Rolnummers 6590, 6597, 6599 en 6601
Arrest nr. 57/2021 van 22 april 2021

A R R E S T

In zake : de beroepen tot vernietiging van de wet van 29 mei 2016 « betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie », ingesteld door de « Ordre des barreaux francophones et germanophone », door de vzw « Académie Fiscale » en Jean Pierre Riquet, door de vzw « Liga voor Mensenrechten » en de vzw « Ligue des Droits de l'Homme » en door Patrick Van Assche en anderen.

Het Grondwettelijk Hof,

samengesteld uit de voorzitters F. Daoût en L. Lavrysen, en de rechters J.-P. Moerman, T. Merckx-Van Goey, P. Nihoul, T. Giet, R. Leysen, J. Moerman, M. Pâques en Y. Kherbache, bijgestaan door de griffier F. Meersschaut, onder voorzitterschap van voorzitter F. Daoût,

wijst na beraad het volgende arrest :

*

* *

I. *Onderwerp van de beroepen en rechtspleging*

a. Bij verzoekschrift dat aan het Hof is toegezonden bij op 10 januari 2017 ter post aangetekende brief en ter griffie is ingekomen op 11 januari 2017, heeft de « Ordre des barreaux francophones et germanophone », bijgestaan en vertegenwoordigd door Mr. E. Lemmens en Mr. J.-F. Henrotte, advocaten bij de balie te Luik, beroep tot vernietiging ingesteld van de wet van 29 mei 2016 « betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie » (bekendgemaakt in het *Belgisch Staatsblad* van 18 juli 2016).

b. Bij verzoekschrift dat aan het Hof is toegezonden bij op 16 januari 2017 ter post aangetekende brief en ter griffie is ingekomen op 17 januari 2017, is beroep tot vernietiging ingesteld van dezelfde wet door de vzw « Académie Fiscale » en Jean Pierre Riquet.

c. Bij verzoekschrift dat aan het Hof is toegezonden bij op 17 januari 2017 ter post aangetekende brief en ter griffie is ingekomen op 18 januari 2017, is beroep tot vernietiging ingesteld van dezelfde wet door de vzw « Liga voor Mensenrechten », bijgestaan en vertegenwoordigd door Mr. J. Vander Velpen, advocaat bij de balie van Antwerpen, en de vzw « Ligue des Droits de l'Homme », bijgestaan en vertegenwoordigd door Mr. R. Jespers, avocaat bij de balie van Antwerpen.

d. Bij verzoekschrift dat aan het Hof is toegezonden bij op 18 januari 2017 ter post aangetekende brief en ter griffie is ingekomen op 19 januari 2017, is beroep tot vernietiging ingesteld van dezelfde wet door Patrick Van Assche, Christel Van Akeleyen en Karina De Hoog, bijgestaan en vertegenwoordigd door Mr. D. Pattyn, advocaat bij de balie van West-Vlaanderen.

Die zaken, ingeschreven onder de nummers 6590, 6597, 6599 en 6601 van de rol van het Hof, werden samengevoegd.

Bij tussenarrest nr. 96/2018 van 19 juli 2018, bekendgemaakt in het *Belgisch Staatsblad* van 27 september 2018, heeft het Hof de volgende prejudiciële vragen gesteld aan het Hof van Justitie van de Europese Unie :

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

nader in die regeling opgenomen waarborgen op het vlak van de bewaring van de gegevens en van de toegang ertoe ?

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

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

Bij arrest van 6 oktober 2020 in de zaken C-511/18, C-512/18 en C-520/18 heeft het Hof van Justitie van de Europese Unie op de vragen geantwoord.

Bij beschikking van 21 oktober 2020 heeft het Hof, na de rechters-verslaggevers M. Pâques en T. Merckx-Van Goey te hebben behoord, beslist :

- de debatten te heropenen;

- de partijen uit te nodigen, in een uiterlijk op 23 november 2020 in te dienen aanvullende memorie, waarvan ze binnen dezelfde termijn een kopie laten toekomen aan de andere partijen, hun standpunt mee te delen ten aanzien van de weerslag van het voormelde arrest van het Hof van Justitie van de Europese Unie op de thans voorliggende zaken;

- dat geen terechtzitting zal worden gehouden, tenzij een partij binnen zeven dagen na ontvangst van de kennisgeving van die beschikking een verzoek heeft ingediend om te worden gehoord, en

- dat, behoudens zulk een verzoek, de debatten zullen worden gesloten op 25 november 2020 en de zaken in beraad zullen worden genomen.

Aanvullende memories zijn ingediend door :

- de verzoekende partij in de zaak nr. 6590;

- de verzoekende partijen in de zaak nr. 6599;

- de verzoekende partijen in de zaak nr. 6601;

- de Ministerraad, bijgestaan en vertegenwoordigd door Mr. E. de Lophem en Mr. S. Depré, advocaten bij de balie te Brussel (in de zaken nrs. 6590 en 6597);

- de Ministerraad, bijgestaan en vertegenwoordigd door Mr. J. Vanpraet, advocaat bij de balie van West-Vlaanderen (in de zaken nrs. 6599 en 6601).

Ingevolge de verzoeken van meerdere partijen om te worden gehoord, heeft het Hof bij beschikking van 12 november 2020 de dag van de terechtzitting bepaald op 9 december 2020.

Op de openbare terechtzitting van 9 december 2020 :

- zijn verschenen :

. Me E. Kiehl, advocaat bij de balie te Luik, *loco* Mr. E. Lemmens, en Mr. J.-F. Henrotte, voor de verzoekende partij in de zaak nr. 6590;

. Mr. R. Jespers en Mr. J. Fermon, advocaat bij de balie te Brussel, voor de verzoekende partijen in de zaak nr. 6599;

. D. Pattyn, voor de verzoekende partijen in de zaak nr. 6601;

. Mr. E. de Lophem, tevens *loco* Mr. S. Depré, voor de Ministerraad (in de zaken nrs. 6590 en 6597);

. Mr. J. Vanpraet, voor de Ministerraad (in de zaken nrs. 6599 en 6601);

- hebben de rechters-verslaggevers M. Pâques en T. Merckx-Van Goey 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 aanvullende memories ingediend na het op 6 oktober 2020 door het Hof van Justitie van de Europese Unie gewezen arrest

A.1.1. De « Ordre des barreaux francophones et germanophone » (hierna : OBFG) betoogt dat de wet « betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie » (hierna : de bestreden wet) aan geen enkele voorwaarde voldoet met betrekking tot de uitzonderingen op het verbod

op de algemene bewaring van de gegevens, die door het Hof van Justitie van de Europese Unie zijn aanvaard bij zijn arrest van 6 oktober 2020, in zake *La Quadrature du Net en andere* (C-511/18, C-512/18 en C-520/18), en dat daarbij niet in de vereiste daadwerkelijke waarborgen wordt voorzien.

A.1.2. Volgens de OBFG wordt bij de bestreden wet in geen enkel stadium van de procedure een jurisdictionele controle georganiseerd van het verzamelen van de gegevens, noch van het bewaren ervan. De rechterlijke controle op de toegang waarom wordt verzocht in het kader van een strafonderzoek of de door de BIM-commissie uitgeoefende controle, wat de inlichtingendiensten betreft, hebben immers alleen betrekking op de toegang tot de gegevens. Die controles zijn daarenboven geen rechtsmiddelen die openstaan voor belanghebbende derden.

Wat betreft de mogelijkheid voor een lidstaat om wettelijke maatregelen te nemen die toelaten gebruik te maken van een bevel aan de aanbieders van diensten om over te gaan tot een algemene en ongedifferentieerde bewaring van bepaalde gegevens, los van de ontstentenis van voldoende waarborgen, beperkt de bestreden wet zich niet ertoe precieze situaties te beogen die te maken hebben met een ernstige en daadwerkelijke bedreiging van de nationale veiligheid. De bestreden wet voorziet evenmin in een verplichting tot gerichte bewaring van de verkeers- en locatiegegevens en maakt geen enkel onderscheid tussen de betrokken personen, ongeacht of zij al dan niet bij een onderzoek zijn betrokken of al dan niet aan een beroepsgeheim zijn onderworpen.

Wat betreft de mogelijkheid om te voorzien in een algemene en ongedifferentieerde bewaring van de aan de bron van een verbinding toegewezen IP-adressen, beoogt de bestreden wet drie categorieën van gegevens : identificatiegegevens, gegevens met betrekking tot toegang en verbinding, alsook communicatiegegevens. Bovendien wordt de periode niet beperkt tot het strikt noodzakelijke.

De OBFG doet gelden dat de voorwaarden met betrekking tot de laatste twee door het Hof van Justitie aanvaarde uitzonderingen niet vervuld zijn, aangezien het nagestreefde doel, net zoals de bewaarde gegevens, te ruim is, en aangezien niet in enige daadwerkelijke controle wordt voorzien.

De OBFG verwijst naar de punten 117 en 118 van het arrest van het Hof van Justitie met betrekking tot de advocaten en de andere personen die aan het beroepsgeheim zijn onderworpen, en preciseert dat de gegevens die krachtens de bestreden wet worden verzameld en bewaard, het mogelijk maken te bepalen of een advocaat is geraadpleegd door een natuurlijke persoon dan wel een rechtspersoon, en die advocaat en zijn gesprekpartners, alsook de data en uren van de communicatie te identificeren.

