van Justitie en de minister van Defensie en wordt goedgekeurd door de Nationale Veiligheidsraad;

c) voor het transport, de autosnelwegen en de bijhorende openbare parkeerterreinen;

d) voor de nationale soevereiniteit en de instellingen opgericht door de Grondwet en de wetten, decreten of ordonnanties :

i) de wetgevende vergaderingen bedoeld in artikel 1 van de wet van 2 maart 1954 tot voorkoming en beteugeling der aanslagen op de vrije uitoefening van de door de Grondwet ingestelde soevereine machten;

ii) de gemeentehuizen en de stadhuizen;

iii) het koninklijk paleis;

iv) de koninklijke domeinen;

v) de gebouwen toegewezen aan de instellingen bedoeld in titel III, hoofdstukken 5 tot 7 van de Grondwet;

vi) de gemeenten waar zich militaire domeinen bevinden;

vii) de gebouwen bestemd voor de lokale en de federale politie, alsook voor de Veiligheid van de Staat;

e) voor de integriteit van het nationaal grondgebied, de grensgemeenten;

f) voor de belangrijke economische of financiële belangen, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, de volksgezondheid en de sociale zekerheid :

i) de ziekenhuizen bedoeld in artikel 2 van de gecoördineerde wet van 10 juli 2008 op de ziekenhuizen en andere verzorgingsinrichtingen;

ii) de Nationale Bank van België;

g) in voorkomend geval, en onverminderd artikel 126/1, § 5, derde lid, de andere zones waar er een mogelijke ernstige bedreiging is voor de vitale belangen van het land of de essentiële behoeften van de bevolking vastgesteld bij koninklijk besluit.

§ 5. De gegevens bedoeld in artikel 126/2, § 2, worden bewaard in de zones waar er een mogelijk ernstige bedreiging bestaat voor de belangen van de op het nationale grondgebied gevestigde internationale instellingen, dit wil zeggen :

a) de ambassades en diplomatieke vertegenwoordigingen;

b) de gebouwen bestemd voor de Europese Unie;

c) de gebouwen en de infrastructuren bestemd voor de NAVO;

d) de instellingen van de Europese Economische Ruimte;

e) de instellingen van de Verenigde Naties;

f) in voorkomend geval, en onverminderd artikel 126/1, § 5, derde lid, de andere zones waar er een mogelijk ernstige bedreiging bestaat voor de belangen van de op het nationale grondgebied gevestigde internationale instellingen vastgesteld bij koninklijk besluit.

§ 6. Voor elke categorie van zone bedoeld in de paragrafen 3 tot 5, bepaalt de Koning de omvang van de perimeter van de zone.

Elke autoriteit die bevoegd is voor een van de aangelegenheden bedoeld in de paragrafen 3 tot 5, deelt jaarlijks op de door de Koning vastgestelde datum alleen aan de door de Koning aangewezen dienst de gegevens mee die nodig zijn voor de concrete vaststelling van de geografische zones.

Wanneer een geografische zone niet langer aan het bedoeld criterium voldoet, stellen deze autoriteiten alleen deze dienst daarvan onverwijld in kennis, zodat de verplichting tot bewaring bedoeld artikel 126/1, § 1, in deze zone zo spoedig mogelijk kan worden beëindigd.

Met uitzondering van de in paragraaf 4, *b)*, bedoelde lijst van plaatsen, die door de inlichtingen- en veiligheidsdiensten exclusief ter beschikking van het Vast Comité I wordt gesteld, stelt de door de Koning aangewezen dienst de bijgewerkte lijst van zones bedoeld in de paragrafen 3 tot 5 waar de gegevensbewaring verplicht is, ter beschikking van het Controleorgaan op de politionele informatie en van het Vast Comité I, elk binnen het kader van hun bevoegdheden.

Het Controleorgaan op de politionele informatie en het Vast Comité I kunnen, elk binnen het kader van hun bevoegdheden, aanbevelingen doen met betrekking tot deze lijst of het met redenen omklede bevel geven dat bepaalde geografische zones bedoeld in de paragrafen 3 tot 5, van de lijst geschrapt worden.

Op voorstel van de door de Koning aangewezen dienst stellen de minister van Defensie, de minister van Justitie, en de minister van Binnenlandse Zaken jaarlijks en bij elke wijziging bedoeld in het vijfde lid de lijst vast van de geografische zones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaringstermijn.

Het ministeriële besluit bedoeld in het zesde lid wordt bekendgemaakt via vermelding in het *Belgisch Staatsblad*.

Na deze goedkeuring, zendt de door de Koning aangewezen dienst de lijst van de geografische zones die aan de gegevensbewaringsplicht zijn onderworpen, samen met hun bewaringstermijn, naar de operatoren.

Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de gegevens die door de bevoegde autoriteiten aan de door de Koning aangewezen dienst worden meegedeeld of van de lijst van de geografische zones die aan de gegevensbewaringsplicht zijn onderworpen, of zijn medewerking verleent aan de uitvoering van dit artikel, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek ».

B.75.1. De verzoekende partij in de zaak nr. 7930 leidt een eerste, een tweede en een derde middel af uit de schending van de artikelen 11, 12, 22 en 29 van de Grondwet, van artikel 15, lid 1, en van de artikelen 5, 6 en 9 van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8, 11, 47 en 52, lid 1, van het Handvest, van de artikelen 6, 8, 10, 11 en 18 van het Europees Verdrag voor de rechten van de mens en van de artikelen 13 en 54 van de richtlijn (EU) 2016/680. Volgens haar stellen de artikelen 9 tot 11 van de wet van 20 juli 2022 een algemene verplichting in om communicatiegegevens te bewaren, zonder dat die bewaring noodzakelijk noch strikt beperkt blijkt ten aanzien van het nagestreefde doel. Zij betoogt dat artikel 9 tegenstrijdig is wat betreft de erin opgesomde doeleinden van bewaring. Wat betreft artikel 11 stelt zij bovendien dat die bepaling *de facto* een bewaring op het gehele Belgische grondgebied toestaat, dat de gegevensbewaring in het kader van de nationale veiligheid op basis van het door het OCAD bepaalde dreigingsniveau niet aan een onafhankelijke controle is onderworpen en dat dat niveau onder de drempel blijft die door het Hof van Justitie wordt vereist, dat de bepaalde bewaringstermijnen niet zijn beperkt tot wat strikt noodzakelijk is, dat het systeem van zones die worden bepaald op basis van het aantal strafbare feiten noch relevant, noch evenredig is, met name wat betreft het begrip « zware criminaliteit » en het gekozen statistische systeem, en tot slot dat de bedoelde specifieke zones in werkelijkheid het gehele

Belgische grondgebied bestrijken. De verzoekende partij klaagt ook de omstandigheid aan dat de perimeter van de zones wordt vastgesteld door de Koning, hetgeen zou indruisen tegen het beginsel van de formele wettigheid.

B.75.2. De verzoekende partij in de zaak nr. 7931 leidt een enig middel af uit de schending van de artikelen 11, 12, 22 en 29 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 7, 8, 11, 47 en 52, lid 1, van het Handvest, met artikel 8 van het Europees Verdrag voor de rechten van de mens, met de artikelen 5, 6 en 15 van de richtlijn 2002/58/EG en met de artikelen 13 en 54 van de richtlijn (EU) 2016/680.

Wat betreft de zones die worden gekenmerkt door een hoge graad van zware criminaliteit, voert de verzoekende partij aan dat de artikelen 9 tot 11 van de wet van 20 juli 2022 voorzien in de bewaring van gegevens gedurende een periode die niet voldoet aan het noodzakelijkheidsbeginsel en dat zij bepaalde strafbare feiten beogen die onder gewone criminaliteit vallen. Dienaangaande vraagt de verzoekende partij in ondergeschikte orde om een prejudiciële vraag te stellen aan het Hof van Justitie. Zij voegt eraan toe dat de in aanmerking genomen statistieken verwijzen naar de kwalificatie van de feiten bij de aanvang van een onderzoek en niet naar de strafbare feiten die tot een strafrechtelijke veroordeling leiden, hetgeen niet pertinent zou zijn, en dat het aan de Koning staat om de perimeter van de zone vast te stellen, hetgeen niet bestaanbaar zou zijn met het beginsel van de formele wettigheid.

Wat betreft de zones die worden gekenmerkt door een bedreiging van de nationale veiligheid, betwist de verzoekende partij het in aanmerking genomen dreigingsniveau, dat niet in overeenstemming zou zijn met de eisen van het Hof van Justitie, en de omstandigheid dat de gegevens voor andere doeleinden mogen worden bewaard dan dat van de vrijwaring van de nationale veiligheid. De verzoekende partij klaagt eveneens het gebrek aan een daadwerkelijke door een onafhankelijke autoriteit uitgevoerde controle aan, alsook de mogelijkheid waarover de Koning beschikt om de perimeter van de zones vast te stellen en de lijst van de zones aan te vullen, hetgeen niet bestaanbaar zou zijn met het beginsel van de formele wettigheid.

Wat betreft de maatregelen die door de operatoren mogen worden genomen, is de verzoekende partij van mening dat artikel 9 van de wet van 20 juli 2022 een uitgebreidere gegevensbewaring toestaat wanneer de operator niet in staat is de locatie van de gebruikers te bepalen of de bewaring te beperken tot de betrokken zone, hetgeen niet evenredig zou zijn.

B.75.3. De verzoekende partijen in de zaak nr. 7932 leiden een eerste middel af uit de schending van de artikelen 10, 11, 13, 15, 22, 23 en 29 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 5, 6, 8, 9, 10, 11, 14 en 18 van het Europees Verdrag voor de rechten van de mens, met de artikelen 7, 8, 11, 47 en 52 van het Handvest, met artikel 5, lid 4, van het Verdrag betreffende de Europese Unie, alsook met artikel 6 van de richtlijn 2002/58/EG, met de richtlijn (EU) 2016/680 en met de AVG.

In het derde onderdeel van dat middel betogen de verzoekende partijen dat de gegevensbewaringsmaatregelen bepaald bij de artikelen 9, 10 en 11 van de wet van 20 juli 2022 *de facto* leiden tot een ongedifferentieerde gegevensbewaring. In dat verband wijzen zij erop dat die bepalingen geen enkel onderscheid maken onder de doeleinden die ermee worden nagestreefd, in tegenstelling tot hetgeen wordt vereist door het Hof van Justitie. De verzoekende partijen voeren bovendien aan dat de in de bestreden bepalingen bedoelde bewaringstermijn van de gegevens onevenredig is en dat die bepalingen een bewaring buiten de betrokken geografische zone toestaan. Daarnaast stellen zij dat de verschillende in artikel 11 van de wet van 20 juli 2022 opgesomde geografische zones te ruim zijn en het noodzakelijkheidsbeginsel niet in acht nemen. Zij klagen eveneens het ontbreken aan van een daadwerkelijk rechtsmiddel dat is gericht tegen de bewaringsmaatregel bepaald bij de artikelen 9 tot 11 van de wet van 20 juli 2022, alsook de machtiging aan de Koning om de perimeter van de zones te bepalen. Tot slot zijn de bij artikel 9 van de wet van 20 juli 2022 bepaalde bijkomende verplichtingen tot bewaring voor de OTT-diensten volgens de verzoekende partijen niet evenredig.

B.76. De grieven van de verzoekende partijen zijn in hoofdzaak afgeleid uit de schending van het recht op eerbiediging van het privéleven en van het recht op bescherming van persoonsgegevens, gewaarborgd bij artikel 22 van de Grondwet, bij artikel 8 van het Europees Verdrag voor de rechten van de mens, bij de artikelen 7, 8 en 52, lid 1, van het Handvest, bij de richtlijn 2002/58/EG, bij de richtlijn (EU) 2016/680 en bij de AVG.

B.77. Het Hof van Justitie heeft bij zijn voormelde arrest van 6 oktober 2020 geoordeeld dat de verplichting tot bewaring van de gegevens met betrekking tot elektronische communicatie de uitzondering moet zijn, en niet de regel.

B.78.1. De artikelen 126/1 tot 126/3 van de wet van 13 juni 2005, ingevoegd bij de artikelen 9 tot 11 van de wet van 20 juli 2022, verplichten de erin bedoelde operatoren ertoe een reeks gegevens (artikel 126/2) te bewaren ten behoeve van de vrijwaring van de nationale veiligheid, de strijd tegen zware criminaliteit, de voorkoming van ernstige bedreigingen van de openbare veiligheid en de bescherming van de vitale belangen van een natuurlijke persoon (artikel 126/1) in vijf types van geografische zones, namelijk, ten eerste, die zones die worden gekenmerkt door een aantal van minstens drie in artikel 90*ter*, §§ 2 tot 4, van het Wetboek van strafvordering bedoelde strafbare feiten per 1 000 inwoners per jaar (artikel 126/3, § 1), ten tweede, die waarvoor het dreigingsniveau ten minste niveau 3 bedraagt, zoals vastgesteld op basis van de evaluatie bedoeld in artikel 8, 1° en 2°, van de wet van 10 juli 2006 « betreffende de analyse van de dreiging », overeenkomstig artikel 11 van het koninklijk besluit van 28 november 2006 « tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging » (artikel 126/3, § 2), ten derde, die welke in het bijzonder zijn blootgesteld aan bedreigingen van de nationale veiligheid of aan het plegen van daden van zware criminaliteit, bestaande uit een reeks limitatief opgesomde plaatsen (artikel 126/3, § 3), ten vierde, die welke worden gekenmerkt door een mogelijke ernstige bedreiging van de vitale belangen van het land of de essentiële behoeften van de bevolking, bestaande uit een reeks limitatief opgesomde plaatsen (artikel 126/3, § 4) en, ten vijfde, die welke worden gekenmerkt door een mogelijke ernstige bedreiging van de belangen van de op het nationale grondgebied gevestigde internationale instellingen, bestaande uit een reeks limitatief opgesomde plaatsen (artikel 126/3, § 5).

B.78.2. In het dictum van zijn voormelde arrest van 6 oktober 2020 heeft het Hof van Justitie voor recht gezegd dat artikel 15, lid 1, van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8 en 11 en van artikel 52, lid 1, van het Handvest, zich verzet tegen wettelijke maatregelen die voor de in dat artikel 15, lid 1, bepaalde doeleinden preventief voorzien in een algemene en ongedifferentieerde bewaring van de verkeers- en locatiegegevens.

In hetzelfde dictum heeft het Hof van Justitie voor recht gezegd dat artikel 15, lid 1, van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8 en 11 en 52, lid 1, van het Handvest, zich evenwel niet verzet tegen wettelijke maatregelen :

- die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien

in een gerichte bewaring van verkeers- en locatiegegevens, die op basis van objectieve en niet-discriminatoire factoren wordt afgebakend aan de hand van categorieën betrokken personen of aan de hand van een geografisch criterium, voor een periode die niet langer is dan strikt noodzakelijk, maar die kan worden verlengd;

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

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

De voormelde wettelijke maatregelen dienen evenwel middels duidelijke en nauwkeurige regels te waarborgen dat de in het geding zijnde gegevensbewaring dient te voldoen aan materiële en procedurele voorwaarden en dat de betrokken personen over effectieve waarborgen beschikken tegen het risico van misbruik.

B.79.1. Voor de in artikel 126/2 van de wet van 13 juni 2005 bedoelde gegevens kan, in beginsel, in een gerichte preventieve bewaring worden voorzien ten behoeve van de vrijwaring van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid, bedoeld in artikel 126/1, § 1, derde lid, van de wet van 13 juni 2005.

Zoals de afdeling wetgeving van de Raad van State opmerkte in haar advies over het voorontwerp van wet dat aan de oorsprong ligt van de wet van 20 juli 2022, kan het doeleinde inzake de « bescherming van de vitale belangen van een natuurlijke persoon », dat eveneens wordt beoogd in artikel 126/1, § 1, derde lid, van de wet van 13 juni 2005, worden geacht te vallen onder het doeleinde inzake bescherming van de openbare veiligheid (*Parl. St.,* Kamer, 2021-2022, DOC 55-2572/001, p. 279).

B.79.2. Het staat aan het Hof om ten aanzien van de voormelde in B.76 aangehaalde referentienormen na te gaan of de artikelen 126/1 tot 126/3 van de wet van 13 juni 2005 in duidelijke en nauwkeurige regels voorzien met betrekking tot de draagwijdte en de toepassing van de daarin bepaalde gegevensbewaringsmaatregel en minimale eisen opleggen. De inmenging moet worden beperkt tot het strikt noodzakelijke en beantwoorden aan objectieve criteria die een verband leggen tussen de bewaarde gegevens en het nagestreefde doel. Het staat aan de wetgever tussen de verschillende soorten aan bewaring onderworpen gegevens het onderscheid te maken dat geboden is, zodat wordt gewaarborgd dat voor elk soort gegeven de inmenging tot het strikt noodzakelijke wordt beperkt.

B.80.1. Wat betreft de gegevensbewaringsmaatregel ten behoeve van de nationale veiligheid, heeft het Hof van Justitie bij zijn voormelde arrest van 6 oktober 2020 geoordeeld :

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

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

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

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

kunnen worden verlengd mocht de noodzaak van een dergelijke bewaring blijven bestaan » (HvJ, 6 oktober 2020, C-511/18, C-512/18 en C-520/18, voormeld).

B.80.2. Uit de parlementaire voorbereiding van de bestreden bepalingen blijkt dat de wetgever met de artikelen 126/1 tot 126/3 van de wet van 13 juni 2005 de mogelijkheid wilde aanwenden om een gegevensbewaringsmaatregel af te bakenen op basis van een geografisch criterium, mogelijkheid waarop wordt gewezen in het voormelde arrest van het Hof van Justitie van 6 oktober 2020 (*Parl. St.,* Kamer, 2021-2022, DOC 55-2572/001, pp. 45-49).

B.80.3.1. De toepassing van het voormelde geografische criterium moet evenwel pertinent en evenredig zijn ten aanzien van de nagestreefde doeleinden.

B.80.3.2. Zoals de afdeling wetgeving van de Raad van State heeft opgemerkt in haar advies over het voorontwerp van wet dat aan de oorsprong ligt van de wet van 20 juli 2022, zijn het aantal en de verscheidenheid aan zones bedoeld in artikel 126/3 van de wet van 13 juni 2005 aanzienlijk en leidt het feit dat zij samen worden beschouwd ertoe dat een vrij groot deel van het grondgebied wordt gedekt (*ibid.*, p. 283).

B.80.3.3. Uit de memorie van toelichting bij het wetsontwerp dat aanleiding gaf tot de wet van 20 juli 2022 blijkt dat de wetgever van oordeel is dat de term « geografische gebieden » bedoeld in punt 150 van het voormelde arrest van het Hof van Justitie van 6 oktober 2020 « na bestudering van de statistieken voor elk arrondissement, het gehele nationale grondgebied kan omvatten indien in elk van deze arrondissementen een hoog misdaadcijfer wordt vastgesteld » (*ibid.*, p. 65).

Wat betreft de eerste categorie van geografische zones, bepaald bij artikel 126/3, § 1, van de wet van 13 juni 2005, dat voorziet in de bewaring van de gegevens bedoeld in artikel 126/2, § 2, van de wet van 13 juni 2005 op basis van plaatsen die worden gekenmerkt door een groot aantal zware criminele feiten (statistisch criterium), erkent de wetgever dat « dus niet [kan worden] ontkend [...] dat de mogelijkheid bestaat dat op basis van de statistische gegevens, die per definitie dynamisch en evolutief zijn, vastgesteld wordt dat gegevens bewaard moeten worden in alle gerechtelijke arrondissementen, en dus voor het gehele grondgebied » (*ibid.*, p. 66).

De wetgever merkt eveneens op dat « dadergroepen bovendien zeer mobiel zijn en zich verplaatsen, en dat de georganiseerde criminaliteit in essentie polycrimineel is. Het lijkt niet juist om zich voor dit soort criminaliteit te beperken tot bepaalde zeer gerichte plaatsen op lokaal niveau » (*ibid.*, pp. 63-64).

Tijdens de bespreking van het wetsontwerp in de bevoegde commissie van de Kamer van volksvertegenwoordigers merkte de minister van Justitie met betrekking tot de in artikel 126/3, §§ 3 tot 5, van de wet van 13 juni 2005 opgesomde strategische zones op dat « in totaal [...] ongeveer 30 % van het grondgebied een strategische zone [zal] uitmaken, wat in de eerste plaats aantoont dat België een klein en dichtbevolkt land is » (*Parl. St.,* Kamer, 2021-2022, DOC 55-2572/003, p. 104).

B.80.3.4. De loutere vaststelling dat de in de artikelen 126/1 tot 126/3 bedoelde gegevensbewaringsmaatregel in bepaalde omstandigheden gericht kan zijn op het volledige grondgebied, betekent evenwel niet dat hij moet worden gelijkgesteld met een algemene gegevensbewaringsmaatregel die zonder onderscheid betrekking heeft op alle gebruikers van elektronische-communicatiemiddelen.

Zulks is immers niet het opzet van de wetgever, maar zou enkel het gevolg zijn van de statistische gegevens van de geografische zones en gebieden die in artikel 126/3 nauwkeurig zijn afgebakend en op gedetailleerde wijze zijn omschreven. De statistieken betreffende het aantal strafbare feiten in die geografische zones bepalen op objectieve en pertinente wijze de toepasselijke regeling inzake de bewaring en verwerking van gegevens.

De regeling voldoet bijgevolg aan het vereiste, vermeld in punt 150 van het voormelde arrest van het Hof van Justitie van 6 oktober 2020, dat « de bevoegde nationale autoriteiten op basis van objectieve factoren van mening zijn dat er in een of meer geografische gebieden sprake is van een situatie die wordt gekenmerkt door een hoog risico dat zware misdrijven worden voorbereid of gepleegd ».

B.81. Bijgevolg heeft de wetgever zich met de gegevensbewaringsmaatregel bepaald bij de artikelen 9 tot 11 van de wet van 20 juli 2022 beperkt tot wat strikt noodzakelijk is.

B.82. Het eerste, het tweede en het derde middel in de zaak nr. 7930, het enige middel in de zaak nr. 7931 en het derde onderdeel van het eerste middel in de zaak nr. 7932 zijn niet gegrond in zoverre zij zijn afgeleid uit de schending van artikel 22 van de Grondwet, in samenhang gelezen met artikel 8 van het Europees Verdrag voor de rechten van de mens, met de artikelen 7, 8 en 52, lid 1, van het Handvest en met artikel 15, lid 1, van de richtlijn 2002/58/EG.

8. De opsomming van de bevoegde autoriteiten en van de doeleinden in het kader van de toegang tot de gegevens (artikel 13)

B.83. Het eerste en het vierde middel in de zaak nr. 7930, het enige middel in de zaak nr. 7931 en het eerste en het tweede onderdeel van het derde middel in de zaak nr. 7932 hebben betrekking op artikel 13 van de wet van 20 juli 2022.

Die bepaling voegt in de wet van 13 juni 2005 een artikel 127/1 in, dat bepaalt :

« § 1. Voor de toepassing van dit artikel omvat zware criminaliteit met name de feiten waarvoor er ernstige aanwijzingen bestaan :

1° dat ze de minimale correctionele hoofdgevangenisstraf bedoeld in artikel 88*bis*, § 1, eerste lid, van het Wetboek van strafvordering tot gevolg kunnen hebben;

2° dat ze kunnen leiden tot een sanctie van niveau 5 of 6 zoals bedoeld in artikel XV.70 van het Wetboek van economisch recht;

3° dat ze een inbreuk zouden kunnen vormen op de artikelen 14 of 15 van Verordening (EU) nr. 596/2014 van het Europees Parlement en de Raad van 16 april 2014 betreffende marktmisbruik (verordening betreffende machtsmisbruik [lees : marktmisbruik]) en houdende intrekking van Richtlijn 2003/6/EG van het Europees Parlement en de Raad en Richtlijnen 2003/124, 2003/125/EG en 2004/72/EG van de Commissie of op de bepalingen die worden genomen op basis of ter uitvoering van deze artikelen.

§ 2. Enkel de volgende autoriteiten mogen van een operator gegevens krijgen die worden bewaard krachtens de artikelen 122 en 123, voor de doeleinden hieronder voor zover dit bepaald is door en onder de voorwaarden die vastgesteld zijn in een formele wettelijke norm :

1° de inlichtingen- en veiligheidsdiensten, teneinde de opdrachten te volbrengen die hen worden toegewezen krachtens de organieke wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten;

2° de bevoegde autoriteiten met het oog op de voorkoming van ernstige bedreigingen voor de openbare veiligheid;

3° de autoriteiten belast met het vrijwaren van de vitale belangen van natuurlijke personen;

4° de autoriteiten bevoegd voor het onderzoek van een veiligheidslek in het elektronische-communicatienetwerk of in de elektronische-communicatiedienst of in informatiesystemen;

5° de administratieve of gerechtelijke autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing of de vervolging van een online gepleegde inbreuk of een inbreuk gepleegd via een elektronische-communicatienetwerk of -dienst;

6° de administratieve of gerechtelijke autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing of de vervolging van een feit dat onder de zware criminaliteit valt;

7° de administratieve autoriteiten belast met het vrijwaren van een belangrijk economisch of financieel belang van de Europese Unie of van België, met inbegrip van de monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid;

8° de administratieve of gerechtelijke autoriteiten die bevoegd zijn voor de preventie, het onderzoek, de opsporing of de vervolging van een feit dat een strafrechtelijke inbreuk vormt, maar niet onder de zware criminaliteit valt;

9° het Instituut in het kader van de controle van deze wet en de autoriteiten bevoegd voor de bescherming van de gegevens in het kader van hun controleopdrachten;

10° de autoriteiten die wettelijk gemachtigd zijn om data te hergebruiken voor doeleinden van wetenschappelijk of historisch onderzoek of voor statistische doeleinden.

§ 3. De gegevens die worden bewaard krachtens de artikelen 126 en 127, worden bewaard voor de autoriteiten en de doeleinden bedoeld in paragraaf 2, 1° tot 8°.

Enkel de autoriteiten bedoeld in paragraaf 2 mogen van een operator gegevens ontvangen die worden bewaard krachtens de artikelen 126 en 127, voor de doeleinden waarin dezelfde paragraaf voorziet, voor zover dit bepaald is door en onder de voorwaarden die vastgesteld zijn in een formele wettelijke norm.

In afwijking van het tweede lid, mogen de in paragraaf 2, 10°, bedoelde autoriteiten van een operator geen aan de bron van de verbinding toegewezen IP-adressen krijgen.

In afwijking van het tweede lid, is een verzoek van een autoriteit om van een operator een IP-adres te krijgen dat is toegewezen aan de bron van een verbinding, enkel toegestaan voor de doeleinden van de vrijwaring van de nationale veiligheid, de bestrijding van zware criminaliteit, de preventies van ernstige dreigingen tegen de openbare veiligheid en de vrijwaring van de vitale belangen van een fysieke persoon, wanneer die autoriteit in staat zou zijn om, met behulp van de informatie in haar bezit en de aan de bron van de verbinding toegewezen IP-adressen die ze van de operator heeft verkregen, het traject van een eindgebruiker op internet te achterhalen.

§ 4. De gegevens die worden bewaard krachtens de artikelen 126/1 en 126/3 worden bewaard voor de autoriteiten en doeleinden bedoeld in paragraaf 2, 1° tot 3° en 6°.

Enkel de in paragraaf 2, 1° tot 3°, 6° en 9°, bedoelde autoriteiten mogen van een operator voor de doeleinden beoogd in dezelfde paragraaf, de krachtens de artikelen 126/1 en 126/3 bewaarde gegevens krijgen, voor zover dit bepaald is door en onder de voorwaarden die vastgesteld zijn in een formele wettelijke norm.

§ 5. De formele wettelijke norm van Belgisch recht bedoeld in de paragrafen 2 tot 4 preciseert :

- de categorie of categorieën van ondernemingen waaraan de autoriteit gegevens kan vragen;

- de categorieën van gegevens die mogen gevraagd worden;

- de beoogde doeleinden;

- de mechanismen ter controle van het verzoek om gegevens, die intern wordt uitgevoerd of, in voorkomend geval, door een rechterlijke instantie of door een onafhankelijke administratieve autoriteit.

De minister laat in het *Belgisch Staatsblad* een omzendbrief publiceren die een lijst omvat met de Belgische autoriteiten die gemachtigd zijn om van een operator gegevens te ontvangen die worden bewaard krachtens de artikelen 122, 123, 126, 126/1, 126/3 en 127.

Op het verzoek van de minister of van het Instituut verstrekken de Belgische autoriteiten bedoeld in de paragrafen 2 tot 4 de informatie die nodig is om deze omzendbrief op te stellen.

§ 6. De verzoeken die de autoriteiten richten aan de operatoren om bepaalde gegevens te verkrijgen die worden bewaard krachtens de artikelen 122, 123, 126, 126/1, 126/3 of 127, omvatten de volgende minimale vermeldingen :

1° de identiteit van de verzoekende autoriteit, of, wanneer het verzoek naar de operator verzonden wordt door een centrale dienst voor rekening van die autoriteit, de identiteit van die dienst;

2° de functie van de contactpersoon bij de verzoekende autoriteit, of, wanneer het verzoek naar de operator verzonden wordt door een centrale dienst voor rekening van die autoriteit, de functie van de contactpersoon bij die centrale dienst;

3° de juridische grondslag waarop het verzoek gebaseerd is, behalve wanneer het verzoek naar de operator wordt verzonden via een centrale dienst voor rekening van een andere autoriteit;

4° de gewenste antwoordtermijn.

§ 7. Het Instituut stuurt jaarlijks aan de minister en de minister van Justitie statistieken over de verstrekking aan de autoriteiten van gegevens bewaard krachtens de artikelen 122, 123,

126, 126/1, 126/3 en 127. Deze ministers sturen die jaarlijks door naar de Kamer van volksvertegenwoordigers.

Die statistieken omvatten met name :

1° de gevallen waarin bewaarde gegevens zijn verstrekt aan de bevoegde autoriteiten overeenkomstig de toepasselijke wettelijke bepalingen;

2° de tijd die is verstreken tussen de datum waarop de gegevens zijn bewaard en de datum waarop de bevoegde autoriteiten om de overdracht ervan verzochten;

3° de gevallen waarin verzoeken om bewaarde gegevens niet konden worden ingewilligd.

Die statistieken mogen geen persoonsgegevens noch vertrouwelijke informatie omvatten.

De gegevens die betrekking hebben op de toepassing van het tweede lid, 1°, worden tevens bijgevoegd bij het verslag dat de minister van Justitie overeenkomstig artikel 90*decies* van het Wetboek van strafvordering uitbrengt aan het Parlement.

Het Instituut vraagt aan de operatoren en aan de door de Koning aangewezen dienst de informatie aan de hand waarvan het de in het eerste lid bedoelde verplichting kan vervullen ».

B.84.1. De verzoekende partij in de zaak nr. 7930 leidt een eerste en een vierde middel af uit de schending van de artikelen 11, 12, 22 en 29 van de Grondwet, van artikel 15, lid 1, en van de artikelen 5, 6 en 9 van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8, 11, 47 en 52, lid 1, van het Handvest, de artikelen 6, 8, 10, 11 en 18 van het Europees Verdrag voor de rechten van de mens en de artikelen 13 en 54 van de richtlijn (EU) 2016/680, in zoverre artikel 13 van de wet van 20 juli 2022 een zeer ruime toegang verleent tot de betrokken gegevens, waarvoor op zich een algemene bewaarplicht bestaat. Zij voert in het bijzonder aan dat de bedoelde autoriteiten buiten het kader van de in artikel 15, lid 1, van de richtlijn 2002/58/EG opgesomde doeleinden vallen, dat er geen hiërarchie van doeleinden is vastgesteld, dat het in aanmerking genomen begrip « zware criminaliteit » niet in overeenstemming is met de rechtspraak van het Hof van Justitie en dat het aan de bevoegde minister staat om te bepalen welke autoriteiten toegang mogen hebben tot de gegevens, hetgeen niet bestaanbaar is met het formele wettigheidsbeginsel.

B.84.2. De verzoekende partij in de zaak nr. 7931 leidt een enig middel af uit de schending van de artikelen 11, 12, 22 en 29 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 7, 8, 11, 47 en 52, lid 1, van het Handvest, met artikel 8 van het Europees Verdrag voor de rechten van de mens, met de artikelen 5, 6 en 15 van de richtlijn 2002/58/EG en met de artikelen 13 en 54 van de richtlijn (EU) 2016/680. De verzoekende partij stelt dat artikel 13 van

de wet van 20 juli 2022 de bevoegde minister toestaat de autoriteiten op te sommen die gemachtigd zijn om toegang te hebben tot de bedoelde gegevens, hetgeen het formele wettigheidsbeginsel schendt, dat die bepaling niet vereist dat het verzoek om toegang wordt gemotiveerd ten opzichte van het nagestreefde doeleinde en dat de manier waarop « zware criminaliteit » wordt gedefinieerd niet in overeenstemming is met de rechtspraak van het Hof van Justitie.

B.84.3. De verzoekende partijen in de zaak nr. 7932 leiden een derde middel af uit de schending van de artikelen 10, 11, 15, 22 en 29 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 5, 6, 8, 9, 10, 11, 14 en 18 van het Europees Verdrag voor de rechten van de mens, met de artikelen 7, 8, 11, 47 en 52 van het Handvest, met artikel 5, lid 4, van het Verdrag betreffende de Europese Unie, met de richtlijn 2002/58/EG, met de richtlijn (EU) 2016/680 en met de AVG.