A.1.3. Tot slot is de OBFG van mening dat het Hof niet ertoe gemachtigd is om, in geval van vernietiging, de gevolgen van de bestreden wet te handhaven.

A.2.1. De verzoekende partijen in de zaak nr. 6599 betogen dat uit het arrest van het Hof van Justitie van 6 oktober 2020 volgt dat de middelen gegrond zijn en dat de bestreden wet in haar geheel moet worden vernietigd. Alle bepalingen van de bestreden wet zijn immers verbonden met de verplichting tot algemene en ongedifferentieerde bewaring van de verkeers- en locatiegegevens, die door het Hof van Justitie is afgekeurd.

A.2.2. De verzoekende partijen zijn van mening dat geen enkele van de bepalingen van de bestreden wet overeenstemt met een van de vijf hypotheses die het Hof van Justitie verenigbaar heeft geacht met 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 » (hierna : de richtlijn 2002/58/EG). Zo bevat de bestreden wet geen enkele specifieke bepaling met betrekking tot de bewaring van de IP-adressen voor een periode die vanuit een temporeel oogpunt tot het strikt noodzakelijke is beperkt, de bewaring van de gegevens inzake de burgerlijke identiteit van de gebruikers, de verplichting die aan diegenen die de gegevens bewaren en aan de operatoren zou kunnen worden opgelegd om realtime een analyse van de verkeers- en de locatiegegevens uit te voeren, of de realtimebewaring van technische gegevens met betrekking tot de locatie van de eindapparatuur. In elk geval bevat de bestreden wet geen duidelijke en nauwkeurige regels volgens dewelke de gegevens worden bewaard overeenkomstig de daaraan verbonden materiële en procedurele modaliteiten, noch daadwerkelijke waarborgen tegen het risico van misbruik, zoals het Hof van Justitie nochtans vereist.

A.2.3. De verzoekende partijen zijn van mening dat het arrest van het Hof van Justitie het niet mogelijk maakt in geval van vernietiging de gevolgen van de bestreden wet te handhaven en dat het de strafrechter niet is toegestaan informatie of bewijselementen die zijn verzameld met toepassing van die wet te gebruiken, zodat die informatie of die elementen bijgevolg uit het dossier moeten worden verwijderd. Zij vragen zich af of de drie door

het Hof van Justitie vermelde voorwaarden die, wanneer zij vervuld zijn, de strafrechter de verplichting opleggen de informatie of de bewijselementen terzijde te schuiven die door de algemene en ongedifferentieerde bewaring van de gegevens zijn verkregen, al dan niet cumulatief zijn, en zijn in ondergeschikte orde van mening dat het bestaan van een enkele van de drie voorwaarden volstaat om de voormelde informatie of elementen uit de debatten te weren.

A.3.1. Wat het eerste onderdeel van het eerste middel betreft, doen de verzoekende partijen in de zaak nr. 6601 gelden dat de bestreden wet geen systeem invoert dat een algemeen bevel tot bewaring van de gegevens, noch een gerichte bewaring, noch een bevel tot snelle bewaring in de zin waarin het Hof van Justitie dat begrijpt, mogelijk maakt. De verplichting tot bewaring is het directe en uitsluitende gevolg van de bestreden wet, zonder dat een bevoegde overheid daartoe de in de wet beoogde aanbieders en operatoren dat dient te gelasten.

De verzoekende partijen doen gelden dat de bestreden wet niet voorziet in een specifieke regeling ten aanzien van de IP-adressen en de identificatiegegevens. Artikel 126, § 3, vierde lid, van de wet van 13 juni 2005 « betreffende de elektronische communicatie » (hierna : de wet van 13 juni 2005) verleent dienaangaande een delegatie aan de Koning. In die delegatie worden de te bewaren gegevens niet voldoende nauwkeurig beschreven en worden de essentiële voorwaarden waaraan die gegevens moeten voldoen, evenmin vastgelegd. Zij voldoet bijgevolg niet aan de vereisten van het Hof van Justitie. Bovendien bevat de bestreden wet geen enkel onderscheid, geen enkele beperking of geen enkele uitzondering naar gelang van het met de bewaring van de gegevens nagestreefde doel. Zij betreft alle personen die gebruikmaken van elektronische communicatiemiddelen, zelfs indien er geen enkele aanwijzing is dat hun gedrag verbonden is met ernstige strafbare feiten. De bewaring van die gegevens is evenmin beperkt tot hetgeen strikt noodzakelijk is met het oog op de verwezenlijking van de nagestreefde doelen. Het staat aan de wetgever een geheel nieuwe volledige regeling in te voeren.

Wat het derde onderdeel betreft, verwijzen de verzoekende partijen naar punt 118 van het arrest van het Hof van Justitie over de weerslag van de verplichting tot algemene bewaring van de gegevens op personen die tot het beroepsgeheim zijn gehouden en op klokkenluiders.

A.3.2. Wat het tweede middel betreft, betogen de verzoekende partijen dat de vernietiging van de verplichting tot bewaring van de gegevens noodzakelijkerwijs de vernietiging van de toegang tot die gegevens met zich meebrengt.

Wat het eerste onderdeel betreft, doen de verzoekende partijen gelden dat de bestreden wet de gerechtelijke autoriteiten ertoe machtigt toegang te hebben tot de gegevens voor elk misdrijf. Bovendien kunnen de inlichtingen- en veiligheidsdiensten in het kader van een groot aantal onvoldoende afgebakende potentiële bedreigingen toegang hebben tot de gegevens, zonder dat hun machtiging voldoende wordt beperkt. De bestreden wet beperkt dus niet de toegang tot de gegevens die aldus worden bewaard teneinde de nationale veiligheid te waarborgen en de zware criminaliteit te bestrijden.

De verzoekende partijen doen gelden dat in tegenstelling tot het arrest van 2 oktober 2018, *Ministerio Fiscal* (C-207/16), dat betrekking heeft op identificatiegegevens van commerciële aard, waartoe de bevoegde autoriteiten toegang kunnen hebben zonder dat die toegang wordt beperkt tot de doeleinden van de strijd tegen zware criminaliteit, het arrest van het Hof van Justitie van 6 oktober 2020 de toegang tot de gegevens beperkt tot heel precieze doeleinden, namelijk de nationale veiligheid waarborgen, zware criminaliteit bestrijden en ernstige bedreigingen voor de openbare veiligheid voorkomen.

De verzoekende partijen doen gelden dat het arrest van het Hof van Justitie van 6 oktober 2020 niet relevant is om het tweede onderdeel van het middel te beoordelen, dat de ontstentenis betreft van voorafgaande controle van de toegang tot de gegevens die een rechterlijke instantie of een onafhankelijke bestuurlijke autoriteit moet uitoefenen, aangezien de gegevens die zijn verzameld op basis van een met het Unierecht strijdig geachte verplichting tot bewaring niet mogen worden verwerkt, los van de vraag of een voorafgaande controle al dan niet is georganiseerd.

Artikel 88*bis* van het Wetboek van strafvordering, zoals het is gewijzigd bij artikel 9 van de bestreden wet, biedt de onderzoeksrechter de mogelijkheid toegang te hebben tot de bewaarde gegevens voor het opsporen, onderzoeken en vervolgen van strafbare feiten die een correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben. Met die toegang wordt het opsporen van de verkeersgegevens van elektronische communicatiemiddelen van waaruit of waarnaar elektronische communicaties worden of werden gedaan en het lokaliseren van de oorsprong of de bestemming van elektronische communicaties beoogd. Die toegang betreft dus niet de identificatiegegevens. Het voormelde artikel 88*bis* kan dus niet worden gehandhaafd

teneinde de toegang tot die gegevens te verkrijgen. De (commerciële) identificatiegegevens mogen door de aanbieders en de operatoren pas worden medegedeeld nadat de onderzoeksrechter daartoe een bevel heeft gegeven, overeenkomstig artikel 88*quater*, § 2, van het Wetboek van strafvordering.

A.3.3. Wat het derde middel betreft, doen de verzoekende partijen gelden dat de vernietiging van de verplichting tot bewaring zich noodzakelijkerwijs ook uitstrekt tot de bewaringstermijnen van die gegevens en dat het aan de betrokken personen (aanbieders en operatoren, inlichtingen- en veiligheidsdiensten, enz.) staat de met toepassing van de bestreden wet verzamelde telecommunicatiegegevens te wissen.

A.3.4. Wat het vierde middel betreft, verwijzen de verzoekende partijen naar het in het geding zijnde arrest van 16 juli 2020, *Schrems II*, waarbij het Hof van Justitie het uitvoeringsbesluit (EU) 2016/1250 van de Commissie van 12 juli 2016 « overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad betreffende de gepastheid van de door het EU-VS-privacyschild geboden bescherming » vernietigt.