In een eerste onderdeel betogen de verzoekende partijen dat artikel 13 van de wet van 20 juli 2022 de door de rechtspraak van het Hof van Justitie opgelegde hiërarchie van de doeleinden niet in acht neemt, dat de in aanmerking genomen definitie van « zware criminaliteit » niet in overeenstemming is met die rechtspraak, dat de bedoelde autoriteiten te talrijk zijn en dat laatstgenoemde buiten het kader van de in artikel 15, lid 1, van de richtlijn 2002/58/EG opgesomde doeleinden vallen.

In een tweede onderdeel voeren de verzoekende partijen aan dat de grieven gericht tegen artikel 13 van de wet van 20 juli 2022 ook gelden voor de specifieke regels voor de toegang tot de gegevens bepaald bij de hoofdstukken 3 tot 10 van de wet van 20 juli 2022, die daarenboven niet systematisch in de nodige procedurele waarborgen noch in een onafhankelijke controle bij de toegang tot gevoelige gegevens voorzien. In dat verband citeren de verzoekende partijen de artikelen 21, 24, 26, 27, 28, 33, 34, 35, 37, 40, 41, 42 en 44 van de wet van 20 juli 2022.

B.85. De grieven van de verzoekende partijen zijn in hoofdzaak afgeleid uit de schending van het recht op eerbiediging van het privéleven en het recht op bescherming van de persoonsgegevens, gewaarborgd bij artikel 22 van de Grondwet, bij artikel 8 van het Europees Verdrag voor de rechten van de mens, bij de artikelen 7, 8 en 52, lid 1, van het Handvest, bij de

richtlijn 2002/58/EG, bij de richtlijn (EU) 2016/680 en bij de AVG. Zij formuleren niet uitdrukkelijk een grief die is afgeleid uit de schending van de andere in B.84.1 tot B.84.3 aangehaalde referentienormen.

B.86. Artikel 127/1 van de wet van 13 juni 2005 heeft betrekking op de toegang tot de gegevens die worden bewaard krachtens de artikelen 122, 123, 126, 126/1, 126/3 en 127 van die wet.

B.87.1. Uit de bewoordingen van artikel 127/1 van de wet van 13 juni 2005 en uit de parlementaire voorbereiding ervan blijkt dat die bepaling niet de toegang regelt tot de bij de artikelen 122, 123, 126, 126/1, 126/3 en 127 van de wet van 13 juni 2005 bedoelde gegevens (*Parl. St.,* Kamer, 2021-2022, DOC 55-2572/001, pp. 96-97).

B.87.2. Artikel 127/1 van de wet van 13 juni 2005 is immers beperkt tot de opsomming van de autoriteiten en de doeleinden die de toegang tot de op grond van de artikelen 122, 123, 126, 126/1, 126/3 en 127 van de wet van 13 juni 2005 bewaarde gegevens mogelijk kunnen maken. Hoewel artikel 127/1 zich ertegen verzet dat een andere autoriteit wordt aangewezen of dat een ander doeleinde wordt aangevoerd met het oog op de toegang tot de voormelde gegevens, verleent het op zich evenmin toegang voor alle erin opgesomde autoriteiten en doeleinden, zoals de afdeling wetgeving van de Raad van State heeft opgemerkt in haar advies over het voorontwerp van wet dat aan de oorsprong ligt van de wet van 20 juli 2022 (*ibid.*, pp. 309-311).

B.87.3. De in artikel 127/1 van de wet van 13 juni 2005 bepaalde voorwaarden zijn inderdaad niet toereikend om de toegang tot de betrokken gegevens mogelijk te maken. Er wordt immers vereist dat een specifieke « formele wettelijke norm » wordt aangenomen (artikel 127/1, §§ 2 en 3) en dat in die norm « de categorie of categorieën van ondernemingen waaraan de autoriteit gegevens kan vragen » worden verduidelijkt, alsook « de categorieën van gegevens die mogen gevraagd worden », « de beoogde doeleinden » en « de mechanismen ter controle van het verzoek om gegevens, die intern wordt uitgevoerd of, in voorkomend geval, door een rechterlijke instantie of door een onafhankelijke administratieve autoriteit » (artikel 127/1, § 5).

Het is via de verschillende « formele wettelijke normen » bedoeld in artikel 127/1 dat het aan de wetgever staat om tussen de verschillende soorten bewaarde gegevens het onderscheid te maken dat geboden is, zodat wordt gewaarborgd dat, voor elke soort gegevens, de inmenging tot het strikt noodzakelijke wordt beperkt.

B.88. Derhalve kunnen de grieven van de verzoekende partijen, in zoverre zij betrekking hebben op de toegang tot de gegevens waarvan de bewaring is toegestaan bij de wet van 13 juni 2005, niet worden toegeschreven aan artikel 127/1 van die wet, maar aan de in die bepaling bedoelde « formele wettelijke normen » die bepalen welke gegevens worden beoogd, welke autoriteiten toegang ertoe mogen vragen, welke precieze doeleinden worden nagestreefd en welke eventuele controlemechanismen voorhanden zijn.

In dat kader kan het tweede onderdeel van het derde middel dat de verzoekende partijen in de zaak nr. 7932 aanvoeren, niet worden geacht betrekking te hebben op dergelijke formele wetskrachtige normen, aangezien die partijen zich beperken tot de vermelding van de artikelen 21, 24, 26, 27, 28, 33, 34, 35, 37, 40, 41, 42 en 44 van de wet van 20 juli 2022, zonder dat daarbij wordt aangetoond in welk opzicht die artikelen een toepassing vormen van artikel 127/1 van de wet van 13 juni 2005, en zij evenmin staven in welk opzicht die bepalingen de in B.85 aangehaalde referentienormen concreet zouden schenden.

B.89. Tot slot, wat betreft de bestaanbaarheid van artikel 127/1, § 5, tweede lid, van de wet van 13 juni 2005 met het beginsel van de formele wettigheid, in zoverre die bepaling erin voorziet dat de bevoegde minister in het *Belgisch Staatsblad* een omzendbrief laat publiceren met de lijst van de Belgische autoriteiten die gemachtigd zijn om van een operator toegang te krijgen tot de gegevens die worden bewaard krachtens de artikelen 122, 123, 126, 126/1, 126/3 en 127 van de wet van 13 juni 2005, strekt die bepaling enkel ertoe de voormelde minister toe te staan om in een omzendbrief alle autoriteiten bedoeld in de « formele wettelijke normen », waarvan sprake is in artikel 127/1 van de wet van 13 juni 2005, op te sommen.

Artikel 127/1, § 5, tweede lid, machtigt een minister niet ertoe te bepalen welke autoriteiten bevoegd zijn om toegang te hebben tot de in de artikelen 122, 123, 126, 126/1, 126/3 en 127 van de wet van 13 juni 2005 bedoelde gegevens.

B.90. Het eerste en het vierde middel in de zaak nr. 7930, het enige middel in de zaak nr. 7931 en het eerste en het tweede onderdeel van het derde middel in de zaak nr. 7932 zijn niet gegrond in zoverre zij betrekking hebben op artikel 13 van de wet van 20 juli 2022.

B.91.1. In haar enige middel klaagt de verzoekende partij in de zaak nr. 7931 eveneens aan dat de persoon tot wiens gegevens toegang wordt verleend, niet wordt ingelicht en dat er geen rechtsmiddelen voorhanden zijn in geval van onwettige toegang tot die gegevens. Wat het voormelde gebrek aan informatieverstrekking betreft, vraagt zij in ondergeschikte orde dat een prejudiciële vraag wordt gesteld aan het Hof van Justitie.

B.91.2. De verzoekende partijen in de zaak nr. 7932 leiden een vierde middel af uit de schending van de artikelen 10, 11, 13 en 22 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 5, 6, 8, 9, 10, 11, 14 en 18 van het Europees Verdrag voor de rechten van de mens, met de artikelen 7, 8, 11, 47 en 52 van het Handvest, met artikel 5, lid 4, van het Verdrag betreffende de Europese Unie, met de richtlijn 2002/58/EG, met de richtlijn (EU) 2016/680 en met de AVG. In dat middel klagen de verzoekende partijen in het algemeen aan dat de gebruiker niet in kennis wordt gesteld wanneer de bevoegde autoriteiten toegang hebben tot de gegevens, wat strijdig zou zijn met het recht op toegang tot de rechter en met het recht op een daadwerkelijk rechtsmiddel, zonder daarbij evenwel een specifieke bepaling van de wet van 20 juli 2022 te beogen.

B.91.3. Hoewel die middelen kunnen worden geacht betrekking te hebben op artikel 127/1 van de wet van 13 juni 2005, moet in herinnering worden gebracht, zoals vermeld in B.87.1, dat die bepaling op zich geen toegang verleent tot de betrokken gegevens. Bijgevolg is het verzoek van de verzoekende partij in de zaak nr. 7931 om een prejudiciële vraag te stellen niet pertinent in het kader van artikel 127/1 van de wet van 13 juni 2005.

In zoverre het vierde middel in de zaak nr. 7932 betrekking zou hebben op de specifieke « formele wettelijke normen » bedoeld in artikel 127/1 van de wet van 13 juni 2005, beogen de verzoekende partijen geen specifieke wetsbepaling om hun grieven te staven, noch leggen zij uit in welk opzicht die specifieke formele wetskrachtige normen de in B.85 aangehaalde referentienormen zouden schenden.

B.91.4. Het enige middel in de zaak nr. 7931, in zoverre het betrekking heeft op de in B.91.1 vermelde grieven, en het vierde middel in de zaak nr. 7932 zijn niet gegrond.

9. De bevoegdheden van de officieren van gerechtelijke politie van het BIPT (artikel 24)

B.92. Het enige middel in de zaak nr. 7931 heeft betrekking op artikel 24 van de wet van 20 juli 2022. Die bepaling voegt een artikel 25/1 in de wet van 17 januari 2003 « met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector » (hierna : de wet van 17 januari 2003) in, dat bepaalt :

« § 1. Om een inbreuk bedoeld in artikel 145, § 3 of § 3*bis*, van de wet van 13 juni 2005 betreffende de elektronische communicatie of in artikel 24, § 1, 2°, te kunnen opsporen, vaststellen of vervolgen, kan een officier van gerechtelijke politie van het Instituut, schriftelijk :

1° van een operator eisen om te antwoorden op een verzoek om identificatiegegevens, dat voor deze doeleinden noodzakelijk is;

2° de medewerking vorderen van de personen en instellingen bedoeld in artikel 46*quater*, § 1, van het Wetboek van strafvordering en van verenigingen die hen vertegenwoordigen, op basis van het kenmerk van de onlinebetaling specifiek voor een elektronische-communicatiedienst die voorafgaandelijk meegedeeld is door een operator overeenkomstig de bepaling onder 1°, om de persoon te identificeren die de dienst heeft betaald;

3° de medewerking vorderen van de gesloten centra of woonunits in de zin van de artikelen 74/8 en 74/9 van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen, waar de inschrijving van de abonnee op een elektronische-communicatiedienst heeft plaatsgevonden, op basis van de contactgegevens van het centrum of de woonunit die voorafgaandelijk meegedeeld zijn door een operator overeenkomstig de bepaling onder 1°, om de abonnee te identificeren;

4° de medewerking vorderen van alle andere rechtspersonen die abonnee zijn van een operator, of die intekenen in naam en voor rekening van natuurlijke personen op een elektronische-communicatiedienst, op basis van de gegevens die voorafgaandelijk meegedeeld zijn door een operator overeenkomstig de bepaling onder 1°, om de abonnee of de gewoonlijke gebruiker van de dienst te identificeren.

Een in het eerste lid bedoeld verzoek mag aan een in het eerste lid bedoelde actor pas worden doorgestuurd na de schriftelijke toestemming van een in artikel 24, § 2, bedoelde officier van gerechtelijke politie. Deze toestemming mag maar worden verleend op schriftelijk en met redenen omkleed verzoek gericht aan deze officier overeenkomstig paragraaf 5.

§ 2. Ten behoeve van de vervulling van zijn opdrachten kan een officier van gerechtelijke politie van het Instituut van een operator schriftelijk eisen om te antwoorden op een verzoek

om metagegevens, die nodig zijn om een inbreuk bedoeld in artikel 145, § 3, of § 3*bis*, van de wet van 13 juni 2005 betreffende de elektronische communicatie of in artikel 24, § 1, 2°, te kunnen opsporen, vaststellen of vervolgen.

Tenzij in geval van een naar behoren gerechtvaardigde hoogdringendheid, mag de officier van gerechtelijke politie van het Instituut het verzoek aan de operator pas richten na het voorleggen van een schriftelijk en met redenen omkleed verzoek aan de onderzoeksrechter en na schriftelijke toestemming van deze laatste.

In geval van een naar behoren gerechtvaardigde hoogdringendheid zoals bedoeld in het tweede lid, deelt de officier van gerechtelijke politie van het Instituut na de verzending van het verzoek naar de operator onverwijld een kopie van dit verzoek, de motivering van het verzoek alsook de rechtvaardiging van de hoogdringendheid mee aan de onderzoeksrechter. De onderzoeksrechter voert daarna een controle uit.

Wanneer na deze latere controle de onderzoeksrechter weigert de geldigheid te bevestigen van het verzoek dat door de officier van gerechtelijke politie van het Instituut naar de operator is verstuurd, laat deze officier dat onverwijld aan de betrokken operator weten en wist hij de ontvangen metagegevens.

§ 3. In afwijking van de paragrafen 1 en 2, teneinde de naleving te controleren van de artikelen 126, 126/1, 126/2, 126/3 of 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van de uitvoeringsbesluiten ervan en op schriftelijk en met redenen omkleed verzoek van een officier van gerechtelijke politie van het Instituut, verleent een operator binnen de termijn die vastgesteld is in de vordering toegang zodat zijn databanken die een van deze artikelen of een van deze uitvoeringsbesluiten uitvoeren, geraadpleegd kunnen worden.

Een in het eerste lid bedoeld verzoek mag pas naar een operator worden doorgestuurd na de schriftelijke toestemming van een in artikel 24, § 2, bedoelde officier van gerechtelijke politie van het Instituut. Deze toestemming mag maar worden verleend op schriftelijk en met redenen omkleed verzoek overeenkomstig paragraaf 5.

Het aan de operator gerichte verzoek vermeldt nauwkeurig de naam van de officieren van gerechtelijke politie van het Instituut die de databank kunnen raadplegen.

Deze officieren mogen enkel een kopie nemen van de gegevens en documenten die worden geraadpleegd in het kader van het eerste lid teneinde inbreuken vast te stellen gepleegd door de operator.

§ 4. Voor de toepassing van de paragrafen 1 en 2, delen de actoren bedoeld in paragraaf 1, eerste lid, aan wie een officier van gerechtelijke politie van het Instituut gegevens gevraagd heeft, de gevraagde gegevens mee in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering.

Voor de toepassing van de paragrafen 1 tot 3, is iedere persoon die uit hoofde van zijn functie kennis krijgt van de maatregel of daaraan zijn medewerking verleent, tot geheimhouding verplicht. Iedere schending van de geheimhoudingsplicht wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

Iedere persoon die de gegevens weigert mee te delen of niet meedeelt in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering, wordt gestraft met een geldboete van zesentwintig euro tot tienduizend euro.

Iedere persoon die weigert de raadpleging van de databank mogelijk te maken overeenkomstig paragraaf 3 of die deze raadpleging niet mogelijk maakt binnen de termijn bepaald in de vordering, wordt gestraft met een geldboete van zesentwintig euro tot tienduizend euro.

§ 5. Voor de toepassing van de paragrafen 1 tot 3 moet de motivering van het verzoek gericht aan de officier van gerechtelijke politie bedoeld in artikel 24, § 2, of aan de onderzoeksrechter uitgewerkt zijn in het licht van de omstandigheden van het onderzoek.

Voor de toepassing van de paragrafen 1 en 2 vermeldt deze motivering :

1° het verband tussen de gevraagde gegevens en het doel van de opsporing, vaststelling of de vervolging van de specifieke inbreuk dat het verzoek rechtvaardigt;

2° de strikt noodzakelijke aard van de gegevens die worden gevraagd in het kader van het onderzoek.

§ 6. De officieren van gerechtelijke politie van het Instituut nemen op in een inventaris :

1° alle verzoeken bedoeld in de paragrafen 1, 2 en 3;

2° de motivering van het verzoek en de rechtvaardiging van de hoogdringendheid die meegedeeld zijn aan de onderzoeksrechter overeenkomstig paragraaf 2, derde lid;

3° de in de paragrafen 1, 2 en 3 bedoelde toestemmingen ».

B.93. De verzoekende partij in de zaak nr. 7931 leidt een enig middel af uit de schending van de artikelen 11, 12, 22 en 29 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 7, 8, 11, 47 en 52, lid 1, van het Handvest, met artikel 8 van het Europees Verdrag voor de rechten van de mens, met de artikelen 5, 6 en 15 van de richtlijn 2002/58/EG en met de artikelen 13 en 54 van de richtlijn (EU) 2016/680. Zij voert aan dat artikel 25/1 van de wet van 17 januari 2003 de voormelde referentienormen schendt in zoverre het de toegang tot de gegevens toestaat, in het kader van een strafrechtelijke procedure, door een officier van gerechtelijke politie, die geen onafhankelijke instantie is, en in zoverre het geen rechterlijke toetsing vóór die toegang oplegt. Zij klaagt overigens ook het feit aan dat de persoon tot wiens gegevens men zich toegang verschaft, daarover niet wordt geïnformeerd, alsook de ontstentenis van rechtsmiddelen bij een onwettige toegang tot de gegevens. Wat het voormelde gebrek aan informatie betreft, verzoekt zij in ondergeschikte orde om een prejudiciële vraag te stellen aan het Hof van Justitie.

B.94. De grieven van de verzoekende partijen zijn enkel afgeleid uit de schending van het recht op eerbiediging van het privéleven en van het recht op de bescherming van persoonsgegevens, die worden gewaarborgd door artikel 22 van de Grondwet, door artikel 8 van het Europees Verdrag voor de rechten van de mens, door de artikelen 7, 8 en 52, lid 1, van het Handvest, door de richtlijn 2002/58/EG, door de richtlijn (EU) 2016/680 en door de AVG.

B.95. In het kader van een strafrechtelijke procedure machtigt artikel 25/1 van de wet van 17 januari 2003 een officier van gerechtelijke politie van het BIPT ertoe zich in twee gevallen toegang te verschaffen tot de gegevens. Ten eerste kan de officier van gerechtelijke politie zich toegang verschaffen tot identificatiegegevens om de in artikel 145, §§ 3 en 3*bis*, van de wet van 13 juni 2005 en in artikel 24, § 1, 2°, van de wet van 17 januari 2003 bedoelde inbreuken op te sporen, vast te stellen of te vervolgen (artikel 25/1, § 1). Ten tweede kan de officier van gerechtelijke politie zich, ten behoeve van de vervulling van zijn opdrachten, toegang verschaffen tot de metagegevens die noodzakelijk zijn om de voormelde inbreuken op te sporen, vast te stellen of te vervolgen (artikel 25/1, § 2).

B.96. Ten aanzien van hetgeen voorafgaat, beperkt het Hof zijn onderzoek tot artikel 25/1, §§ 1 en 2, van de wet van 17 januari 2003.

B.97. Daar de bestreden bepaling verwijst naar bepalingen waaromtrent het Hof prejudiciële vragen stelt aan het Hof van Justitie, past het de uitspraak over het onderzoek omtrent die middelen aan te houden in afwachting van het antwoord van het Hof van Justitie op de gestelde prejudiciële vragen.

10. De bevoegdheden van de procureur des Konings (artikelen 25 en 26)

B.98.1. Het enige middel in de zaak nr. 7931 heeft onder meer betrekking op de artikelen 25 en 26 van de wet van 20 juli 2022.

B.98.2. Bij artikel 25 van de wet van 20 juli 2022 wordt een artikel 39*quinquies* ingevoegd in het Wetboek van strafvordering, dat bepaalt :

« § 1. Bij het opsporen van de misdaden en de wanbedrijven kan de procureur des Konings, wanneer er ernstige aanwijzingen zijn dat de misdrijven een correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben, bij een met redenen omklede en schriftelijke beslissing aan een of meerdere van de actoren bedoeld in het tweede lid bevelen de gegevens bedoeld in artikel 88*bis*, § 1, eerste lid, die hij noodzakelijk acht en die door hen worden gegenereerd of verwerkt in het kader van de verstrekking van de betrokken communicatiediensten, te bewaren.

Het bevel bedoeld in het eerste lid kan, rechtstreeks of via de door de Koning aangewezen politiedienst, gegeven worden aan :

- de operator van een elektronische communicatienetwerk; en

- iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronische communicatienetwerk informatie te verkrijgen, te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen.

De met redenen omklede en schriftelijke beslissing vermeldt :

- de naam van de procureur des Konings die de bewaring beveelt;

- het strafbare feit waarop het bevel betrekking heeft;

- de feitelijke omstandigheden van de zaak die de bewaring van de gegevens rechtvaardigen;

- de precieze aanduiding van één of meerdere van de volgende elementen : de persoon of de personen, de communicatiemiddelen of de plaatsen waarop de bewaring betrekking heeft;

- in voorkomend geval, de categorieën van verkeers- en locatiegegevens die bewaard moeten worden;

- de duur van de maatregel, die niet langer kan zijn dan twee maanden te rekenen vanaf het bevel, onverminderd een hernieuwing;

- de duur van bewaring van deze gegevens, die niet langer mag zijn dan zes maanden. Deze termijn kan schriftelijk worden verlengd.

In spoedeisende gevallen kan het bevel tot bewaring mondeling worden gegeven. Het bevel moet zo spoedig mogelijk worden bevestigd in de vorm bepaald in het derde lid.

§ 2. De actoren bedoeld in paragraaf 1, tweede lid, zorgen ervoor dat de integriteit, de kwaliteit en de beschikbaarheid van de gegevens gewaarborgd is en dat de gegevens op een veilige manier bewaard worden.

§ 3. Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

Iedere persoon die weigert mee te werken, of die de bewaarde gegevens doet verdwijnen, vernietigt of wijzigt, wordt gestraft met een gevangenisstraf van zes maanden tot een jaar en met een geldboete van zesentwintig euro tot twintigduizend euro of met één van die straffen alleen.

§ 4. De toegang tot de overeenkomstig dit artikel bewaarde gegevens is slechts mogelijk met toepassing van artikel 88*bis* ».

B.98.3. Artikel 26 van de wet van 20 juli 2022 wijzigt artikel 46*bis* van het Wetboek van strafvordering als volgt :

« 1° in paragraaf 1 wordt tussen het tweede en het derde lid een lid ingevoegd, luidende :

‘ Met het oog op de identificatie van de abonnee of de gewoonlijke gebruiker van een dienst bedoeld in het tweede lid, tweede streepje, kan hij ook, rechtstreeks of via de door de Koning aangewezen politiedienst, de medewerking vorderen van :

- de personen of instellingen bedoeld in artikel 46*quater*, § 1, op basis van de referentie van een elektronische banktransactie die voorafgaandelijk meegedeeld is door een van de actoren bedoeld in het tweede lid, eerste en tweede streepje, met toepassing van het eerste lid;

- de gesloten centra of woonunits in de zin van de artikelen 74/8 en 74/9 van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen, op basis van de contactgegevens van het centrum of de woonunit waar de intekening door de abonnee op een mobiele elektronische communicatiedienst heeft plaatsgevonden, die voorafgaandelijk meegedeeld zijn door een van de actoren bedoeld in het tweede lid, eerste en tweede streepje, met toepassing van het eerste lid;

- andere rechtspersonen die de abonnee zijn van een van de actoren bedoeld in het tweede lid, eerste of tweede streepje, of die zich in naam en voor rekening van natuurlijke personen abonneren op een elektronische communicatiedienst, op basis van gegevens die voorafgaandelijk meegedeeld zijn door een van de actoren bedoeld in het tweede lid, eerste en tweede streepje, met toepassing van het eerste lid. ’;

2° in paragraaf 2 worden het derde en het vierde lid opgeheven;

3° het artikel wordt aangevuld met de paragrafen 3 en 4, luidende :

‘ § 3. De actoren bedoeld in paragraaf 1, derde lid, eerste tot derde streepje, van wie de identificatie van de abonnee of de gewoonlijke gebruiker van een dienst bedoeld in paragraaf 1, tweede lid, tweede streepje, gevorderd wordt, verstrekken de procureur des Konings of de officier van gerechtelijke politie de gegevens in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering.

§ 4. Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

Iedere persoon die de gegevens weigert mee te delen of niet meedeelt in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering, wordt gestraft met geldboete van zesentwintig euro tot tienduizend euro. ' ».

B.99.1. De verzoekende partij in de zaak nr. 7931 leidt een enig middel af uit de schending van de artikelen 11, 12, 22 en 29 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 7, 8, 11, 47 en 52, lid 1, van het Handvest, met artikel 8 van het Europees Verdrag voor de rechten van de mens, met de artikelen 5, 6 en 15 van de richtlijn 2002/58/EG en met de artikelen 13 en 54 van de richtlijn (EU) 2016/680.

De verzoekende partij in de zaak nr. 7931 voert aan dat artikel 39*quinquies* van het Wetboek van strafvordering betrekking heeft op criminaliteit « in het algemeen », terwijl, enerzijds, het Hof van Justitie zich beperkt tot de gevallen van « zware » criminaliteit en, anderzijds, die bepaling voorziet in een onevenredige bewaringstermijn.

Wat de in artikel 46*bis* van het Wetboek van strafvordering aangebrachte wijzigingen betreft, voert de verzoekende partij allereerst aan dat die bepaling de procureur des Konings of, in geval van uiterst dringende noodzakelijkheid, een officier van gerechtelijke politie toestaat om zich toegang te verschaffen tot identificatiegegevens zonder dat die toegang afhankelijk wordt gesteld van een voorafgaande en onafhankelijke toetsing, zoals het Hof van Justitie vereist. In ondergeschikte orde verzoekt zij om een prejudiciële vraag te stellen aan het Hof van Justitie. Bovendien voert de verzoekende partij aan dat artikel 46*bis* van het Wetboek van strafvordering, zoals het werd gewijzigd, de procureur des Konings, in geval van dringende noodzakelijkheid, toestaat om zich toegang te verschaffen tot de verkeers- en locatiegegevens met het oog op de bestrijding van criminaliteit in het algemeen, hetgeen evenmin verenigbaar is met de vereisten van het Hof van Justitie. In ondergeschikte orde verzoekt zij om in dat verband een prejudiciële vraag te stellen aan dat rechtscollege. Bovendien voert de verzoekende partij aan dat de medewerking van de gesloten centra en woonunits, bedoeld in artikel 46*bis* van het Wetboek van strafvordering, niet verantwoord is ten aanzien van de bestrijding van criminaliteit. Ten slotte betoogt zij dat artikel 46*bis* van het Wetboek van strafvordering niet erin voorziet dat de persoon wordt geïnformeerd over de toegang tot de gegevens, noch over

het bestaan van een specifiek rechtsmiddel. Wat het voormelde gebrek aan informatie betreft, verzoekt zij om een prejudiciële vraag te stellen aan het Hof van Justitie.

B.99.2. De grieven van de verzoekende partij die zijn gericht tegen de artikelen 39*quinquies* en 46*bis* van het Wetboek van strafvordering, zijn enkel afgeleid uit de schending van het recht op eerbieding van het privéleven en van het recht op de bescherming van persoonsgegevens, zoals gewaarborgd door artikel 22 van de Grondwet, door artikel 8 van het Europees Verdrag voor de rechten van de mens, door de artikelen 7, 8 en 52, lid 1, van het Handvest, door de richtlijn 2002/58/EG en door de richtlijn (EU) 2016/680.

B.100. Het Hof onderzoekt eerst de grieven die zijn gericht tegen artikel 39*quinquies* van het Wetboek van strafvordering, en vervolgens die met betrekking tot artikel 46*bis* van hetzelfde Wetboek.

B.101.1. In het dictum van zijn voormelde arrest van 6 oktober 2020 heeft het Hof van Justitie voor recht verklaard dat artikel 15, lid 1, van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8, 11 en 52, lid 1, van het Handvest, zich niet verzet tegen een maatregel « die het mogelijk [maakt] om ten behoeve van de bestrijding van zware criminaliteit en, *a fortiori*, de bescherming van de nationale veiligheid via een aan effectieve rechterlijke toetsing onderworpen beslissing van de bevoegde autoriteit aan aanbieders van elektronische-communicatiediensten een bevel op te leggen tot spoedbewaring van de in hun handen zijnde verkeers- en locatiegegevens gedurende een bepaalde periode ».

B.101.2. In zijn rechtspraak omschrijft het Hof van Justitie het begrip « zware criminaliteit » niet. Zoals blijkt uit de conclusie van de advocaat-generaal die voorafgaan aan het voormelde in grote kamer gewezen arrest van het Hof van Justitie van 2 oktober 2018 in zake *Ministerio Fiscal* behoort dat begrip in beginsel tot de bevoegdheid van de lidstaten, ook al staat het aan het Hof van Justitie om de eerbiediging te verzekeren van alle vereisten die uit het recht van de Europese Unie voortvloeien, en met name toe te zien op een eenvormige toepassing van de bescherming waarin de bepalingen van het Handvest voorzien. De juridische kwalificatie van een strafbaar feit kan immers niet alleen van lidstaat tot lidstaat verschillen, naargelang van de in iedere lidstaat gevolgde tradities en gestelde prioriteiten, maar is ook tijdsgebonden en kan veranderen als gevolg van een strengere of juist minder strenge koers van het strafrechtbeleid teneinde rekening te houden met de ontwikkeling van de criminaliteit,

alsook, in meer algemene zin, met de veranderingen van de maatschappij en van de bestaande behoeften, met name op het vlak van repressie, op nationaal niveau. Bovendien, wat de zwaarte van de straf betreft, zegt het feit dat een lidstaat op een bepaald strafbaar feit een korte gevangenisstraf of zelfs een alternatieve straf stelt, niets over de intrinsieke ernst van het type strafbaar feit (conclusie van advocaat-generaal Henrik Saugmandsgaard Øe, voorafgaand aan HvJ, grote kamer, 2 oktober 2018, C-207/16, voormeld, punten 93-100).

Het Hof van Justitie heeft in dat verband benadrukt dat de definitie die in het nationale recht wordt gegeven van « ernstige strafbare feiten » op grond waarvan toegang kan worden verleend tot de door de aanbieders van elektronische-communicatiediensten bewaarde gegevens, op basis waarvan precieze conclusies kunnen worden getrokken over de persoonlijke levenssfeer van de betrokkenen, niet zo ruim mag zijn dat de toegang tot die gegevens de regel in plaats van de uitzondering wordt. Die definitie kan dus niet de overgrote meerderheid van de strafbare feiten omvatten, hetgeen het geval zou zijn indien de drempel waarboven de maximumgevangenisstraf van een strafbaar feit als ernstig strafbaar feit wordt aangemerkt, op een buitensporig laag niveau zou worden vastgesteld (HvJ, grote kamer, 30 april 2024, C-178/22, *Procura della Repubblica presso il Tribunale di Bolzano,* ECLI:EU:C:2024:371, punt 55).

B.101.3. Wat de evenredigheid van de termijn voor het bewaren van de voormelde gegevens betreft, heeft het Hof van Justitie bij zijn voormelde arrest van 6 oktober 2020 geoordeeld dat « de bewaartermijn niet langer [mag] zijn dan strikt noodzakelijk, zij het dat die termijn kan worden verlengd wanneer de omstandigheden en het met de betrokken maatregel beoogde doel dit rechtvaardigen » (punt 164).

B.102.1. Te dezen toont de verzoekende partij niet aan in welk opzicht de wetgever de nationale beoordelingsmarge te buiten zou zijn gegaan door, in artikel 39*quinquies*, § 1, eerste lid, van het Wetboek van strafvordering, het begrip « zware criminaliteit » te omschrijven onder verwijzing naar de misdrijven die « een correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben ». Evenmin blijkt in welk opzicht die definitie de in B.99.2 aangehaalde referentienormen zou schenden. In dat verband heeft de afdeling wetgeving van de Raad van State in haar advies over het voorontwerp van wet dat aan de oorsprong van de wet van 20 juli 2022 ligt, net opgemerkt dat, « wat het openbaar ministerie betreft, [...] de naleving van het criterium ‘ zware criminaliteit ’ tevens uit het ontworpen artikel 39*quinquies*,

van het Wetboek van Strafvordering [volgt] » (*Parl. St.,* Kamer, 2021-2022, DOC 55-2572/001, p. 310). Overigens moet de kwalificatie van een strafbaar feit als ernstig misdrijf concreet worden beoordeeld, onder toezicht van de strafrechter, in het licht van de aard van het gepleegde feit en van het geheel van feiten van de zaak.

De strafrechter moet de toegang tot de betrokken gegevens met name kunnen weigeren wanneer die wordt gevraagd in het kader van een strafvervolging wegens een strafbaar feit dat kennelijk niet ernstig is (HvJ, grote kamer, 30 april 2024, C-178/22, voormeld, punt 62).