A.3.5. De verzoekende partijen doen gelden dat in geval van vernietiging, het arrest van het Hof van Justitie C-511/18 zich verzet tegen de handhaving van de gevolgen van de bestreden wet. Artikel 32 van de voorafgaande titel van het Wetboek van strafvordering moet in die zin worden geïnterpreteerd dat het de rechter ertoe verplicht de met toepassing van de bestreden wet verzamelde gegevens als bewijs uit te sluiten. Het gebruik van die gegevens is immers strijdig met het recht op een eerlijk proces, indien de personen die ervan worden verdacht een strafbaar feit te hebben gepleegd, niet over een reële mogelijkheid beschikken om die informatie en de bewijselementen op dienstige wijze uit te leggen, indien die informatie en bewijselementen betrekking hebben op een technisch domein waarover de rechter geen kennis heeft en indien zij een beslissende invloed kunnen hebben op zijn beoordeling van de feiten. Voor het overige moeten de gegevens, wat betreft een ander gebruik ervan dan als bewijs in een strafprocedure, door de betrokken personen (aanbieders en operatoren, inlichtingen- en veiligheidsdiensten, enz.) worden vernietigd.

A.4.1. Volgens de Ministerraad volgt uit het arrest van het Hof van Justitie van 6 oktober 2020 dat een algemene en ongedifferentieerde wettelijke verplichting tot bewaring, in elk geval wat betreft de aan de bron van een verbinding toegewezen IP-adressen en de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronische communicatiemiddelen, verenigbaar is met de richtlijn 2002/58/EG en met het Handvest van de grondrechten van de Europese Unie.

A.4.2. De Ministerraad betoogt dat de verplichting tot bewaring van de aan de bron toegewezen IP-adressen, zoals bepaald bij de bestreden wet, er is « met het oog op de strijd tegen de zware criminaliteit en de preventie van ernstige bedreigingen van de openbare veiligheid […], net zoals de vrijwaring van de nationale veiligheid », zoals wordt aangetoond door het feit dat de toegang tot die gegevens wordt geregeld in artikel 126, § 2, van de wet van 13 juni 2005. Dat geldt des te meer daar bij de toegang tot de gegevens steeds de beginselen van evenredigheid en subsidiariteit in acht moeten worden genomen.

Zo is, volgens de Ministerraad, de toegang tot die gegevens in het kader van een strafonderzoek slechts mogelijk voor de opsporing van de strafbare feiten bedoeld in artikel 88*bis*, § 2, van het Wetboek van strafvordering. In het kader van een opsporingsonderzoek, daarentegen, is het slechts mogelijk toegang te hebben tot de in artikel 46*bis* van hetzelfde Wetboek bedoelde identificatiegegevens teneinde misdaden en wanbedrijven op te sporen en onder voorbehoud dat de beginselen van evenredigheid en subsidiariteit in acht worden genomen. De inlichtingen- en veiligheidsdiensten kunnen slechts toegang hebben tot de aan de bron toegewezen IP-adressen in het belang van het vervullen van hun opdrachten, zoals zij wettelijk zijn beschreven. Elke officier van gerechtelijke politie van het BIPT kan slechts toegang hebben tot de gegevens met het oog op het opsporen, het onderzoek en de vervolging van inbreuken op de artikelen 114, 124 en 126 van de wet van 13 juni 2005. Tot slot draagt de toegang tot die gegevens door een officier van de Cel Vermiste Personen, voor een periode die tot 48 uren is beperkt, ook bij tot de door het Hof van Justitie bepaalde doelstellingen. Dienaangaande is de Ministerraad van oordeel dat de bewaringstermijn van de aan de bron toegewezen IP-adressen, die twaalf maanden bedraagt, niet verder reikt dan hetgeen strikt noodzakelijk is om de nagestreefde doelstelling te bereiken.

Volgens de Ministerraad zijn de bewaring en de toegang tot de voormelde IP-adressen aan strikte voorwaarden onderworpen en maken zij het voorwerp uit van de vereiste controlemechanismen.

A.4.3. De Ministerraad betoogt dat de verplichting tot bewaring van de civiele-identiteitsgegevens van de gebruikers van elektronische communicatiemiddelen verenigbaar is met de in de middelen aangevoerde bepalingen. Hij herinnert eraan dat die verplichting tot bewaring gepaard gaat met de noodzakelijke waarborgen op het vlak van toegang, bewaring en controle.

A.4.4. Wat betreft de weerslag van het arrest van het Hof van Justitie op de bestreden wet, onderstreept de Ministerraad dat de aan de bron toegewezen IP-adressen identificatiegegevens vormen in de zin van artikel 126, § 3, eerste lid, van de wet van 13 juni 2005. Dat soort van gegevens vormen geen verkeersgegevens. Zowel de algemene en ongedifferentieerde verplichting tot het bewaren van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronische communicatie als de algemene en ongedifferentieerde verplichting tot het bewaren van de aan de bron van een verbinding toegewezen IP-adressen worden beoogd in artikel 126, § 3, eerste lid, van de wet van 13 juni 2005. Naar de mening van de Ministerraad is de bestreden wet dus in elk geval wat betreft die punten verenigbaar met de in de middelen aangevoerde bepalingen. Een eventuele vernietiging van de bestreden wet zou moeten worden beperkt tot artikel 126, § 3, tweede en derde lid, van de wet van 13 juni 2005. Aangezien de algemene en ongedifferentieerde verplichting tot het bewaren van die twee soorten van gegevens verenigbaar is met de in de middelen aangevoerde bepalingen, zouden de andere bepalingen van de bestreden wet evenmin moeten worden vernietigd. Zij bevatten immers de noodzakelijke waarborgen op het vlak van bewaring en toegang tot die gegevens.

- *B* –

Ten aanzien van de bestreden wet en de context ervan

B.1. De verzoekende partijen vorderen de vernietiging van de wet van 29 mei 2016 « betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie », die bepaalt :

« HOOFDSTUK 1. - *Algemene bepaling*

Artikel 1. Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.

HOOFDSTUK 2. - *Wijzigingen van de wet van 13 juni 2005 betreffende de elektronische communicatie*

Art. 2. In artikel 2 van de wet [van] 13 juni 2005 betreffende de elektronische communicatie, laatstelijk gewijzigd bij de wet van 18 december 2015, en gedeeltelijk vernietigd bij arrest nr. 84/2015 van het Grondwettelijk Hof, worden de volgende wijzigingen aangebracht :

a) de bepaling onder 11° wordt vervangen als volgt :

‘ 11° “ operator ” : ieder persoon die onder de verplichting valt een kennisgeving te doen overeenkomstig artikel 9; ’;

b) in de plaats van de bepaling onder 74°, vernietigd bij arrest nr. 84/2015 van het Grondwettelijk Hof, wordt een als volgt luidende bepaling onder 74° ingevoegd :

‘ 74° “ Oproeppoging zonder resultaat ” : een communicatie waarbij een oproep wel tot een verbinding heeft geleid, maar onbeantwoord is gebleven of via het netwerkbeheer is beantwoord. ’.

Art. 3. Artikel 125, § 2, van dezelfde wet wordt opgeheven.

Art. 4. In dezelfde wet wordt in de plaats van artikel 126, vernietigd bij arrest nr. 84/2015 van het Grondwettelijk Hof, het als volgt luidende artikel 126 ingevoegd :

‘ Art. 126. § 1. Onverminderd de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, dienen de aanbieders aan het publiek van telefoniediensten, via internet inbegrepen, van internettoegang, van e-mail via het internet, de operatoren die openbare elektronische-communicatienetwerken aanbieden, alsook de operatoren die een van deze diensten verstrekken, de in paragraaf 3 bedoelde gegevens die door hen worden gegenereerd of verwerkt in het kader van de verstrekking van de betrokken communicatiediensten, te bewaren.

Dit artikel heeft geen betrekking op de inhoud van de communicatie.

De verplichting om de in paragraaf 3 bedoelde gegevens te bewaren, is ook van toepassing op oproeppogingen zonder resultaat, voor zover die gegevens in verband met de aanbieding van de bedoelde communicatiediensten :

1° wat de telefoniegegevens betreft, worden gegenereerd of verwerkt door de operatoren van openbare elektronische-communicatiediensten of van een openbaar netwerk voor elektronische communicatie, of

2° wat de internetgegevens betreft, door deze aanbieders worden gelogd.