B.102.2. Wat de duur van bewaring van de beoogde gegevens betreft, voorziet artikel 39*quinquies* van het Wetboek van strafvordering in een termijn die niet langer mag zijn dan zes maanden, die evenwel schriftelijk kan worden verlengd (artikel 39*quinquies*, § 1, derde lid). De precieze duur van bewaring moet, behalve in spoedeisende gevallen, schriftelijk worden vermeld en met redenen zijn omkleed, zodat het aan de procureur des Konings staat om, onder toezicht van de strafrechter, te bewijzen dat de bewaringstermijn die hij oplegt, zich beperkt tot wat strikt noodzakelijk is en om, in geval van verlenging, de omstandigheden en de doelstellingen die een dergelijke maatregel rechtvaardigen, aan te tonen.

B.103.1. Artikel 46*bis* van het Wetboek van strafvordering, zoals gewijzigd bij de wet van 20 juli 2022, strekt ertoe de procureur des Konings de mogelijkheid te bieden om over te gaan tot de identificatie van de abonnee of de gewoonlijke gebruiker van een dienst bedoeld in het tweede lid van die bepaling, namelijk die welke wordt verleend door « de operator van een elektronisch communicatienetwerk » en « iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen, te ontvangen of te verspreiden », definitie die ook « de verstrekker van een elektronische communicatiedienst » omvat.

B.103.2. Uit de parlementaire voorbereiding van de wet van 20 juli 2022 blijkt dat artikel 46*bis* van het Wetboek van strafvordering, zoals gewijzigd bij die wet, betrekking moet hebben op de in artikel 127 van de wet van 13 juni 2005 bedoelde identificatiegegevens (*Parl. St.,* Kamer, 2021-2022, DOC 55-2572/002, pp. 148-151).

B.103.3. Aangezien, om de redenen vermeld in B.48.1 tot B.48.4, artikel 126 van de wet van 13 juni 2005, ingevoegd bij artikel 8 van de wet van 20 juli 2022, de in B.49 aangehaalde referentienormen niet schendt, geldt hetzelfde wat betreft artikel 46*bis* van het Wetboek van strafvordering, zoals gewijzigd bij de wet van 20 juli 2022.

B.103.4. Het Hof van Justitie en het Europees Hof voor de Rechten van de Mens eisen noch dat een voorafgaande rechterlijke of bestuurlijke toetsing wordt ingevoerd, noch dat de betrokken persoon wordt ingelicht over een toegang tot identificatiegegevens, noch dat in een specifiek beroep wordt voorzien. Bijgevolg kan de wetgever niet worden verweten dat hij in artikel 46*bis* van het Wetboek van strafvordering, zoals gewijzigd bij de wet van 20 juli 2022, niet in dergelijke nadere regels heeft voorzien, aangezien die bepaling enkel betrekking heeft op identificatiegegevens. Bijgevolg is het niet noodzakelijk om de door de verzoekende partij in dat verband gevraagde prejudiciële vragen te stellen.

B.103.5. In zoverre de verzoekende partij aanvoert dat artikel 46*bis* van het Wetboek van strafvordering de procureur des Konings, in geval van dringende noodzakelijkheid, toestaat om zich toegang te verschaffen tot de verkeers- en locatiegegevens met het oog op de bestrijding van criminaliteit in het algemeen, mist het enige middel feitelijke grondslag, aangezien, zoals in B.103.2 is vermeld, artikel 26 van de wet van 20 juli 2022, dat het voormelde artikel 46*bis* wijzigt, enkel betrekking heeft op de identificatiegegevens en niet op de verkeers- en locatiegegevens. Bijgevolg is er geen aanleiding om de door de verzoekende partij in dat verband gevraagde prejudiciële vraag te stellen.

B.103.6. Ten slotte, wat betreft de mogelijkheid waarover de procureur des Konings beschikt om de medewerking van de gesloten centra en woonunits, bedoeld in artikel 46*bis*, § 1, tweede lid, tweede streepje, van het Wetboek van strafvordering, te vorderen, zet de verzoekende partij geen enkel concreet element uiteen dat de ontstentenis van het noodzakelijke karakter van de maatregel kan aantonen.

B.103.7. Het enige middel in de zaak nr. 7931 is niet gegrond in zoverre het betrekking heeft op de artikelen 25 en 26 van de wet van 20 juli 2022.

11. De bevoegdheden van de onderzoeksrechter (artikel 27)

B.104. Het vijfde middel in de zaak nr. 7930 en het enige middel in de zaak nr. 7931 hebben betrekking op artikel 27 van de wet van 20 juli 2022, dat bepaalt :

« In artikel 88*bis* van [het Wetboek van strafvordering], ingevoegd bij de wet van 11 februari 1991, vervangen bij de wet van 10 juni 1998 en laatstelijk gewijzigd bij de wet van 5 mei 2019, worden de volgende wijzigingen aangebracht :

1° paragraaf 2, vervangen bij artikel 9 van de wet van 29 mei 2016, zelf vernietigd door arrest n° 57/2021 van het Grondwettelijk Hof, wordt vervangen als volgt :

‘ § 2. Wat betreft de toepassing van de maatregel bedoeld in paragraaf 1, eerste lid, op de verkeers- of lokalisatiegegevens die worden bewaard krachtens de artikelen 126/1 en 126/3 van de wet van 13 juni 2005 betreffende de elektronische communicatie, zijn de volgende bepalingen van toepassing :

- voor een strafbaar feit bedoeld in boek II, titel I*ter*, van het Strafwetboek mag de onderzoeksrechter in zijn bevelschrift de gegevens opvragen voor een periode van twaalf maanden voorafgaand aan het bevelschrift;

- voor een ander strafbaar feit bedoeld in artikel 90*ter*, §§ 2 tot 4, dat niet bedoeld is in het eerste gedachtestreepje, of een strafbaar feit dat gepleegd is in het kader van een criminele organisatie als bedoeld in artikel 324*bis* van het Strafwetboek, of een strafbaar feit dat een hoofdgevangenisstraf van vijf jaar of een zwaardere straf tot gevolg kan hebben, kan de onderzoeksrechter in zijn bevelschrift de gegevens vorderen voor een periode van negen maanden voorafgaand aan het bevelschrift;

- voor andere strafbare feiten kan de onderzoeksrechter de gegevens slechts vorderen voor een periode van zes maanden voorafgaand aan het bevelschrift. ’;

2° in de plaats van paragraaf 3, ingevoegd bij artikel 9 van de wet van [29] mei 2016, zelf vernietigd bij arrest nr. 57/2021 van het Grondwettelijk Hof, wordt de als volgt luidende paragraaf 3 ingevoegd :

‘ § 3. De maatregel kan alleen betrekking hebben op de elektronische communicatiemiddelen van een advocaat of een arts, indien deze er zelf van verdacht worden een strafbaar feit bedoeld in paragraaf 1 te hebben gepleegd of eraan deelgenomen te hebben, of, indien precieze feiten doen vermoeden dat derden die ervan verdacht worden een strafbaar feit bedoeld in paragraaf 1 te hebben gepleegd, gebruik maken van diens elektronische communicatiemiddelen.

De maatregel mag niet ten uitvoer worden gelegd zonder dat, naar gelang het geval, de stafhouder of de vertegenwoordiger van de provinciale orde van geneesheren ervan op de hoogte werd gebracht. Dezelfde personen zullen door de onderzoeksrechter in kennis worden gesteld van hetgeen volgens hem onder het beroepsgeheim valt. Deze gegevens worden niet opgenomen in het proces-verbaal. Deze personen zijn tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek. ’ ».

B.105.1. De verzoekende partij in de zaak nr. 7930 leidt een vijfde middel af uit de schending van de artikelen 11, 12, 22 en 29 van de Grondwet, al dan niet in samenhang gelezen met artikel 15, lid 1, en de artikelen 5, 6 en 9 van de richtlijn 2002/58/EG, met de artikelen 6, 8, 10, 11 en 18 van het Europees Verdrag voor de rechten van de mens en met de artikelen 13 en 54 van de richtlijn (EU) 2016/680. Zij voert aan dat artikel 88*bis*, § 3, van het Wetboek van strafvordering, zoals gewijzigd bij de wet van 20 juli 2022, voorziet in een specifieke maatregel met betrekking tot de toegang tot de gegevens van advocaten en van artsen die het niet mogelijk maakt om de ongrondwettigheid van de algemene bewaring van gegevens als dusdanig te verhelpen, en dat die maatregel enkel betrekking heeft op de onderzoeksrechter en niet op de andere overheden die ook om toegang tot de gegevens van advocaten, artsen en journalisten kunnen verzoeken.

B.105.2. De verzoekende partij in de zaak nr. 7931 leidt een enig middel af uit de schending van de artikelen 11, 12, 22 en 29 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 7, 8, 11, 47 en 52, lid 1, van het Handvest, met artikel 8 van het Europees Verdrag voor de rechten van de mens, met de artikelen 5, 6 en 15 van de richtlijn 2002/58/EG en met de artikelen 13 en 54 van de richtlijn (EU) 2016/680. Zij voert aan dat artikel 88*bis*, § 2, van het Wetboek van strafvordering, zoals gewijzigd bij de wet van 20 juli 2022, een toegang tot de gegevens toestaat bij ernstige aanwijzingen dat een strafbaar feit werd gepleegd dat een correctionele hoofdgevangenisstraf van één jaar of een zwaardere straf tot gevolg kan hebben, hetgeen in werkelijkheid betrekking heeft op de overgrote meerderheid van de strafbare feiten en zich niet beperkt tot het geval van zware criminaliteit. In ondergeschikte orde vraagt de verzoekende partij om over dat punt een prejudiciële vraag te stellen aan het Hof van Justitie. Bovendien klaagt de verzoekende partij ook het feit aan dat de persoon tot wiens gegevens men zich toegang verschaft, niet wordt geïnformeerd, alsook de ontstentenis van rechtsmiddelen bij een illegale toegang tot de gegevens. Wat het voormelde gebrek aan informatie betreft, verzoekt zij in ondergeschikte orde om een prejudiciële vraag te stellen aan het Hof van Justitie.

B.106.1. De grieven van de verzoekende partijen die tegen artikel 88*bis* van het Wetboek van strafvordering zijn gericht, zijn enkel afgeleid uit de schending van het recht op eerbiediging van het privéleven en van het recht op de bescherming van persoonsgegevens, gewaarborgd door artikel 22 van de Grondwet, door artikel 8 van het Europees Verdrag voor

de rechten van de mens, door de artikelen 7, 8 en 52, lid 1, van het Handvest, door de richtlijn 2002/58/EG en door de richtlijn (EU) 2016/680.

B.106.2. Het Hof onderzoekt eerst de grieven die zijn gericht tegen paragraaf 2 van artikel 88*bis* van het Wetboek van strafvordering, en vervolgens die met betrekking tot paragraaf 3 van die bepaling.

B.107.1. Artikel 88*bis*, § 2, van het Wetboek van strafvordering heeft betrekking op de toegang, door de onderzoeksrechter, tot de gegevens die worden bewaard krachtens de artikelen 126/1 en 126/3 van de wet van 13 juni 2005, namelijk de verkeers- en locatiegegevens (zie *Parl. St.,* Kamer, 2021-2022, DOC 55-2572/001, p. 145).

B.107.2. Wat de doeleinden betreft, verleent artikel 88*bis*, § 2, van het Wetboek van strafvordering, zoals gewijzigd bij artikel 27 van de wet van 20 juli 2022, de onderzoeksrechter toegang tot de bewaarde gegevens wanneer er ernstige aanwijzingen zijn dat er een strafbaar feit werd gepleegd dat een correctionele hoofdgevangenisstraf van één jaar of een zwaardere straf tot gevolg kan hebben.

Zoals in B.102.1 is vermeld, toont de verzoekende partij niet aan in welk opzicht de wetgever zijn beoordelingsmarge te buiten zou zijn gegaan door, in artikel 88*bis*, § 2, van het Wetboek van strafvordering, het begrip « zware criminaliteit » te omschrijven onder verwijzing naar strafbare feiten die « een correctionele hoofdgevangenisstraf van één jaar of een zwaardere straf tot gevolg kunnen hebben ». Die omschrijving druist niet in tegen de in B.105.2 aangehaalde referentienormen. Overigens moet de kwalificatie van een strafbaar feit als ernstig misdrijf concreet worden beoordeeld, onder toezicht van de strafrechter, in het licht van de aard van het gepleegde feit en van het geheel van feiten van de zaak.

B.107.3. De verzoekende partijen klagen eveneens het feit aan dat de persoon tot wiens gegevens men zich toegang verschaft, niet wordt geïnformeerd en de ontstentenis van de rechtsmiddelen bij een illegale toegang tot de gegevens.

Hoewel artikel 88*bis,* § 2, van het Wetboek van strafvordering niet voorziet in een specifiek rechterlijk toezicht op de toegang van de onderzoeksrechter tot de krachtens de artikelen 126/1 en 126/3 bewaarde gegevens, zij opgemerkt dat de onderzoeksrechter een onafhankelijke en

onpartijdige magistraat is wiens optreden een essentiële waarborg is voor de inachtneming van de voorwaarden waaraan een aantasting van het recht op eerbiediging van het privéleven is onderworpen. Ook al hebben de beslissingen die hij neemt geen gezag van gewijsde, toch vloeien zij voort uit de uitoefening van de rechtsprekende functie en passen zij in het kader van een gerechtelijke procedure.

Overigens volstaan de gemeenrechtelijke rechtsmiddelen tegen een beschikking van de onderzoeksrechter ter zake. Er dient met name te worden opgemerkt dat, in het kader van de strafprocedure, de beklaagde in dat verband over het recht beschikt om voor de onderzoeksgerechten of voor de vonnisrechter de nietigheid van een onderzoekshandeling aan te voeren die zijn recht op eerbiediging van het privéleven of zijn recht op een eerlijk proces schendt. De betrokkene kan trouwens krachtens artikel 58 van de wet van 3 december 2017 « tot oprichting van de Gegevensbeschermingsautoriteit » kosteloos een klacht indienen bij de Gegevensbeschermingsautoriteit in geval van een onrechtmatige verwerking van zijn persoonsgegevens.

Met betrekking tot het informeren van de betrokken persoon gebeurt zulks overeenkomstig de regels van het Wetboek van strafvordering die van toepassing zijn op het onderzoek.

B.107.4. Het enige middel in de zaak nr. 7931 is niet gegrond in zoverre het betrekking heeft op artikel 88*bis,* § 2, van het Wetboek van strafvordering.

B.108.1. Wat artikel 88*bis*, § 3, van het Wetboek van strafvordering betreft, hebben de grieven van de verzoekende partij in de zaak nr. 7930 in werkelijkheid geen betrekking op die bepaling. « De maatregel tot algemene bewaring van de gegevens als dusdanig », die de verzoekende partij beoogt, wordt immers niet geregeld bij artikel 88*bis*, § 3, en bovendien kan de omstandigheid dat het in die bepaling bedoelde systeem niet wordt uitgebreid tot de « andere overheden » die om toegang tot de gegevens van advocaten, artsen en journalisten kunnen verzoeken, niet worden toegeschreven aan artikel 88*bis*, aangezien dat artikel enkel de bevoegdheden afbakent van de onderzoeksrechter en, in geval van ontdekking op heterdaad, van de procureur des Konings (paragraaf 1, eerste lid).

B.108.2. Het vijfde middel in de zaak nr. 7930 is niet gegrond in zoverre het is afgeleid uit de schending van artikel 20, 2°, van de wet van 20 juli 2022.

12. De bevoegdheden van de inlichtingen- en veiligheidsdiensten (artikelen 33, 34 en 37)

B.109.1. Het eerste middel in de zaak nr. 7932 heeft onder meer betrekking op de artikelen 33, 34 en 37 van de wet van 20 juli 2022.

B.109.2. Artikel 33 van de wet van 20 juli 2022 wijzigt de wet van 30 november 1998, door een artikel 13/6 erin in te voegen, dat bepaalt :

« § 1. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, de medewerking vorderen van een operator van een elektronisch communicatienetwerk of een verstrekker van een elektronische communicatiedienst om over te gaan tot :

1° de bewaring van de verkeers- en lokalisatiegegevens van elektronische communicatiemiddelen waarover hij beschikt op het tijdstip van de vordering;

2° de bewaring van de verkeers- en lokalisatiegegevens die hij op basis van de vordering genereert en verwerkt.

De in het eerste lid bedoelde vordering is gebaseerd op een schriftelijke en met redenen omklede beslissing van het diensthoofd of zijn gedelegeerde.

§ 2. De in paragraaf 1, eerste lid, bedoelde vordering vermeldt :

1° de aard van de verkeers- en lokalisatiegegevens die moeten worden bewaard;

2° de personen, groeperingen, geografische gebieden, communicatiemiddelen en/of gebruikswijze waarvan de verkeers- en lokalisatiegegevens moeten bewaard worden;

3° voor de maatregel bedoeld in paragraaf 1, eerste lid, 1°, de bewaartermijn van de gegevens, die niet langer mag zijn dan zes maanden, te rekenen vanaf de datum van de vordering, onverminderd de mogelijkheid tot verlenging volgens dezelfde procedure;

4° voor de maatregel bedoeld in paragraaf 1, eerste lid, 2° :

- de duur van de maatregel, die niet langer mag zijn dan zes maanden, te rekenen vanaf de datum van de vordering, onverminderd de mogelijkheid tot verlenging volgens dezelfde procedure;

- de bewaartermijn van gegevens, die niet langer mag zijn dan zes maanden, te rekenen vanaf de datum van de communicatie, onverminderd de mogelijkheid tot verlenging volgens dezelfde procedure;

5° de datum van de vordering;

6° de handtekening van het diensthoofd of van zijn gedelegeerde.

§ 3. In geval van hoogdringendheid kan het diensthoofd of zijn gedelegeerde de bewaring mondeling vorderen. Deze mondelinge vordering wordt schriftelijk bevestigd uiterlijk op de eerstvolgende werkdag.

§ 4. De inlichtingen- en veiligheidsdiensten houden een register bij van alle vorderingen tot bewaring.

Elke beslissing tot vordering en de motivering ervan worden ter kennis gebracht van het Vast Comité I. Indien het Vast Comité I een onwettigheid vaststelt, maakt het een einde aan de vordering.

Indien de vordering voortijdig wordt beëindigd, wordt de gevorderde operator van een elektronisch communicatienetwerk of de verstrekker van een elektronische communicatiedienst daarvan zo spoedig mogelijk op de hoogte gebracht.

§ 5. Voor de uitvoering van de vordering kan het diensthoofd of zijn gedelegeerde de medewerking vorderen van het Instituut bedoeld in artikel 2, 1°, van de wet van 13 juni 2005 betreffende de elektronische communicatie, alsook van de personen waarvan hij veronderstelt dat zij over een nuttige technische deskundigheid beschikken. Deze vordering gebeurt schriftelijk en vermeldt de wettelijke grondslag.

§ 6. Eenieder die weigert zijn medewerking te verlenen aan de in de paragrafen 1 en 5 bedoelde vorderingen, wordt gestraft met een geldboete van zesentwintig euro tot twintigduizend euro.

§ 7. De Koning kan, op voorstel van de minister van Justitie, de minister van Landsverdediging en de minister bevoegd voor de Elektronische Communicatie, de nadere regels bepalen voor de samenwerking van de operatoren van een elektronisch communicatienetwerk of de verstrekkers van een elektronische communicatiedienst ».

Artikel 34 van de wet van 20 juli 2022 wijzigt de wet van 30 november 1998 door een artikel 13/7 erin in te voegen, dat bepaalt :

« § 1. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten en in geval van een reële en actuele of voorzienbare ernstige dreiging tegen de nationale veiligheid, de medewerking vorderen van de operatoren van een elektronisch communicatienetwerk en de verstrekkers van een elektronische communicatiedienst om over te gaan tot de algemene en ongedifferentieerde bewaring van de door hen gegenereerde en verwerkte verkeers- en lokalisatiegegevens van elektronische communicatiemiddelen.

§ 2. De in paragraaf 1 bedoelde vordering kan enkel ingesteld worden mits een voorafgaand schriftelijk akkoord van de commissie. De commissie geeft haar akkoord binnen vier dagen na ontvangst van de schriftelijke en gemotiveerde vraag van het diensthoofd.

§ 3. De vraag van het diensthoofd om een vordering tot bewaring in te stellen vermeldt, op straffe van onwettigheid :

1° de ernstige dreiging tegen de nationale veiligheid die reëel en actueel of voorzienbaar is;

2° de feitelijke omstandigheden die de ongedifferentieerde en algemene bewaring van de verkeers- en lokalisatiegegevens rechtvaardigen;

3° de aard van de verkeers- en lokalisatiegegevens die moeten worden bewaard;

4° de duur van de bewaringsmaatregel, die niet langer mag zijn dan zes maanden, te rekenen vanaf de datum van de vordering. Hij kan volgens dezelfde procedure worden verlengd;

5° de bewaartermijn van de gegevens, die niet langer mag zijn dan zes maanden, te rekenen vanaf de datum van de communicatie. Hij kan volgens dezelfde procedure worden verlengd;

6° in voorkomend geval, de redenen die de in paragraaf 5 bedoelde hoogdringendheid rechtvaardigen;

7° de datum van de vraag;

8° de handtekening van het diensthoofd.

§ 4. De in paragraaf 1 bedoelde vordering vermeldt :

1° de datum van het akkoord van de commissie;

2° de aard van de verkeers- en lokalisatiegegevens die moeten worden bewaard;

3° de duur van de maatregel en de bewaartermijn van de gegevens;

4° de datum van de vordering;

5° de handtekening van het diensthoofd of zijn gedelegeerde.

§ 5. In geval van hoogdringendheid vraagt het diensthoofd vooraf om het mondelinge akkoord van de voorzitter van de commissie of, indien deze niet beschikbaar is, een ander lid van de commissie. De auteur van het akkoord informeert onmiddellijk de andere commissieleden. Het diensthoofd bevestigt zijn vraag schriftelijk binnen vierentwintig uur volgend op het akkoord. De voorzitter of het gecontacteerde lid bevestigt eveneens zo spoedig mogelijk schriftelijk zijn akkoord. Dit akkoord is gedurende vijf dagen geldig.

§ 6. De vordering tot een algemene en ongedifferentieerde bewaring wordt bevestigd bij koninklijk besluit.

Het koninklijk besluit vermeldt enkel :

1° de datum van het akkoord van de commissie;

2° de datum van de vordering;

3° de aard van de verkeers- en lokalisatiegegevens die moeten worden bewaard;

4° de duur van de maatregel en de bewaartermijn van de gegevens.

Bij gebrek aan bevestiging bij koninklijk besluit binnen een maand na de vordering, eindigt deze vordering.

De gevorderde operatoren van een elektronisch communicatienetwerk en verstrekkers van een elektronische communicatiedienst worden hiervan zo spoedig mogelijk op de hoogte gebracht.

§ 7. Voor de uitvoering van de vordering kan het diensthoofd de medewerking vorderen van het Instituut bedoeld in artikel 2, 1°, van de wet van 13 juni 2005 betreffende de elektronische communicatie, alsook van de personen waarvan hij veronderstelt dat zij over een nuttige technische deskundigheid beschikken. Deze vordering gebeurt schriftelijk en vermeldt de wettelijke grondslag en het akkoord van de commissie.

§ 8. Eenieder die weigert zijn medewerking te verlenen aan de in de paragrafen 1 en 7 bedoelde vorderingen wordt gestraft met een geldboete van zesentwintig euro tot twintigduizend euro.

§ 9. De commissie geeft onverwijld de vraag van het diensthoofd en haar akkoord door aan het Vast Comité I.

§ 10. De inlichtingen- en veiligheidsdienst brengt om de twee weken verslag uit aan de commissie over de evolutie van de dreiging. Dit verslag belicht de elementen die ofwel de handhaving van de algemene en ongedifferentieerde bewaring, ofwel de beëindiging ervan, rechtvaardigen.

§ 11. Het diensthoofd beëindigt de vordering, niettegenstaande de bevestiging bij koninklijk besluit, wanneer de bewaring niet langer van nut is voor de bestrijding van de reële en actuele of voorzienbare ernstige dreiging tegen de nationale veiligheid, wanneer deze dreiging is verdwenen of wanneer hij een onwettigheid vaststelt.

Wanneer de commissie of het Vast Comité I een onwettigheid vaststelt, wordt een einde gemaakt aan de vordering niettegenstaande de bevestiging bij koninklijk besluit.

Indien de vordering voortijdig wordt beëindigd, worden de gevorderde operatoren van een elektronisch communicatienetwerk of de verstrekkers van een elektronische communicatiedienst daarvan zo spoedig mogelijk op de hoogte gebracht.

§ 12. De Koning bepaalt, op voorstel van de minister van Justitie, de minister van Landsverdediging en de minister bevoegd voor de Elektronische Communicatie, de nadere regels voor de samenwerking van de operatoren van een elektronisch communicatienetwerk of de verstrekkers van een elektronische communicatiedienst ».

Artikel 37 van de wet van 20 juli 2022 vervangt artikel 18/8 van de wet van 30 november 1998, dat voortaan bepaalt :

« § 1. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, zo nodig door daartoe de medewerking van de operator van een elektronisch communicatienetwerk of van de verstrekker van een elektronische communicatiedienst te vorderen, overgaan of doen overgaan tot :

1° het opsporen van de verkeersgegevens van elektronische communicatiemiddelen van waaruit of waarnaar elektronische communicaties worden of werden gedaan;

2° het lokaliseren van de oorsprong of de bestemming van elektronische communicaties.

In de gevallen bedoeld in het eerste lid worden voor elk elektronisch communicatiemiddel waarvan de verkeersgegevens worden opgespoord of waarvan de oorsprong of de bestemming van de elektronische communicatie wordt gelokaliseerd de dag, het tijdstip en de duur en indien nodig de plaats van de elektronische communicatie aangegeven en vastgelegd in een verslag.

De aard van de beslissing wordt meegedeeld aan de gevorderde operator van het elektronisch communicatienetwerk of aan de verstrekker van de elektronische communicatiedienst die wordt gevorderd.

§ 2. [...]

§ 3. Iedere operator van een elektronisch communicatienetwerk en iedere verstrekker van een elektronische communicatiedienst die verzocht wordt de in paragraaf 1 bedoelde gegevens mee te delen, verstrekt het diensthoofd de gevraagde gegevens binnen een termijn en overeenkomstig de nadere regels te bepalen bij koninklijk besluit genomen op voorstel van de minister van Justitie, de minister van Landsverdediging en de minister bevoegd voor de Elektronische Communicatie.

Elke in het eerste lid bedoelde persoon die weigert zijn technische medewerking te verlenen aan de vorderingen bedoeld in dit artikel wordt gestraft met geldboete van zesentwintig euro tot twintigduizend euro.

§ 4. [...] ».

B.109.3. Het eerste middel in de zaak nr. 7932 is afgeleid uit de schending van de artikelen 10, 11, 13, 15, 22, 23 en 29 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 5, 6, 8, 9, 10, 11, 14 en 18 van het Europees Verdrag voor de rechten van de mens, met de artikelen 7, 8, 11, 47 en 52 van het Handvest, met artikel 5, lid 4, van het Verdrag betreffende de Europese Unie, met artikel 6 van de richtlijn 2002/58/EG, met de richtlijn (EU) 2016/680 en met de AVG.

In een vierde onderdeel voeren de verzoekende partijen aan dat artikel 13/6 van de wet van 30 november 1998 het door artikel 22 van de Grondwet gewaarborgde beginsel van voorzienbaarheid schendt, in zoverre het de verkeers- en locatiegegevens die erin worden beoogd, niet nauwkeurig beschrijft. Bovendien beweren zij dat artikel 13/6 niet in overeenstemming is met de rechtspraak van het Hof van Justitie in zoverre het, enerzijds, voorziet in een verplichting tot bewaring die verder reikt dan wat strikt noodzakelijk is en die in werkelijkheid neerkomt op een verplichting tot algemene en ongedifferentieerde bewaring van gegevens en, anderzijds, noch een rechtsmiddel, noch de kennisgeving van de bewaring van gegevens, noch het optreden van een rechter invoert, noch vaststelt dat de verzamelde gegevens worden gewist wanneer de vordering voortijdig wordt beëindigd door het Vast Comité I wegens een onwettigheid.

In een vijfde onderdeel voeren de verzoekende partijen aan dat artikel 13/7 van de wet van 30 november 1998 het criterium van voorzienbaarheid dat voortvloeit uit artikel 22 van de Grondwet en uit de rechtspraak van het Hof van Justitie, niet in acht neemt in zoverre het begrip « verkeers- en lokalisatiegegevens » dat erin wordt beoogd, daarin niet wordt omschreven. Bovendien beweren zij dat niet wordt voorzien in enige kennisgeving aan de betrokken personen, hetgeen de mogelijkheid in de weg staat om de inmenging in het recht op eerbiediging van het privéleven te betwisten. Ten slotte voeren zij aan dat artikel 13/7 niet erin voorziet dat de bewaarde gegevens worden gewist in geval van onwettigheid van de maatregel, in tegenstelling tot hetgeen het Hof van Justitie vereist.

In een zesde onderdeel voeren de verzoekende partijen aan dat artikel 18/8 van de wet van 30 november 1998 het begrip « verkeers- en lokalisatiegegevens » dat erin wordt beoogd, niet omschrijft, noch de duur van de bewaringsmaatregel, hetgeen het beginsel van voorzienbaarheid schendt dat wordt gewaarborgd door artikel 22 van de Grondwet en door de rechtspraak van het Hof van Justitie. Bovendien voeren de verzoekende partijen aan dat artikel 18/8 niet in enige toetsing met betrekking tot de noodzakelijkheid van de maatregel voorziet, in tegenstelling tot hetgeen het Hof van Justitie vereist.

B.109.4. Gelet op de onderlinge samenhang ervan, worden die onderdelen samen onderzocht.

B.110. Uit hetgeen in B.109.2 is vermeld, blijkt dat de grieven van de verzoekende partijen die tegen de artikelen 13/6, 13/7 en 18/8 van de wet van 30 november 1998 zijn gericht, in essentie betrekking hebben op de bestaanbaarheid van die bepalingen met het recht op eerbiediging van het privéleven en met het recht op de bescherming van persoonsgegevens.

B.111.1. Krachtens artikel 1, lid 3, van de richtlijn 2002/58/EG is die richtlijn « niet van toepassing op activiteiten die niet onder het EG-Verdrag vallen, zoals die bedoeld in de titels V en VI van het Verdrag betreffende de Europese Unie, en in geen geval op activiteiten die verband houden met de openbare veiligheid, defensie, staatsveiligheid (met inbegrip van het economische welzijn van de staat wanneer de activiteit verband houdt met de staatsveiligheid) en de activiteiten van de staat op strafrechtelijk gebied ».

Krachtens artikel 2, lid 2, *a)*, van de AVG is die verordening « niet van toepassing op de verwerking van persoonsgegevens in het kader van activiteiten die buiten de werkingssfeer van het Unierecht vallen ». Krachtens artikel 2, lid 2, *d)*, van de AVG is zij evenmin van toepassing op de verwerking van persoonsgegevens door de bevoegde autoriteiten met het oog op de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.

Krachtens artikel 2, lid 3, *a)*, van de richtlijn (EU) 2016/680 is die richtlijn niet van toepassing op de verwerking van persoonsgegevens « in het kader van activiteiten die buiten de werkingssfeer van het Unierecht vallen ».

Bij zijn voormelde arrest van 6 oktober 2020 heeft het Hof van Justitie geoordeeld :

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

B.111.2. Krachtens de artikelen 13/6, 13/7 en 18/8 van de wet van 30 november 1998 kunnen de inlichtingen- en veiligheidsdiensten, in het belang van de uitoefening van hun

opdrachten, de medewerking vorderen van een operator van elektronische-communicatienetwerken of van een verstrekker van elektronische-communicatiediensten om over te gaan tot het bewaren en meedelen van verkeers- en locatiegegevens.

B.111.3. Aangezien de artikelen 13/6, 13/7 en 18/8 van de wet van 30 november 1998 slechts van toepassing zijn in het kader van de opdrachten van de inlichtingen- en veiligheidsdiensten, vallen zij buiten het toepassingsgebied van het recht van de Europese Unie. Bijgevolg is het middel onontvankelijk in zoverre het is afgeleid uit de schending van de aangevoerde bepalingen van het Verdrag betreffende de Europese Unie, van het Handvest, van de AVG, van de richtlijn (EU) 2016/680 of van de richtlijn 2002/58/EG, zoals geïnterpreteerd door de rechtspraak van het Hof van Justitie.

B.112.1. De andere grieven van de verzoekende partijen met betrekking tot de artikelen 13/6, 13/7 en 18/8 van de wet van 30 november 1998 zijn afgeleid uit de schending van artikel 22 van de Grondwet.

B.112.2. Zoals in B.11.3 is vermeld, heeft de Grondwetgever gestreefd naar een zo groot mogelijke concordantie tussen artikel 22 van de Grondwet en artikel 8 van het Europees Verdrag voor de rechten van de mens (*Parl. St.*, Kamer, 1992-1993, nr. 997/5, p. 2).

De draagwijdte van dat artikel 8 is analoog aan die van de voormelde grondwetsbepaling, zodat de waarborgen die beide bepalingen bieden, een onlosmakelijk geheel vormen.