§ 2. Enkel de volgende overheden mogen op eenvoudig verzoek van de in paragraaf 1, eerste lid, bedoelde aanbieders en operatoren gegevens ontvangen die worden bewaard krachtens dit artikel om de doeleinden en volgens de hieronder opgesomde voorwaarden :

1° de gerechtelijke autoriteiten, met het oog op het opsporen, het onderzoek en de vervolging van inbreuken, voor de uitvoering van de in de artikelen 46*bis* en 88*bis* van het Wetboek van strafvordering beoogde maatregelen en volgens de voorwaarden bepaald in die artikelen;

2° de inlichtingen- en veiligheidsdiensten, teneinde de inlichtingenopdrachten met inzet van de methoden voor het vergaren van gegevens zoals bedoeld in de artikelen 16/2, 18/7 en 18/8 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten te vervullen en volgens de voorwaarden vastgelegd in die wet;

3° elke officier van gerechtelijke politie van het Instituut, met het oog op het opsporen, het onderzoek en de vervolging van inbreuken op de artikelen 114, 124 en dit artikel;

4° de hulpdiensten die hulp ter plaatse bieden, wanneer ze naar aanleiding van een noodoproep, van de betrokken aanbieder of operator niet de identificatiegegevens van de oproeper ontvangen met behulp van de databank beoogd in artikel 107, § 2, derde lid, of onvolledige of onjuiste gegevens krijgen. Enkel de identificatiegegevens van de oproeper mogen worden gevraagd en uiterlijk binnen 24 uur na de oproep;

5° de officier van gerechtelijke politie van de Cel Vermiste Personen van de federale politie, in het kader van zijn opdracht tot het verlenen van hulp aan personen in nood, opsporing

van personen van wie de verdwijning onrustwekkend is en wanneer er ernstige vermoedens of aanwijzingen bestaan dat de fysieke integriteit van de vermiste persoon in onmiddellijk gevaar is. Enkel de gegevens die zijn beoogd in paragraaf 3, eerste en tweede lid, met betrekking tot de vermiste persoon en bewaard gedurende de 48 uur voorafgaand aan het verzoek om de gegevens te krijgen, mogen worden gevraagd aan de operator of de aanbieder in kwestie via een door de Koning aangewezen politiedienst;

6° de Ombudsdienst voor telecommunicatie, met het oog op de identificatie van de persoon die kwaadwillig gebruik heeft gemaakt van een elektronische-communicatienetwerk of -dienst, conform de voorwaarden beoogd in artikel 43*bis*, § 3, 7°, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven. Enkel de identificatiegegevens mogen worden gevraagd.

De aanbieders en operatoren bedoeld in paragraaf 1, eerste lid, zorgen ervoor dat de in paragraaf 3 bedoelde gegevens onbeperkt toegankelijk zijn vanuit België en dat deze gegevens, en alle andere daarmee verband houdende vereiste informatie onverwijld en uitsluitend aan de in deze paragraaf bedoelde autoriteiten kunnen worden meegedeeld.

Onverminderd andere wettelijke voorschriften mogen de aanbieders en operatoren bedoeld in paragraaf 1, eerste lid, de krachtens paragraaf 3 bewaarde gegevens niet gebruiken voor andere doeleinden.

§ 3. De gegevens ter identificatie van de gebruiker of de abonnee en de communicatiemiddelen, met uitzondering van de gegevens waarin het tweede en derde lid specifiek voorzien, worden gedurende twaalf maanden bewaard vanaf de datum waarop communicatie voor de laatste maal mogelijk is via de gebruikte dienst.

De gegevens met betrekking tot de toegang tot en de verbinding van de eindapparatuur met het netwerk en met de dienst en met betrekking tot de plaats van die apparatuur, inclusief het netwerkaansluitpunt, worden bewaard gedurende twaalf maanden, vanaf de datum van de communicatie.

De communicatiegegevens, met uitzondering van de inhoud, met inbegrip van hun herkomst en hun bestemming, worden gedurende twaalf maanden bewaard vanaf de datum van de communicatie.

De Koning bepaalt, bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van Justitie en van de minister, en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de te bewaren gegevens per type van categorie bedoeld in het eerste tot derde lid alsook de vereisten waaraan deze gegevens moeten beantwoorden.

§ 4. Wat betreft de bewaring van de gegevens bedoeld in paragraaf 3, dienen de aanbieders en operatoren bedoeld in paragraaf 1, eerste lid :

1° te garanderen dat de bewaarde gegevens dezelfde kwaliteit hebben en onderworpen worden aan dezelfde beveiligings- en beschermingsmaatregelen als de gegevens in het netwerk;

2° ervoor te zorgen dat de bewaarde gegevens worden onderworpen aan passende technische en organisatorische maatregelen om de gegevens te beveiligen tegen vernietiging,

hetzij per ongeluk, hetzij onrechtmatig, tegen verlies of wijziging per ongeluk, niet-toegelaten of onrechtmatige opslag, verwerking, toegang of openbaarmaking;

3° te garanderen dat de toegang tot de bewaarde gegevens om te antwoorden op de verzoeken van de autoriteiten bedoeld in paragraaf 2, enkel gebeurt door een of meer leden van de Coördinatiecel bedoeld in artikel 126/1, § 1;

4° de gegevens op het grondgebied van de Europese Unie te bewaren;

5° te zorgen voor 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;

6° ervoor te zorgen dat de bewaarde gegevens na afloop van de bewaringstermijn die voor die gegevens geldt zoals vastgelegd in paragraaf 3, worden verwijderd van elke drager, onverminderd de artikelen 122 en 123;

7° ervoor te zorgen dat het gebruik van de bewaarde gegevens kan worden opgespoord voor elk verzoek om deze gegevens te verkrijgen vanwege een autoriteit bedoeld in paragraaf 2.

De in het eerste lid, 7°, bedoelde opspoorbaarheid wordt verwezenlijkt aan de hand van een logboek. Het Instituut en de Commissie voor de bescherming van de persoonlijke levenssfeer mogen dat logboek raadplegen of een kopie van een deel of van het geheel van dat logboek eisen. Het Instituut en de Commissie voor de bescherming van de persoonlijke levenssfeer sluiten een protocol tot samenwerking voor de raadpleging van en het toezicht op dat logboek.

§ 5. De minister en de minister van Justitie zorgen ervoor dat statistieken inzake de bewaring van de gegevens die worden gegenereerd of verwerkt in het kader van de verstrekking van openbaar toegankelijke communicatienetwerken en -diensten jaarlijks worden bezorgd aan de Kamer van volksvertegenwoordigers.

Die statistieken omvatten met name :

1° de gevallen waarin overeenkomstig de toepasselijke wettelijke bepalingen gegevens zijn verstrekt aan de bevoegde autoriteiten;

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 gegevens niet konden worden ingewilligd.

Die statistieken mogen geen persoonsgegevens omvatten.

De gegevens die betrekking hebben op de toepassing van paragraaf 2, 1°, worden tevens bijgevoegd bij het verslag dat de minister van Justitie overeenkomstig artikel 90*decies* van het Wetboek van strafvordering moet uitbrengen aan het Parlement.

De Koning bepaalt, op voorstel van de minister van Justitie en de minister en op advies van het Instituut, de statistieken die de aanbieders en operatoren bedoeld in paragraaf 1, eerste lid,

jaarlijks bezorgen aan het Instituut en die welke het Instituut bezorgt aan de minister en aan de minister van Justitie.

§ 6. Onverminderd het verslag bedoeld in paragraaf 5, vierde lid, brengen de minister en de minister van Justitie, twee jaar na de inwerkingtreding van het in paragraaf 3, vierde lid, bedoelde koninklijk besluit een evaluatieverslag uit aan de Kamer van volksvertegenwoordigers over de toepassing van dit artikel, teneinde na te gaan of het nodig is bepalingen aan te passen, inzonderheid wat betreft de te bewaren gegevens en de bewaringstermijn. ’.

Art. 5. In dezelfde wet wordt een artikel 126/1 ingevoegd, luidende :

‘ Art. 126/1. § 1. Binnen elke operator en elke aanbieder bedoeld in artikel 126, § 1, eerste lid, wordt een Coördinatiecel opgericht, belast met het verstrekken aan de wettelijk bevoegde Belgische autoriteiten, op hun verzoek, van de gegevens bewaard krachtens de artikelen 122, 123 en 126, de identificatiegegevens van de oproeper krachtens artikel 107, § 2, eerste lid, of de gegevens die kunnen worden gevorderd krachtens de artikelen 46*bis*, 88*bis* en 90*ter* van het Wetboek van strafvordering en de artikelen 18/7, 18/8, 18/16 en 18/17 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

In voorkomend geval kunnen verscheidene operatoren of aanbieders een gemeenschappelijke Coördinatiecel oprichten. In dergelijk geval moet deze Coördinatiecel voorzien in dezelfde dienst voor elke operator of aanbieder.

Om deel uit te maken van de Coördinatiecel dienen de leden :

1° het voorwerp [te] hebben uitgemaakt van een positief en niet-achterhaald veiligheidsadvies conform artikel 22*quinquies* van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen;

2° niet het voorwerp [te] hebben uitgemaakt van een weigering door de minister van Justitie, waarbij die weigering met redenen moet worden omkleed en zich te allen tijde kan voordoen.

Een advies wordt als achterhaald beschouwd 5 jaar na zijn verstrekking.

De operatoren en aanbieders die geen van de diensten bedoeld in artikel 126, § 1, verstrekken, zijn vrijgesteld van de in het derde lid, 1°, beoogde voorwaarde.

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 of van de aanbieder.

De leden van de Coördinatiecel en de aangestelden die technische bijstand verlenen, zijn onderworpen aan het beroepsgeheim.

Elke operator en elke aanbieder bedoeld in artikel 126, § 1, eerste lid, waakt over de vertrouwelijkheid van de gegevens die worden behandeld door de Coördinatiecel en deelt onverwijld aan het Instituut en aan de Commissie voor de bescherming van de persoonlijke

levenssfeer de contactgegevens van de Coördinatiecel en van zijn leden mee alsook elke wijziging van die gegevens.