B.112.3. Bovendien, zoals in B.24.1 en B.24.2 in herinnering is gebracht, wordt bij artikel 22 van de Grondwet aan de bevoegde wetgever de bevoegdheid voorbehouden om te bepalen in welke gevallen en onder welke voorwaarden afbreuk kan worden gedaan aan het recht op eerbiediging van het privéleven. Het waarborgt aldus aan elke burger dat geen inmenging in de uitoefening van dat recht kan plaatsvinden dan krachtens regels die zijn aangenomen door een democratisch verkozen beraadslagende vergadering. In dat opzicht moeten de essentiële elementen van de verwerking van persoonsgegevens in de wet, het decreet of de ordonnantie zelf worden vastgelegd. In dat verband maken de volgende elementen, ongeacht de aard van de betrokken aangelegenheid, in beginsel essentiële elementen uit : (1°) de categorie van verwerkte gegevens; (2°) de categorie van betrokken personen; (3°) de met de

verwerking nagestreefde doelstelling; (4°) de categorie van personen die toegang hebben tot de verwerkte gegevens; (5°) de maximumtermijn voor het bewaren van de gegevens.

Naast het formele wettigheidsvereiste legt artikel 22 van de Grondwet, in samenhang gelezen met artikel 8 van het Europees Verdrag voor de rechten van de mens, de verplichting op dat de inmenging in de uitoefening van het recht op eerbiediging van het privéleven en van het recht op de bescherming van persoonsgegevens in duidelijke en voldoende nauwkeurige bewoordingen wordt geformuleerd die het mogelijk maken de hypothesen te voorzien waarin de wetgever een dergelijke inmenging toestaat. Inzake gegevensbescherming impliceert dat vereiste van voorzienbaarheid dat voldoende precies moet worden bepaald in welke omstandigheden de verwerkingen van persoonsgegevens zijn toegestaan. Derhalve moet eenieder een voldoende duidelijk beeld kunnen hebben van de verwerkte gegevens, de bij een bepaalde gegevensverwerking betrokken personen en de voorwaarden voor en de doeleinden van de verwerking.

B.113.1. De artikelen 13/6, 13/7 en 18/8 van de wet van 30 november 1998 voorzien erin dat de inlichtingendiensten, in het belang van de uitoefening van hun opdrachten, de medewerking kunnen vorderen van een operator van elektronische-communicatienetwerken of van een verstrekker van elektronische-communicatiediensten om over te gaan tot het bewaren en meedelen van « verkeers- en lokalisatiegegevens ». Zodoende heeft de wetgever het door artikel 22 van de Grondwet gewaarborgde formele wettigheidsbeginsel in acht genomen, aangezien hij de categorieën van verwerkte gegevens heeft gepreciseerd.

B.113.2. Bovendien zetten de artikelen 13/6, 13/7 en 18/8 van de wet van 30 november 1998 in duidelijke en gedetailleerde bewoordingen uiteen welke verkeers- en locatiegegevens de inlichtingendiensten mogen bewaren en verwerken, alsook onder welke voorwaarden en op welke wijze dat moet gebeuren, hetgeen de betrokken personen de mogelijkheid biedt om op voldoende wijze de hypothesen te voorzien waarin de wetgever een inmenging in het recht op eerbiediging van het privéleven en in het recht op de bescherming van persoonsgegevens toestaat.

B.114. De maatregel die is bedoeld in artikel 18/8 van de wet van 30 november 1998, betreft ten slotte de opsporing of lokalisatie van gegevens en niet de bewaring ervan.

In de toelichting bij de artikelen wordt op dat punt immers gepreciseerd :

« Dit artikel 18/8 betreft de toegang tot de gegevens met betrekking tot elektronische communicatie door de inlichtingen- en veiligheidsdiensten en niet de bewaring van deze gegevens. [...]

[...]

Het is [...] aangewezen om te preciseren dat geen enkele wijziging werd aangebracht aan de toegang tot de gegevens met betrekking tot de elektronische communicatie door de inlichtingen- en veiligheidsdiensten, noch aan de modaliteiten ervan.

De enige wijziging betreft de opheffing van paragraaf 2, die logischerwijze werd vernietigd door het Grondwettelijk Hof.

De toegang tot de gegevens door de inlichtingen- en veiligheidsdiensten bedoeld in artikel 18/8, heeft betrekking op alle gegevens bewaard door de operatoren, ongeacht de doelstelling.

[...]

In reactie op een opmerking van het Vast Comité I (punten 16-18) wensen de indieners van het ontwerp erop te wijzen dat er geen reden meer is om de toegang tot de gegevens te moduleren omdat de toegang zal afhangen van de effectieve, gemoduleerde, bewaartermijn. De toegang zal trouwens steeds gemotiveerd moeten worden zodat de Commissie en het vast Comité I de proportionaliteit, subsidiariteit en wettelijkheid van de opgevraagde historiek kunnen controleren. Deze motivatieplicht is trouwens, op vraag van het Comité, terug ingevoerd in artikel 18/3, 2, 12° » (*Parl. St.*, Kamer, 2021-2022, DOC 55-2572/001, pp. 163-164).

Daaruit volgt dat het zesde onderdeel van het eerste middel in de zaak nr. 7932, dat betrekking heeft op de bewaring van gegevens, niet gegrond is.

B.115. Het vierde, vijfde en zesde onderdeel van het eerste middel in de zaak nr. 7932 zijn niet gegrond.

13. De inwerkingtreding (artikel 45)

B.116.1. Het derde middel in de zaak nr. 7930 heeft betrekking op artikel 45 van de wet van 20 juli 2022, dat bepaalt :

« De gerichte gegevensbewaring op basis van de criteria bedoeld in artikel 126/3, §§ 3 tot 5, van de wet van 13 juni 2005 betreffende de elektronische communicatie treedt in werking op de door de Koning bij een besluit vastgesteld na overleg in de Ministerraad bepaalde datum en uiterlijk op 1 januari 2027.

Bij de eerste toepassing van artikel 126/3, §§ 3 tot 5, van de wet van 13 juni 2005 betreffende de elektronische communicatie, maken de in artikel 126/3, § 6, tweede lid, van dezelfde wet bedoelde bevoegde autoriteiten de nodige informatie over aan de [...] door de Koning aangewezen dienst op een datum die vastgesteld wordt bij het in het eerste lid bedoelde koninklijk besluit en uiterlijk op 1 januari 2026 ».

B.116.2. Het derde middel in de zaak nr. 7930 is afgeleid uit de schending van de artikelen 11, 12, 22 en 29 van de Grondwet, van artikel 15, lid 1, en van de artikelen 5, 6 en 9 van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8, 11, 47 en 52, lid 1, van het Handvest, van de artikelen 6, 8, 10, 11 en 18 van het Europees Verdrag voor de rechten van de mens en van de artikelen 13 en 54 van de richtlijn (EU) 2016/680. De verzoekende partij voert aan dat de bij artikel 45 geregelde inwerkingtreding het door artikel 22 van de Grondwet gewaarborgde wettigheidsbeginsel schendt.

B.116.3. Uit de uiteenzetting van het middel blijkt niet in welk opzicht het voormelde wettigheidsbeginsel zou zijn geschonden. Het middel is niet gegrond.

14. De bescherming van het beroepsgeheim

B.117.1. Het enige middel in de zaak nr. 7907, het enige middel in de zaak nr. 7929, het tweede en het vijfde middel in de zaak nr. 7930 en het zevende onderdeel van het eerste middel en het derde onderdeel van het derde middel in de zaak nr. 7932 hebben betrekking op het gebrek aan bescherming van de informatie die wordt gedekt door het beroepsgeheim.

B.117.2.1. Het enige middel in de zaak nr. 7907, dat is afgeleid uit de schending van de artikelen 10 en 11 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 6 en 8 van het Europees Verdrag voor de rechten van de mens en met de artikelen 7, 8 en 47 van het Handvest, heeft betrekking op de artikelen 5, 4° en 6°, 8 tot 11, 13 tot 15, 19, 21, 22, 24 tot 42 en 44 van de wet van 20 juli 2022.

In het bijzonder voert de verzoekende partij aan dat de bestreden bepalingen geen, of minstens onvoldoende, onderscheid maken tussen, enerzijds, de gebruikers die houder zijn van het beroepsgeheim en de andere gebruikers en, anderzijds, de door het beroepsgeheim gedekte gegevens en de andere gegevens. Wat inzonderheid artikel 27 van de wet van 20 juli 2022 betreft, voert de verzoekende partij aan dat die bepaling enkel betrekking heeft op de communicatie die uitgaat van een advocaat of van een arts, maar niet op die welke afkomstig is van de cliënt of de patiënt, hetgeen het niet mogelijk maakt om een adequate specifieke behandeling voor te behouden aan de houders van het beroepsgeheim (eerste en tweede onderdeel). Bovendien voert de verzoekende partij aan dat de bestreden bepalingen een algemeen toezicht op alle burgers in het leven roepen (derde onderdeel) en dat zij niet evenredig zijn met het nagestreefde doel (vierde onderdeel).

B.117.2.2. Het enige middel in de zaak nr. 7929 is afgeleid uit de schending van de artikelen 10 en 11 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 6 en 8 van het Europees Verdrag voor de rechten van de mens en met de artikelen 7, 8, 11 en 47 van het Handvest, en heeft betrekking op de artikelen 2 tot 17 van de wet van 20 juli 2022.

De verzoekende partijen voeren in essentie aan dat de bestreden bepalingen, enerzijds, de gebruikers van telecommunicatie- of elektronische-communicatiediensten die aan het beroepsgeheim zijn onderworpen, met name de boekhoudkundige en fiscale professionals, en, anderzijds, de andere gebruikers van die diensten op identieke wijze behandelen, zonder dat rekening wordt gehouden met het fundamentele karakter van het beroepsgeheim.

B.117.2.3. Het tweede middel in de zaak nr. 7930, dat is afgeleid uit de schending van de artikelen 10, 11, 22 en 29 van de Grondwet, al dan niet in samenhang gelezen met artikel 15, lid 1, 5, 6 en 9 van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8, 11, 47 en 52, lid 1, van het Handvest, met de artikelen 6, 8, 10, 11 en 18 van het Europees Verdrag voor de rechten van de mens en met de artikelen 13 en 54 van de richtlijn (EU) 2016/680, heeft betrekking op de artikelen 5, 6, 8, 9, 10 en 12 van de wet van 20 juli 2022, in zoverre die bepalingen met betrekking tot de bewaring van de gegevens en de toegang ertoe niet in enige uitzondering voorzien voor artsen, advocaten of journalisten.

Het vijfde middel in de zaak nr. 7930, dat is afgeleid uit de schending van de artikelen 10, 11, 22 en 29 van de Grondwet, al dan niet in samenhang gelezen met artikel 15, lid 1, 5, 6 en 9

van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8, 11, 47 en 52, lid 1, van het Handvest, met de artikelen 6, 8, 10, 11 en 18 van het Europees Verdrag voor de rechten van de mens en met de artikelen 13 en 54 van de richtlijn (EU) 2016/680, heeft betrekking op de wet van 20 juli 2022 in haar geheel in zoverre zij niet in enig relevant controlemechanisme voorziet waardoor de begunstigden van het beroepsgeheim zich kunnen verzetten tegen de verzameling, de bewaring of de kennisneming van hun gegevens.

B.117.2.4. Het zevende onderdeel van het eerste middel in de zaak nr. 7932, dat is afgeleid uit de schending van de artikelen 10, 11, 13, 15, 22, 23 en 29 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 5, 6, 8, 9, 10, 11, 14 en 18 van het Europees Verdrag voor de rechten van de mens, met de artikelen 7, 8, 11, 47 en 52 van het Handvest, met artikel 5, lid 4, van het Verdrag betreffende de Europese Unie en met artikel 6 van de richtlijn 2002/58/EG, met de richtlijn (EU) 2016/680 en met de AVG, heeft betrekking op de wet van 20 juli 2022 in zoverre zij niet in enige bijzondere behandeling voorziet voor het bewaren van de verkeers- en locatiegegevens van advocaten, artsen en journalisten, terwijl het gevoelige gegevens betreft die onder het beroepsgeheim vallen.

Het derde onderdeel van het derde middel in die zaak, dat is afgeleid uit de schending van de artikelen 10, 11, 13, 15, 22, 23 en 29 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 5, 6, 8, 9, 10, 11, 14 en 18 van het Europees Verdrag voor de rechten van de mens, met de artikelen 7, 8, 11, 47 en 52 van het Handvest, met artikel 5, lid 4, van het Verdrag betreffende de Europese Unie en met artikel 6 van de richtlijn 2002/58/EG, met de richtlijn (EU) 2016/680 en met de AVG, heeft betrekking op de wet van 20 juli 2022 in zoverre zij niet in een bijzondere bescherming voorziet om zich toegang te verschaffen tot de gegevens van advocaten, artsen en journalisten. De verzoekende partijen voeren bovendien aan dat de voormelde gegevens verschillend worden behandeld naargelang de toegang tot de gegevens al dan niet plaatsvindt op grond van artikel 27 van de wet van 20 juli 2022.

B.117.3. Gelet op de onderlinge samenhang ervan, onderzoekt het Hof de voormelde middelen en onderdelen samen.

B.118. Artikel 88*bis* van het Wetboek van strafvordering, zoals gewijzigd door de bestreden wet, bepaalt :

« § 1. Wanneer er ernstige aanwijzingen zijn dat de strafbare feiten een correctionele hoofdgevangenisstraf van één jaar of een zwaardere straf tot gevolg kunnen hebben en de onderzoeksrechter van oordeel is dat er omstandigheden zijn die het doen opsporen van elektronische communicatie of het lokaliseren van de oorsprong of de bestemming van elektronische communicatie noodzakelijk maken om de waarheid aan de dag te brengen, kan hij :

1° de verkeersgegevens doen opsporen van elektronische communicatiemiddelen van waaruit of waarnaar elektronische communicaties worden of werden gedaan;

2° de oorsprong of de bestemming van elektronische communicatie laten lokaliseren.

Hiertoe kan hij zo nodig, rechtstreeks of via de door de Koning aangewezen politiedienst, de medewerking vorderen van :

- de operator van een elektronisch communicatienetwerk; en

- iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst beschikbaar stelt of aanbiedt, die bestaat in het overbrengen van signalen via elektronische communicatienetwerken, of er in bestaat gebruikers toe te laten via een elektronisch communicatienetwerk informatie te verkrijgen of te ontvangen of te verspreiden. Hieronder wordt ook de verstrekker van een elektronische communicatiedienst begrepen.

In de gevallen bedoeld in het eerste lid wordt voor ieder elektronisch communicatiemiddel waarvan de verkeersgegevens worden opgespoord of waarvan de oorsprong of de bestemming van de elektronische communicatie wordt gelokaliseerd, de dag, het uur, de duur, en, indien nodig, de plaats van de elektronische communicatie vastgesteld en opgenomen in een proces-verbaal.

De onderzoeksrechter doet in een met redenen omkleed bevelschrift opgave van de feitelijke omstandigheden van de zaak die de maatregel rechtvaardigen, van de proportionaliteit met inachtneming van de persoonlijke levenssfeer en de subsidiariteit ten opzichte van elke andere onderzoeksdaad.

Hij vermeldt ook de duur van de maatregel voor de toekomst, die niet langer kan zijn dan twee maanden te rekenen vanaf het bevelschrift, onverminderd een hernieuwing en, in voorkomend geval, de periode in het verleden waarover de vordering zich uitstrekt overeenkomstig paragraaf 2.

In geval van ontdekking op heterdaad kan de procureur des Konings de maatregel bevelen voor de in artikel 90*ter*, §§ 2, 3 en 4, bedoelde strafbare feiten. In dat geval moet de maatregel binnen vierentwintig uur worden bevestigd door de onderzoeksrechter.

Indien het echter het in artikel 137, 347*bis*, 434 of 470 van het Strafwetboek bedoelde strafbare feit betreft, met uitzondering van het in artikel 137, § 3, 6°, van hetzelfde Wetboek bedoelde strafbare feit, kan de procureur des Konings de maatregel bevelen zolang de heterdaadsituatie duurt, zonder dat een bevestiging door de onderzoeksrechter nodig is.

Indien het het in artikel 137 van het Strafwetboek bedoelde strafbare feit betreft, met uitzondering van het in artikel 137, § 3, 6°, van hetzelfde Wetboek bedoelde strafbare feit, kan

de procureur des Konings bovendien de maatregel bevelen binnen de tweeënzeventig uur na de ontdekking van dit strafbare feit, zonder dat een bevestiging door de onderzoeksrechter nodig is.

De procureur des Konings kan evenwel de maatregel bevelen indien de klager erom verzoekt, wanneer deze maatregel onontbeerlijk lijkt voor het vaststellen van een strafbaar feit bedoeld in artikel 145, § 3 en § 3*bis* van de wet van 13 juni 2005 betreffende de elektronische communicatie.

In spoedeisende gevallen kan de maatregel mondeling worden bevolen. Het bevel moet zo spoedig mogelijk worden bevestigd in de vorm bepaald in het vierde en vijfde lid.