§ 2. Elke operator en elke aanbieder bedoeld in artikel 126, § 1, eerste lid, stelt een interne procedure op om te antwoorden op de verzoeken vanwege de autoriteiten om toegang tot de persoonsgegevens betreffende de gebruikers. Hij verstrekt aan het Instituut, op verzoek, gegevens over deze procedures, het aantal ontvangen verzoeken, de aangevoerde wettelijke grondslag en hun antwoord.

Elke operator en elke aanbieder bedoeld in artikel 126, § 1, eerste lid, wordt beschouwd als verantwoordelijk voor de verwerking in de zin van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, voor de gegevens behandeld op basis van artikel 126 en dit artikel.

De operatoren van openbare netwerken voor elektronische communicatie en de aanbieders bedoeld in artikel 126, § 1, eerste lid, nemen artikel 114, § 2, in acht voor de toegang tot de gegevens bedoeld in paragraaf 1 en hun overdracht aan de autoriteiten.

§ 3. Elke aanbieder bedoeld in artikel 126, § 1, eerste lid, en elke operator bedoeld in artikel 126, § 1, eerste lid, wijst een of meer aangestelden aan voor de bescherming van persoonsgegevens, die moet beantwoorden aan de cumulatieve voorwaarden opgesomd in paragraaf 1, derde lid.

Deze aangestelde mag geen deel uitmaken van de Coördinatiecel.

Verscheidene operatoren of aanbieders mogen een of meer gemeenschappelijke aangestelden voor de bescherming van de persoonsgegevens aanduiden. In dat geval moeten deze aangestelden dezelfde opdracht uitvoeren voor elke individuele operator of aanbieder.

Bij de uitvoering van zijn opdrachten handelt de aangestelde voor de bescherming van de persoonsgegevens in volledige onafhankelijkheid, en heeft hij toegang tot alle persoonsgegevens die worden bezorgd aan de autoriteiten, alsook tot alle relevante lokalen van de aanbieder of de operator.

De uitoefening van zijn opdrachten mag voor de aangestelde geen nadelen met zich brengen. Hij mag in het bijzonder als aangestelde niet worden ontslagen of vervangen wegens de uitvoering van de taken die hem zijn toevertrouwd, zonder grondige motivering.

De aangestelde moet de mogelijkheid hebben om rechtstreeks te communiceren met de directie van de operator of de aanbieder.

De aangestelde voor de gegevensbescherming zorgt ervoor dat :

1° de behandelingen door de Coördinatiecel worden uitgevoerd conform de wet;

2° de aanbieder of de operator enkel die gegevens verzamelt en bewaart die hij wettelijk mag bewaren;

3° enkel de wettelijk bevoegde autoriteiten toegang hebben tot de bewaarde gegevens;

4° de maatregelen voor beveiliging en bescherming van persoonsgegevens beschreven in deze wet en in het veiligheidsbeleid van de aanbieder of de operator ten uitvoer worden gebracht.

Elke aanbieder en elke operator bedoeld in artikel 126, § 1, eerste lid, deelt onverwijld aan het Instituut en aan de Commissie voor de bescherming van de persoonlijke levenssfeer de contactgegevens van de aangestelden voor de bescherming van persoonsgegevens mee alsook elke wijziging van die gegevens.

§ 4. De Koning bepaalt, bij een besluit vastgesteld na overleg in de Ministerraad, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut :

1° de nadere regels van het verzoek en de verstrekking van het veiligheidsadvies;

2° de vereisten waaraan de Coördinatiecel moet beantwoorden, door rekening te houden met de situatie van de operatoren en aanbieders die weinig verzoeken krijgen van de gerechtelijke overheden, die geen vestiging hebben in België of voornamelijk vanuit het buitenland handelen;

3° de informatie die moet worden verstrekt aan het Instituut en aan de Commissie voor de bescherming van de persoonlijke levenssfeer conform de paragrafen 1 en 3 alsook de autoriteiten die toegang hebben tot die informatie;

4° de overige regels die de samenwerking van de operatoren en van de aanbieders bedoeld in artikel 126, § 1, eerste lid, met de Belgische autoriteiten of met sommige van hen, regelen, voor de verstrekking van de in paragraaf 1 beoogde gegevens, in voorkomend geval en per betrokken overheid met inbegrip van de vorm en de inhoud van het verzoek. ’.

Art. 6. In artikel 127 van dezelfde wet, gewijzigd door de wetten van 4 februari 2010, 10 juli 2012 en 27 maart 2014, worden de volgende wijzigingen aangebracht :

1° in paragraaf 1 worden de volgende wijzigingen aangebracht :

a) in het eerste lid worden de woorden ‘ , aan de aanbieders bedoeld in artikel 126, § 1, eerste lid, ’ ingevoegd tussen de woorden ‘ aan de operatoren ’ en de woorden ‘ of aan de eindgebruikers ’;

b) in het tweede lid worden de woorden ‘ en de aanbieders bedoeld in artikel 126, § 1, eerste lid, ’ ingevoegd tussen de woorden ‘ de operatoren ’ en de woorden ‘ aan de in het eerste lid, 2°, bedoelde verrichtingen ’;

2° paragraaf 6 wordt opgeheven.

Art. 7. In artikel 145 van dezelfde wet, gewijzigd bij de wetten van 25 april 2007 en 27 maart 2014 worden de volgende wijzigingen aangebracht :

1° de woorden ‘ 126, 126/1, ’ worden ingevoegd tussen de woorden ‘ 124, ’ en ‘ 127 ’;

2° de woorden ‘ , 126, 126/1 ’ worden ingevoegd tussen de woorden ‘ 47 ’ en ‘ en 127 ’;

3° in de plaats van paragraaf 3*ter*, vernietigd bij arrest nr. 84/2015 van het Grondwettelijk Hof, wordt een als volgt luidende paragraaf 3*ter* ingevoegd :

‘ § 3*ter*. Met geldboete van 50 euro tot 50 000 euro en met gevangenisstraf van zes maanden tot drie jaar of met één van die straffen alleen wordt gestraft :

1° iedere persoon die, naar aanleiding van de uitoefening van zijn functie, buiten de gevallen die de wet bepaalt of zonder inachtneming van de vormen die zij voorschrijft, met bedrieglijk opzet of met het oogmerk om te schaden, de gegevens bedoeld in artikel 126 op enige manier overneemt, onder zich houdt, of er enig gebruik van maakt;

2° hij die, terwijl hij weet dat de gegevens bekomen zijn door het plegen van het misdrijf bedoeld in 1°, deze gegevens bij zich houdt, aan een andere persoon onthult of verspreidt, of er enig gebruik van maakt. ’.

HOOFDSTUK 3. - *Wijzigingen van het Wetboek van strafvordering*

Art. 8. In artikel 46*bis*, § 1, van het Wetboek van strafvordering, ingevoegd bij de wet van 10 juni 1998 en vervangen bij de wet van 23 januari 2007, worden de volgende wijzigingen aangebracht :

a) in de Franse tekst worden de woorden ‘ le concours de l'opérateur d'une réseau de communication ’ vervangen door de woorden ‘ le concours de l'opérateur d'un réseau de communication ’;

b) de paragraaf wordt aangevuld met een lid, luidende :

‘ Voor strafbare feiten die geen correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben, kunnen de procureur des Konings of, in geval van uiterst dringende noodzakelijkheid, de officier van gerechtelijke politie, de in het eerste lid bedoelde gegevens slechts vorderen voor een periode van zes maanden voorafgaand aan zijn beslissing. ’.

Art. 9. In artikel 88*bis* van hetzelfde Wetboek, ingevoegd bij de wet van 11 februari 1991, vervangen bij de wet van 10 juni 1998 en gewijzigd bij de wetten van 8 juni 2008 en 27 december 2012, worden de volgende wijzigingen aangebracht :

a) in paragraaf 1 wordt het eerste lid vervangen als volgt :

‘ Wanneer er ernstige aanwijzingen zijn dat de strafbare feiten een correctionele hoofdgevangenisstraf van een 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, zo nodig rechtstreeks of via een door de Koning aangewezen politiedienst de medewerking vorderen van de operator van een elektronisch communicatienetwerk of van de verstrekker van een elektronische communicatiedienst, om over te gaan of te 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. ';

b) in paragraaf 1, tweede lid[,] wordt het woord ' telecommunicatiemiddel ' vervangen door de woorden ' elektronisch communicatiemiddel ' en het woord ' telecommunicatie ' door [de woorden] ' elektronische communicatie ';

c) in paragraaf 1 wordt het derde lid vervangen als volgt :

' 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. ';

d) in paragraaf 1 wordt het vierde lid vervangen als volgt :

' 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. ';

e) paragraaf 1 wordt aangevuld met een lid, luidende :

' In spoedeisende gevallen kan de maatregel mondeling worden bevolen. Hij moet zo spoedig mogelijk worden bevestigd in de vorm bepaald in het derde en vierde lid. ';

f) paragraaf 2, waarvan de huidige tekst paragraaf 4 zal vormen, 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 artikel 126 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 zijn 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. ';

g) het artikel wordt aangevuld met een paragraaf 3, luidende :

‘ § 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. Diezelfden 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. ’;

h) in paragraaf 2, die tot paragraaf 4 vernummerd wordt, worden in het eerste lid de woorden ‘ Iedere operator van een telecommunicatienetwerk en iedere verstrekker van een telecommunicatiedienst ’ vervangen door de woorden ‘ Iedere operator van een elektronisch communicatienetwerk en iedere verstrekker van een elektronische communicatiedienst ’.

Art. 10. Artikel 90*decies* van hetzelfde Wetboek, ingevoegd bij de wet van 30 juni 1994 en gewijzigd bij de wetten van 8 april 2002, 7 juli 2002, 6 januari 2003 en bij de wet van 30 juli 2013 vernietigd bij arrest nr. 84/2015 van het Grondwettelijk Hof, wordt aangevuld met een lid, luidende :

‘ Bij dit verslag wordt tevens het verslag gevoegd dat werd opgesteld met toepassing van artikel 126, § 5, vierde lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie. ’.

Art. 11. In artikel 464/25, § 2, eerste lid, van hetzelfde Wetboek worden de woorden ‘ artikel 88*bis*, § 2, eerste en derde lid, ’ vervangen door de woorden ‘ artikel 88*bis*, § 4, eerste en derde lid, ’.

HOOFDSTUK 4. - *Wijzigingen van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst*

Art. 12. In artikel 13 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst, gewijzigd bij de wet van 4 februari 2010, worden de volgende wijzigingen aangebracht :

1° in het eerste lid wordt het woord ‘ inlichtingen ’ vervangen door het woord ‘ informatie ’;

2° het derde lid wordt vervangen als volgt :

‘ De inlichtingen- en veiligheidsdiensten waken over de veiligheid van de gegevens die betrekking hebben op hun bronnen en van de informatie en persoonsgegevens die deze bronnen leveren. ’;

3° het artikel wordt aangevuld met een lid, luidende :

‘ De agenten van de inlichtingen- en veiligheidsdiensten hebben toegang tot de door hun dienst ingewonnen en verwerkte informatie, inlichtingen en persoonsgegevens, voor zover deze nuttig zijn voor de uitoefening van hun functie of opdracht. ’.

Art. 13. In artikel 18/3 van dezelfde wet, ingevoegd bij de wet van 4 februari 2010, worden de volgende wijzigingen aangebracht :

a) in paragraaf 1 zal het huidige derde lid paragraaf 5 vormen;

b) in paragraaf 1, waarvan het vierde lid paragraaf 7 zal vormen, worden de woorden ‘ om de specifieke methode voor het verzamelen van gegevens aan te wenden ’ vervangen door de woorden ‘ om de aanwending van de specifieke methode voor het verzamelen van gegevens op te volgen ’;

c) paragraaf 2, waarvan het huidige tweede tot vijfde lid paragraaf 6 zullen vormen, wordt vervangen als volgt :

‘ § 2. De beslissing van het diensthoofd vermeldt :

1° de aard van de specifieke methode;

2° naargelang het geval, de natuurlijke personen of rechtspersonen, verenigingen of groeperingen, voorwerpen, plaatsen, gebeurtenissen of informatie die het voorwerp uitmaken van de specifieke methode;

3° de potentiële dreiging die de specifieke methode rechtvaardigt;

4° de feitelijke omstandigheden die de specifieke methode rechtvaardigen, de motivering inzake subsidiariteit en proportionaliteit, inbegrepen het verband tussen de bepalingen onder 2° en 3°;

5° de periode waarin de specifieke methode kan worden aangewend, te rekenen vanaf de kennisgeving van de beslissing aan de Commissie;

6° de naam van de inlichtingenofficier(en) verantwoordelijk om de aanwending van de specifieke methode op te volgen;

7° in voorkomend geval, het technisch middel dat gebruikt wordt bij de aanwending van de specifieke methode;

8° in voorkomend geval, de samenloop met een opsporings- of gerechtelijk onderzoek;

9° in voorkomend geval, de ernstige aanwijzingen waaruit blijkt dat de advocaat, de arts of de journalist persoonlijk en actief meewerkt of heeft meegewerkt aan het ontstaan of de ontwikkeling van de potentiële dreiging;

10° in geval toepassing wordt gemaakt van artikel 18/8, de motivering van de duur van de periode waarop de inzameling van gegevens betrekking heeft;

11° de datum van de beslissing;

12° de handtekening van het diensthoofd. ';

d) paragraaf 3 wordt vervangen als volgt :

' § 3. Op het einde van elke maand wordt, per specifieke methode, een lijst van de uitgevoerde maatregelen overgezonden aan de commissie.

Deze lijsten bevatten de gegevens bedoeld in § 2, 1° tot 3°, 5° en 7°. '.

e) het artikel wordt aangevuld met een paragraaf 8, luidende :

' § 8. Het diensthoofd beëindigt de specifieke methode wanneer de potentiële dreiging die haar rechtvaardigt weggevallen is, wanneer de methode niet langer nuttig is voor het doel waarvoor zij werd ingesteld, of wanneer hij een onwettigheid heeft vastgesteld. Hij brengt zijn beslissing zo spoedig mogelijk ter kennis van de Commissie. '.

Art. 14. In artikel 18/8 van dezelfde wet, ingevoegd bij de wet van 4 februari 2010, worden de volgende wijzigingen aangebracht :

a) in paragraaf 1 wordt het eerste lid vervangen als volgt :

' 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. ';

b) in paragraaf 1, tweede lid, wordt het woord ' oproepgegevens ' vervangen door het woord ' verkeersgegevens '.

c) paragraaf 2, waarvan de huidige tekst paragraaf 4 zal vormen, wordt vervangen als volgt :

' § 2. Wat betreft de toepassing van de methode bedoeld in paragraaf 1 op de gegevens die worden bewaard krachtens artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie, zijn de volgende bepalingen van toepassing :

1° voor een potentiële dreiging die betrekking heeft op een activiteit die verband kan houden met criminele organisaties of schadelijke sektarische organisaties, kan het diensthoofd in zijn beslissing de gegevens slechts vorderen voor een periode van zes maanden voorafgaand aan de beslissing;

2° voor een potentiële dreiging, andere dan deze bedoeld in de bepalingen onder 1° en 3°, kan het diensthoofd in zijn beslissing de gegevens vorderen voor een periode van negen maanden voorafgaand aan de beslissing;

3° voor een potentiële dreiging die betrekking heeft op een activiteit die verband kan houden met terrorisme of extremisme, kan het diensthoofd in zijn beslissing de gegevens vorderen voor een periode van twaalf maanden voorafgaand aan de beslissing. ’.

Art. 15. In artikel 43/3 van dezelfde wet, ingevoegd bij de wet van 4 februari 2010, worden de woorden ‘ bedoeld in artikel 18/3, § 2 ’ vervangen door de woorden ‘ bedoeld in artikel 18/3, § 3 ’.

Art. 16. In artikel 43/5, § 1, tweede lid, van dezelfde wet, worden de woorden ‘ bedoeld in artikel 18/3, § 2 ’ vervangen door de woorden ‘ bedoeld in artikel 18/3, § 3 ’ ».

B.2. Met de bestreden wet is de wetgever willen tegemoetkomen aan de vernietiging, bij het arrest nr. 84/2015 van het Hof van 11 juni 2015, van artikel 126 van de wet van 13 juni 2005 « betreffende de elektronische communicatie » (hierna : de wet van 13 juni 2005), zoals het was gewijzigd bij 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 » (*Parl. St.*, Kamer, 2015-2016, DOC 54-1567/001, p. 4).

B.3. Uit de parlementaire voorbereiding van de bestreden wet blijkt dat de wetgever zowel het voormelde arrest van het Hof nr. 84/2015 van 11 juni 2015 als het daaraan ten grondslag liggende arrest van het Hof van Justitie van de Europese Unie van 8 april 2014, in de gevoegde zaken *Digital Rights Ireland Ltd* (C-293/12*)* en *Kärntner Landesregierung e.a.* (C-594/12), waarbij het Hof van Justitie 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 » ongeldig heeft verklaard, grondig heeft onderzocht.

Het doel dat de wetgever met de bestreden wet nastreeft bestaat erin niet alleen terrorisme en kinderpornografie te bestrijden, maar ook de bewaarde gegevens te kunnen gebruiken in zeer veel verschillende situaties waarin die gegevens zowel het vertrekpunt als een fase van het strafonderzoek kunnen zijn (*Parl. St.*, Kamer, 2015-2016, DOC 54-1567/001, p. 6).

B.4. Uit de memorie van toelichting van de bestreden wet blijkt dat de wetgever een gerichte en gedifferentieerde bewaarplicht in het licht van de vooropgestelde doelstelling niet mogelijk heeft geacht en ervoor heeft gekozen om de algemene en ongedifferentieerde bewaarplicht met strikte waarborgen te omringen, zowel op het vlak van de beveiliging van de bewaring, als op het vlak van de toegang, zodat de inmenging in het recht op de bescherming van de persoonlijke levenssfeer tot een minimum zou worden beperkt. In dat verband is erop gewezen dat een a priori differentiatie naar personen, periodes en geografische zones eenvoudigweg niet mogelijk zou zijn (*ibid.*, pp. 10-18).

Ten gronde

B.5. Het enige middel in de zaken nrs. 6590 en 6597 is afgeleid uit de schending, door de bestreden wet, 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.