§ 2. Wat betreft de toepassing van de maatregel bedoeld in paragraaf 1, eerste lid, op de verkeers- of lokalisatiegegevens die worden bewaard krachtens de artikelen 126/1 en 126/3 van de wet van 13 juni 2005 betreffende de elektronische communicatie, zijn de volgende bepalingen van toepassing :

- voor een strafbaar feit bedoeld in boek II, titel I*ter*, van het Strafwetboek mag de onderzoeksrechter in zijn bevelschrift de gegevens opvragen voor een periode van twaalf maanden voorafgaand aan het bevelschrift;

- voor een ander strafbaar feit bedoeld in artikel 90*ter*, §§ 2 tot 4, dat niet bedoeld is in het eerste gedachtestreepje, of een strafbaar feit dat gepleegd is in het kader van een criminele organisatie als bedoeld in artikel 324*bis* van het Strafwetboek, of een strafbaar feit dat een hoofdgevangenisstraf van vijf jaar of een zwaardere straf tot gevolg kan hebben, kan de onderzoeksrechter in zijn bevelschrift de gegevens vorderen voor een periode van negen maanden voorafgaand aan het bevelschrift;

- voor andere strafbare feiten kan de onderzoeksrechter de gegevens slechts vorderen voor een periode van zes maanden voorafgaand aan het bevelschrift.

§ 3. De maatregel kan alleen betrekking hebben op de elektronische communicatiemiddelen van een advocaat of een arts, indien deze er zelf van verdacht worden een strafbaar feit bedoeld in paragraaf 1 te hebben gepleegd of eraan deelgenomen te hebben, of, indien precieze feiten doen vermoeden dat derden die ervan verdacht worden een strafbaar feit bedoeld in paragraaf 1 te hebben gepleegd, gebruik maken van diens elektronische communicatiemiddelen.

De maatregel mag niet ten uitvoer worden gelegd zonder dat, naar gelang het geval, de stafhouder of de vertegenwoordiger van de provinciale orde van geneesheren ervan op de hoogte werd gebracht. Dezelfde personen zullen door de onderzoeksrechter in kennis worden gesteld van hetgeen volgens hem onder het beroepsgeheim valt. Deze gegevens worden niet opgenomen in het proces-verbaal. Deze personen zijn tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

§ 4. De actoren bedoeld in § 1, tweede lid, delen de gegevens waarom verzocht werd mee in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering, volgens de nadere regels vastgesteld door de Koning, op voorstel van de minister van Justitie en de minister bevoegd voor Telecommunicatie.

Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

Iedere persoon die zijn technische medewerking aan de vorderingen bedoeld in dit artikel weigert of niet verleent in werkelijke tijd of, in voorkomend geval, op het tijdstip bepaald in de vordering, medewerking waarvan de nadere regels vastgesteld worden door de Koning, op voorstel van de minister van Justitie en de minister bevoegd voor Telecommunicatie, wordt gestraft met geldboete van honderd euro tot dertigduizend euro ».

B.119. Buiten het in artikel 88*bis*, § 3, van het Wetboek van strafvordering bedoelde geval voorziet de wet van 20 juli 2022 niet uitdrukkelijk in een bijzondere bescherming voor de gegevens die worden beschermd door het beroepsgeheim.

De bewoordingen zelf van artikel 88*bis*, § 3, van het Wetboek van strafvordering zelf, die zijn vervangen bij artikel 27 van de wet van 20 juli 2022, voorzien in een bijzondere bescherming voor de elektronische-communicatiemiddelen van advocaten en artsen, dus zowel voor de communicatie die afkomstig is van de advocaat en de arts, als voor de communicatie die uitgaat van de cliënten en de patiënten (*Parl. St.*, Kamer, 2021-2022, DOC 55-2572/003, p. 48).

B.120. Het beroepsgeheim waartoe de in artikel 458 van het Strafwetboek bedoelde personen, met name de advocaten en de artsen, zijn gehouden, strekt niet ertoe hun enig voorrecht toe te kennen, maar heeft hoofdzakelijk tot doel het fundamentele recht op eerbiediging van het privéleven te beschermen van diegene die hen in vertrouwen neemt, soms over iets strikt persoonlijks. De vertrouwelijke informatie die wordt toevertrouwd aan een advocaat bij de uitoefening van zijn beroep en wegens die hoedanigheid, geniet bovendien ook, in bepaalde gevallen, de bescherming die voor de rechtzoekende voortvloeit uit de waarborgen die zijn neergelegd in artikel 6 van het Europees Verdrag voor de rechten van de mens, aangezien de aan de advocaat opgelegde regel van het beroepsgeheim een fundamenteel element is van de rechten van de verdediging van de rechtzoekende die hem in vertrouwen neemt.

De effectiviteit van de rechten van de verdediging van iedere rechtzoekende veronderstelt immers noodzakelijkerwijs dat een vertrouwensrelatie tot stand kan komen tussen die persoon en de advocaat die hem raad geeft en hem verdedigt. Die noodzakelijke vertrouwensrelatie kan alleen tot stand komen en behouden blijven indien de rechtzoekende de waarborg heeft dat wat

hij aan zijn advocaat toevertrouwt door die laatstgenoemde niet openbaar zal worden gemaakt. Hieruit volgt dat de aan de advocaat opgelegde regel van het beroepsgeheim een fundamenteel element van de rechten van de verdediging is.

Zoals het Hof van Cassatie erop wijst, « [berust] het beroepsgeheim waaraan de leden van de balie zijn onderworpen, [...] op de noodzaak volledige veiligheid te verzekeren aan degenen die zich aan hen toevertrouwen » (Cass., 13 juli 2010, ECLI:BE:CASS:2010:ARR.20100713.1; zie ook 9 juni 2004, ECLI:BE:CASS:2004:ARR.20040609.10).

Ook al is het « niet onaantastbaar », het beroepsgeheim van de advocaat vormt bijgevolg « een van de grondbeginselen waarop de organisatie van het gerecht in een democratische samenleving berust » (EHRM, 6 december 2012, *Michaud t. Frankrijk*, ECLI:CE:ECHR:2012:1206JUD001232311, § 123).

B.121.1. Tegen die achtergrond dient de wet van 20 juli 2022 op grondwetsconforme wijze te worden geïnterpreteerd rekening houdend met het feit dat het beroepsgeheim van de advocaat een algemeen beginsel is dat verband houdt met de naleving van de fundamentele rechten. Aldus kunnen de regels die daarvan afwijken, slechts strikt worden geïnterpreteerd, rekening houdend met de wijze waarop het beroep van advocaat in de interne rechtsorde is geregeld.

In de parlementaire voorbereiding met betrekking tot die bepaling wordt aangegeven :

« In het 2° van artikel 21 [dat 27 is geworden] wordt de vroegere paragraaf 3, dat de communicatiegegevens van artsen en advocaten beschermt, opnieuw opgenomen. De maatregel kan alleen betrekking hebben op hun elektronische communicatiemiddelen in bepaalde zeer specifieke situaties. Deze paragraaf is een herhaling van de artikelen 39*bis*, § 9, 56*bis*, 88*bis*, § 3 en 90*octies* W. Sv. » (*Parl. St.*, Kamer, 2021-2022, DOC 55-2572/001, p. 145).

Met betrekking tot artikel 39*bis*, § 9, van het Wetboek van strafvordering heeft het Hof bij zijn arrest nr. 66/2021 van 29 april 2021 (ECLI:BE:GHCC:2021:ARR.066) geoordeeld :

« B.11.1. Artikel 39*bis*, § 9, tweede lid, van het Wetboek van strafvordering bepaalt dat de maatregel niet ten uitvoer mag worden gelegd zonder dat, naar gelang van het geval, de stafhouder of de vertegenwoordiger van de provinciale raad van de Orde der artsen ervan op de hoogte werd gebracht, en dat die personen door de procureur des Konings in kennis zullen worden gesteld van wat volgens hem onder het beroepsgeheim valt.

B.11.2. Die bepaling stelt niet de wijze vast waarop het optreden van de vertegenwoordiger van de betrokken orde concreet dient plaats te vinden. In dat verband dient artikel 39*bis*, § 9, van het Wetboek van strafvordering zo te worden geïnterpreteerd dat die bepaling een nuttige uitwerking heeft in het licht van de *ratio legis* ervan, die erin bestaat het beroepsgeheim van de advocaat en van de arts te beschermen. Daaruit volgt dat artikel 39*bis*, § 9, tweede lid, van het Wetboek van strafvordering in die zin dient te worden geïnterpreteerd dat het de procureur des Konings ertoe verplicht de stafhouder of de vertegenwoordiger van de provinciale raad van de Orde der artsen op de hoogte te brengen vóór de uitvoering van de maatregel, zodat die erbij aanwezig kan zijn en in staat wordt gesteld om de documenten, bestanden of elementen die de procureur des Konings wenst in te zien, vooraf te onderzoeken en om hem mee te delen wat volgens hem onder het beroepsgeheim valt. De vertegenwoordiger van de betrokken orde kan daarenboven de adequate maatregelen aanbevelen die het mogelijk maken bepaalde stukken, die door het beroepsgeheim worden gedekt, in te zien zonder dat geheim in gevaar te brengen.

Het staat aan de procureur des Konings zich uit te spreken over het al dan niet vertrouwelijke karakter van de elementen die hij wenst in te zien, na het advies te hebben ingewonnen van, naar gelang van het geval, de stafhouder of de vertegenwoordiger van de provinciale raad van de Orde der artsen. Bij onenigheid kan de vertegenwoordiger van de betrokken orde akte laten nemen van zijn voorbehoud in het proces-verbaal.

B.11.3. Aangezien dat prerogatief van de procureur des Konings samenhangt met zijn bevoegdheid om niet-geheime zoekingen in een informaticasysteem te bevelen, zoals in B.9.3 is vermeld, is het niet zonder redelijke verantwoording dat de procureur des Konings zelf uitspraak doet over het al dan niet vertrouwelijke karakter van de elementen die hij wenst in te zien, op voorwaarde dat de vertegenwoordiger van de betrokken orde advies uitbrengt en onverminderd de toetsing door de kamer van inbeschuldigingstelling en door de vonnisgerechten. De procureur des Konings is immers wettelijk verantwoordelijk voor het goede verloop van het opsporingsonderzoek, dat erin bestaat de misdrijven, hun daders en de bewijzen ervan op te sporen en de gegevens te verzamelen die dienstig zijn voor de uitoefening van de strafvordering (artikel 28*bis*, § 1, eerste en derde lid, van het Wetboek van strafvordering).

B.11.4. Krachtens artikel 39*bis*, § 9, tweede lid, van het Wetboek van strafvordering worden de gegevens die volgens de procureur des Konings onder het beroepsgeheim vallen, niet opgenomen in het proces-verbaal en is de vertegenwoordiger van de betrokken orde tot geheimhouding verplicht.

[...]

B.14. Onder voorbehoud van de in B.11.2 vermelde interpretatie zijn de twee middelen niet gegrond ».

Hetzelfde voorbehoud van interpretatie is van toepassing op het bestreden artikel 88*bis*, § 3, van het Wetboek van strafvordering.

B.121.2. Diezelfde interpretatie dient *mutatis mutandis* op algemene wijze te gelden voor alle gegevens die onder het toepassingsgebied van artikel 458 van het Strafwetboek vallen en bijgevolg voor andere categorieën van beroepsbeoefenaars, volgens de nadere regels en onder de voorwaarden waarin door de wetgever is voorzien. Aldus dient in elk concreet geval waarin een onderzoeksrechter of een andere autoriteit toegang krijgt tot de bewaarde gegevens, de regel van het beroepsgeheim maar te wijken indien zulks kan worden verantwoord door een dwingende reden van algemeen belang en indien het opheffen van het geheim strikt evenredig is ten aanzien van dat doel.

B.122. Rekening houdend met de in B.121 vermelde interpretatie doet de wet van 20 juli 2022 niet op discriminerende wijze afbreuk aan het beroepsgeheim.

B.123. Het enige middel in de zaak nr. 7907, het enige middel in de zaak nr. 7929, het tweede en het vijfde middel in de zaak nr. 7930 en het zevende onderdeel van het eerste middel in de zaak nr. 7932 en het derde onderdeel van het derde middel in de zaak nr. 7932 zijn niet gegrond.

Om die redenen,

het Hof

- alvorens uitspraak te doen over de grieven met betrekking tot de artikelen 5, 6 en 24 van de wet van 20 juli 2022 « betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten », stelt aan het Hof van Justitie van de Europese Unie de volgende prejudiciële vragen :

1. Dient artikel 15, lid 1, van de richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 « betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) », in samenhang gelezen met de artikelen 7, 8 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, in die zin te worden geïnterpreteerd :

a) dat het zich verzet tegen een nationale wetgeving die voorziet in een verplichting voor de operatoren van elektronische-communicatiediensten om in het kader van de verstrekking van dat netwerk of van die dienst, de in die wetgeving bepaalde verkeersgegevens te bewaren en te verwerken gedurende een periode van, naargelang van het geval, vier of twaalf maanden, teneinde de gepaste evenredige, preventieve en curatieve maatregelen te kunnen nemen om fraude en kwaadwillig gebruik op hun netwerken te voorkomen en te verhinderen dat de eindgebruikers schade lijden of lastiggevallen worden, en om fraude of kwaadwillig gebruik van het netwerk of de dienst vast te stellen of om de dader en de herkomst ervan te kunnen identificeren;

b) dat het zich verzet tegen een nationale wetgeving die die operatoren toestaat om de betrokken verkeersgegevens langer dan de voormelde termijnen te bewaren en te verwerken, in geval van een specifieke geïdentificeerde fraude of een specifiek geïdentificeerd kwaadwillig gebruik van het netwerk gedurende de periode die nodig is voor de analyse en het verhelpen ervan of gedurende de periode die nodig is voor de verwerking van dat kwaadwillig gebruik;

c) dat het zich verzet tegen een nationale wetgeving die die operatoren toestaat, zonder te voorzien in de verplichting een voorafgaand advies te vragen of een melding te doen aan een onafhankelijke autoriteit, andere gegevens dan die welke in de wet zijn bepaald te bewaren en te verwerken om fraude of kwaadwillig gebruik van het netwerk of de dienst te kunnen vaststellen of om de dader en de herkomst ervan te kunnen identificeren;

d) dat het zich verzet tegen een nationale wetgeving die de operatoren toestaat, zonder te voorzien in de verplichting een voorafgaand advies te vragen of een melding te doen aan een onafhankelijke autoriteit, de verkeersgegevens voor een duur van twaalf maanden te bewaren en te verwerken die zij noodzakelijk achten om de veiligheid en de correcte werking van hun elektronische-communicatienetwerken en -diensten te garanderen, en in het bijzonder om een mogelijke of werkelijke schending van die veiligheid op te sporen en te analyseren, inclusief om de oorsprong van die schending te identificeren en, in geval van een specifieke schending van de veiligheid van het netwerk, gedurende de periode die nodig is om deze te behandelen;

2. Dient artikel 15, lid 1, van de richtlijn 2002/58/EG, in samenhang gelezen met de artikelen 7, 8 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, in die zin te worden geïnterpreteerd :

a) dat het zich verzet tegen een nationale wetgeving die de operatoren van mobiele netwerken toestaat om locatiegegevens te bewaren en te verwerken, zonder dat de wetgeving precies omschrijft welke gegevens zijn bedoeld, in het kader van de verstrekking van dat netwerk of die dienst, gedurende een periode van, naargelang van het geval, vier of twaalf maanden, wanneer dat noodzakelijk is voor de goede werking en de veiligheid van het netwerk of de dienst, of om fraude of kwaadwillig gebruik van het netwerk op te sporen of te analyseren;

b) dat het zich verzet tegen een nationale wetgeving die aan die operatoren de mogelijkheid biedt om de locatiegegevens langer dan de voormelde termijnen te bewaren en te verwerken in geval van een specifieke schending, specifieke fraude of specifiek kwaadwillig gebruik;

3. Zou het Grondwettelijk Hof, indien het op grond van de antwoorden verstrekt op de eerste of de tweede prejudiciële vraag tot de conclusie zou komen dat sommige bepalingen van de wet van 20 juli 2022 « betreffende het verzamelen en het bewaren van de

identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten », een of meer van de verplichtingen schenden die uit de in die vragen vermelde bepalingen voortvloeien, de gevolgen van de voormelde bepalingen van de wet van 20 juli 2022 tijdelijk kunnen handhaven teneinde rechtsonzekerheid te voorkomen en het mogelijk te maken dat de voorheen verzamelde en bewaarde gegevens alsnog kunnen worden gebruikt voor de door de wet beoogde doeleinden ?

- onder voorbehoud van de in B.121 vermelde interpretatie, verwerpt de overige grieven.

Aldus gewezen in het Frans, het Nederlands en het Duits, overeenkomstig artikel 65 van de bijzondere wet van 6 januari 1989 op het Grondwettelijk Hof, op 26 september 2024.

De griffier, De voorzitter,

Nicolas Dupont Pierre Nihoul