B.6.1. De « Ordre des barreaux francophones et germanophone », verzoekende partij in de zaak nr. 6590, verwijt de bestreden wet dat zij de gebruikers van telecommunicatie- of elektronische-communicatiediensten die aan het beroepsgeheim zijn onderworpen, onder wie met name de advocaten, en de andere gebruikers van die diensten op identieke wijze behandelt. Die verzoekende partij stelt vast dat de wet eveneens een veralgemeende verplichting tot registratie en bewaring van bepaalde metagegevens inhoudt, die het mogelijk maken te bepalen of een advocaat werd geraadpleegd door een natuurlijke persoon of rechtspersoon, die advocaat te identificeren, zijn gesprekspartners en in het bijzonder zijn cliënten te identificeren, alsook de datum en het uur van de communicatie te bepalen. Die veralgemeende verplichting wordt opgelegd aan alle aanbieders van aan het publiek aangeboden vaste telefoniediensten, mobiele telefoniediensten, internettoegangdiensten, internet-e-maildiensten, internettelefoniediensten en openbare elektronische communicatienetwerken.

B.6.2. De verzoekende partij in de zaak nr. 6590 klaagt eveneens aan dat de bestreden wet in een veralgemeende verplichting tot het bewaren van gegevens voorziet zonder een onderscheid tussen de rechtzoekenden te maken naargelang zij al dan niet het voorwerp uitmaken van een onderzoeks- of vervolgingsmaatregel wegens feiten die aanleiding kunnen

geven tot strafrechtelijke veroordelingen. Zij voert eveneens aan dat de in de wet bedoelde categorieën van gegevens uitermate ruim en gevarieerd zijn, in zoverre zij betrekking hebben op de gegevens ter identificatie van de gebruiker of de abonnee en de communicatiemiddelen, de gegevens met betrekking tot de toegang tot en de verbinding van de eindapparatuur met het netwerk en met de dienst en met betrekking tot de plaats van die apparatuur, inclusief het netwerkaansluitpunt, alsook de communicatiegegevens, ook al wordt de inhoud ervan daarentegen uitgesloten.

B.7.1. De verzoekende partijen in de zaak nr. 6597 verwijten de bestreden wet dat zij de gebruikers van telecommunicatie- of elektronische communicatiediensten die aan het beroepsgeheim zijn onderworpen, onder wie met name de boekhoudkundige en fiscale professionals, en de andere gebruikers van die diensten op identieke wijze behandelt, zonder rekening te houden met het bijzondere statuut van de boekhoudkundige en fiscale professionals, het fundamentele karakter van het beroepsgeheim waaraan zij onderworpen zijn en de noodzakelijke vertrouwensrelatie tussen hen en hun cliënten.

B.7.2. Zij verwijten de bestreden wet eveneens dat zij de rechtzoekenden die het voorwerp uitmaken van onderzoeks- of vervolgingsmaatregelen wegens feiten die mogelijk beantwoorden aan de doeleinden van de bewaring van de in het geding zijnde elektronische gegevens, en die welke niet het voorwerp van dergelijke maatregelen uitmaken, op identieke wijze behandelt.

B.8.1. Het eerste middel in de zaak nr. 6599 is afgeleid uit de schending van de artikelen 10, 11, 12, 15, 22 en 29 van de Grondwet, al dan niet in samenhang gelezen met de artikelen 5, 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 en 52 van het Handvest van de grondrechten van de Europese Unie, met artikel 17 van het Internationaal Verdrag inzake burgerrechten en politieke rechten, met het algemene beginsel van rechtszekerheid, van evenredigheid, van het recht op informationele zelfbeschikking en met artikel 5, lid 4, van het Verdrag betreffende de Europese Unie.

B.8.2. De vzw « Liga voor Mensenrechten » en de vzw « Ligue des Droits de l'Homme » (intussen « Ligue des droits humains » geworden), verzoekende partijen in de zaak nr. 6599, verwijten de bestreden wet dat zij in een algemene verplichting tot het bewaren van gegevens

voorziet, hetgeen de operatoren en de aanbieders van openbare telefoniediensten (met inbegrip van internettelefonie), van internettoegang en van e-mail over het internet, alsook de aanbieders van openbare elektronische communicatienetwerken verplicht om de verkeersgegevens betreffende vaste telefonie, mobiele telefonie en internettelefonie en de gegevens betreffende internettoegang *de facto* voor alle - verdachte of niet-verdachte - Belgen gedurende twaalf maanden te bewaren en ter beschikking te stellen van de politie en van het gerecht, van de inlichtingen- en veiligheidsdiensten, van de hulpdiensten, van de Cel Vermiste Personen en van de Ombudsdienst voor telecommunicatie.

B.9.1. Het eerste middel in de zaak nr. 6601 is afgeleid uit de schending, door de bestreden wet, van artikel 8 van het Europees Verdrag voor de rechten van de mens, van de artikelen 7, 8, 11, lid 1, en 52 van het Handvest van de grondrechten van de Europese Unie, van de artikelen 10, 11, 19 en 22 van de Grondwet, van artikel 2, a), van de richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 « betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens », alsook van de artikelen 1, 2, 3, 5, 6, 9 en 15 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).

B.9.2. De verzoekende partijen in de zaak nr. 6601 zijn natuurlijke personen die in België wonen en verschillende elektronischecommunicatiediensten gebruiken in het kader van een met een operator gesloten overeenkomst. In het eerste onderdeel van het eerste middel klagen zij aan dat de bestreden wet voorziet in een algemene en ongedifferentieerde verplichting tot het bewaren van identificatie-, verbindings- en lokalisatiegegevens en van persoonlijke communicatiegegevens ten laste van de aanbieders van telefoniediensten, ook via internet, van internettoegang en van e-mail over het internet, ten laste van de operatoren die openbare elektronische communicatienetwerken aanbieden en ten laste van de operatoren die een van die diensten aanbieden.

B.10. Rekening houdend met de onderlinge samenhang ervan, worden de in de diverse zaken aangevoerde middelen samen onderzocht.

B.11.1. Rekening houdend met, enerzijds, de verschillen in zienswijze, tussen de verzoekende partijen en de Ministerraad, over de interpretatie die moet worden gegeven aan meerdere bepalingen die het Hof in zijn toetsing van de bestreden wet dient te betrekken, inzonderheid artikel 15, lid 1, van de richtlijn 2002/58/EG en de artikelen 7, 8, 11 en 52 van het Handvest van de grondrechten van de Europese Unie, en, anderzijds, de door de Ministerraad gegeven verklaringen om de verenigbaarheid van de bestreden wet met de door de verzoekende partijen aangevoerde referentienormen te verantwoorden, heeft het Hof, bij zijn arrest nr. 96/2018 van 19 juli 2018, aan het Hof van Justitie van de Europese Unie de volgende drie prejudiciële vragen gesteld :

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

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

3. Zou het Grondwettelijk Hof, indien het op grond van het antwoord verstrekt op de eerste of de tweede prejudiciële vraag tot de conclusie zou komen dat de bestreden wet één of meer van de uit de in die vragen vermelde bepalingen voortvloeiende verplichtingen schendt, de gevolgen van de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de

gegevens in de sector van de elektronische communicatie tijdelijk kunnen handhaven teneinde rechtsonzekerheid te voorkomen en het mogelijk te maken dat de voorheen verzamelde en bewaarde gegevens alsnog kunnen gebruikt worden voor de door de wet beoogde doeleinden ? ».

B.11.2. Artikel 15, lid 1, van de richtlijn 2002/58/EG bepaalt :

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

B.11.3. Het Hof heeft ook beslist het onderzoek van de zaken op te schorten totdat het Hof van Justitie uitspraak zal hebben gedaan in de zaken *Ministerio Fiscal* (C-207/16) en *Privacy International t. Secretary of State for Foreign and Commonwealth Affairs e.a.* (C-623/17).

B.12. Bij zijn arrest van 2 oktober 2018, in zake *Ministerio Fiscal* (C-207/16), heeft het Hof van Justitie in grote kamer geoordeeld dat artikel 15, lid 1, van de richtlijn 2002/58/EG, gelezen in samenhang met de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie, aldus moet worden uitgelegd dat de toegang van overheidsinstanties tot de identificatiegegevens van houders van met een gestolen mobiele telefoon geactiveerde simkaarten – zoals hun naam, voornaam en, in voorkomend geval, adres – geen zodanig ernstige inmenging in de door die artikelen van het Handvest gewaarborgde grondrechten van laatstgenoemden oplevert dat die toegang – op het gebied van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten - moet worden beperkt tot de bestrijding van zware criminaliteit . Dat arrest steunt op volgende overwegingen :

« *Ten gronde*

48. Met zijn twee vragen, die samen moeten worden onderzocht, wenst de verwijzende rechter in wezen te vernemen of artikel 15, lid 1, van richtlijn 2002/58, gelezen in samenhang

met de artikelen 7 en 8 van het Handvest, aldus moet worden uitgelegd dat de toegang van overheidsinstanties tot de identificatiegegevens van de houders van met een gestolen mobiele telefoon geactiveerde simkaarten – zoals hun naam, voornaam en, in voorkomend geval, adres – een zodanig ernstige inmenging in de door die artikelen van het Handvest gewaarborgde grondrechten van deze laatsten vormt dat die toegang, wat het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten betreft, zou moeten worden beperkt tot de bestrijding van zware criminaliteit en, zo ja, aan de hand van welke criteria de ernst van het betrokken delict moet worden beoordeeld.

49. In dit verband blijkt uit de verwijzingsbeslissing dat, zoals de advocaat-generaal in punt 38 van zijn conclusie in wezen heeft opgemerkt, het verzoek om een prejudiciële beslissing er niet toe strekt om uit te maken of de aanbieders van elektronische-communicatiediensten de in het hoofdgeding aan de orde zijnde persoonsgegevens hebben bewaard met inachtneming van de voorwaarden van artikel 15, lid 1, van richtlijn 2002/58, gelezen in samenhang met de artikelen 7 en 8 van het Handvest. Zoals uit punt 46 van het onderhavige arrest blijkt, betreft het verzoek uitsluitend de vraag of en in welke mate het doel dat met de in het hoofdgeding aan de orde zijnde nationale regeling wordt nagestreefd, kan rechtvaardigen dat overheidsinstanties zoals de gerechtelijke politie toegang hebben tot dergelijke gegevens, en gaat het verzoek niet over de andere toegangsvoorwaarden die uit voormeld artikel 15, lid 1, voortvloeien.

50. De verwijzende rechter vraagt zich in het bijzonder af welke elementen in aanmerking moeten worden genomen bij de beoordeling of delicten waarvoor politiediensten in het kader van een onderzoek toegang kan worden verleend tot persoonsgegevens die door aanbieders van elektronische-communicatiediensten worden bewaard, voldoende ernstig zijn om de inmenging die een dergelijke toegang betekent in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten, zoals uitgelegd door het Hof in zijn arrest van 8 april 2014, *Digital Rights Ireland e.a.* (C-293/12 en C-594/12, EU:C:2014:238), en in het arrest *Tele2 Sverige en Watson e.a.*, te rechtvaardigen.

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

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

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

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

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

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

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

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

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

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

periode met bepaalde personen is gecommuniceerd. Uit die gegevens kunnen dus geen nauwkeurige conclusies over het privéleven van de betrokken personen worden getrokken.

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

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

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

In het dictum van het arrest heeft het Hof van Justitie verklaard voor recht :

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

B.13. Bij zijn arrest van 6 oktober 2020, in zake *Privacy International* (C-623/17), uitgesproken in grote kamer, heeft het Hof van Justitie geoordeeld dat artikel 15, lid 1, van de richtlijn 2002/58/EG, gelezen in het licht van artikel 4, lid 2, van het Verdrag betreffende de Europese Unie en de artikelen 7, 8, 11 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, 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. Dat arrest steunt op volgende overwegingen :

« *Tweede vraag*

50. Met zijn tweede vraag wenst de verwijzende rechter in wezen te vernemen of artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van artikel 4, lid 2, VEU en de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, aldus moet worden uitgelegd dat het zich verzet tegen een nationale regeling op grond waarvan een overheidsorgaan ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten kan opleggen.

51. Om te beginnen zij eraan herinnerd dat section 94 van de wet van 1984 volgens de informatie in het verzoek om een prejudiciële beslissing de Secretary of State de mogelijkheid biedt om aanbieders van elektronischecommunicatiediensten door middel van aanwijzingen de verplichting op te leggen om bulkcommunicatiegegevens door te zenden aan de veiligheids- en inlichtingendiensten, indien hij dit noodzakelijk acht in het belang van de nationale veiligheid of de betrekkingen met een buitenlandse regering. Deze gegevens omvatten verkeers- en locatiegegevens alsmede informatie over de gebruikte diensten, in de zin van section 21, leden 4 en 6, RIPA. Deze laatste bepaling ziet onder meer op de gegevens die nodig zijn om de bron en de bestemming van een communicatie te identificeren, de datum, het tijdstip, de duur en de aard van die communicatie te bepalen, het gebruikte materiaal te identificeren en de eindapparatuur en de communicatie te lokaliseren. Tot die gegevens behoren met name de naam en het adres van de gebruiker, het telefoonnummer van de beller en het gebelde nummer, het bron- en het doel-IP-adres en de adressen van de bezochte websites.

52. Een dergelijke verstrekking van gegevens door middel van doorzending betreft alle gebruikers van elektronischecommunicatiemiddelen, zonder dat wordt gespecificeerd of die doorzending wel of niet in real time moet plaatsvinden. De doorgezonden gegevens worden volgens de informatie in het verzoek om een prejudiciële beslissing door de veiligheids- en inlichtingendiensten bewaard en blijven ter beschikking van deze diensten ten behoeve van hun activiteiten, net zoals de andere databases van deze diensten. Met name kunnen de aldus verworven gegevens, waarop automatische bulkverwerking en -analyse worden toegepast, worden onderworpen aan kruiscontroles met andere databases die verschillende categorieën bulkpersoonsgegevens bevatten, of buiten die diensten worden bekendgemaakt, ook aan derde staten. Tot slot is voor die bewerkingen geen voorafgaande toestemming van een rechterlijke instantie of een onafhankelijk bestuursorgaan vereist en geldt er geen verplichting om de betrokkenen te informeren.

53. Zoals met name uit de overwegingen 6 en 7 van richtlijn 2002/58 volgt, heeft deze richtlijn tot doel om de gebruikers van elektronischecommunicatiediensten te beschermen tegen de gevaren die de nieuwe technologieën en, met name, de steeds grotere mogelijkheden van geautomatiseerde opslag en verwerking van gegevens voor de persoonsgegevens en de persoonlijke levenssfeer van die gebruikers meebrengen. Zoals in overweging 2 van richtlijn

2002/58 wordt verklaard, beoogt deze richtlijn in het bijzonder de volledige eerbiediging van de in de artikelen 7 en 8 van het Handvest bedoelde rechten te waarborgen. Dienaangaande blijkt uit de toelichting bij het voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie [COM(2000) 385 definitief], waaruit richtlijn 2002/58 is voortgekomen, dat de Uniewetgever heeft willen ‘ zorgen voor een hoge mate van bescherming van de persoonsgegevens en van de persoonlijke levenssfeer voor alle elektronischecommunicatiediensten, ongeacht de gebruikte technologie ’.

54. Daartoe bepaalt artikel 5, lid 1, van richtlijn 2002/58 dat ‘ [d]e lidstaten […] via nationale wetgeving het vertrouwelijke karakter van de communicatie en de daarmee verband houdende verkeersgegevens via openbare communicatienetwerken en via openbare elektronischecommunicatiediensten [garanderen] ’. In diezelfde bepaling wordt benadrukt dat de lidstaten ‘ met name het afluisteren, aftappen, opslaan of anderszins onderscheppen of controleren van de communicatie en de daarmee verband houdende verkeersgegevens door anderen dan de gebruikers [verbieden], indien de betrokken gebruikers daarin niet hebben toegestemd, tenzij dat bij wet is toegestaan overeenkomstig artikel 15, lid 1 ’, en gepreciseerd dat ‘ [d]it lid […] de technische opslag die nodig is voor het overbrengen van informatie onverlet [laat], onverminderd het vertrouwelijkheidsbeginsel ’.

55. Artikel 5, lid 1, legt aldus het beginsel van vertrouwelijkheid van zowel de elektronische communicatie als de daarmee verband houdende verkeersgegevens vast en impliceert met name dat het anderen dan de gebruikers in beginsel moet worden verboden die communicatie en die gegevens op te slaan, indien de gebruikers daarin niet hebben toegestemd. Gelet op haar algemene bewoordingen, bestrijkt die bepaling noodzakelijkerwijs elke voor andere doeleinden dan het overbrengen van informatie uitgevoerde bewerking die derden in staat stelt om kennis te nemen van de communicatie en de daarmee verband houdende gegevens.

56. Het in artikel 5, lid 1, van richtlijn 2002/58 neergelegde verbod op het onderscheppen van de communicatie en de daarmee verband houdende verkeersgegevens omvat dus elke vorm van beschikbaarstelling door aanbieders van elektronischecommunicatiediensten van verkeers- en locatiegegevens aan overheidsinstanties, zoals veiligheids- en inlichtingendiensten, alsmede de bewaring van de beschikbaar gestelde gegevens door die instanties, ongeacht het latere gebruik van die gegevens.

57. Met de vaststelling van richtlijn 2002/58 heeft de Uniewetgever dus de in de artikelen 7 en 8 van het Handvest neergelegde rechten geconcretiseerd, zodat de gebruikers van elektronischecommunicatiemiddelen in beginsel erop mogen vertrouwen dat hun communicatie en de daarmee verband houdende gegevens anoniem blijven en niet mogen worden vastgelegd, tenzij zij daarin hebben toegestemd (arrest van 6 oktober 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 en C-520/18, punt 109).

58. Artikel 15, lid 1, van richtlijn staat 2002/58 staat de lidstaten echter toe, te voorzien in uitzonderingen op de in artikel 5, lid 1, van deze richtlijn geformuleerde principeverplichting om de vertrouwelijkheid van de persoonsgegevens te waarborgen, en op de met name in de artikelen 6 en 9 van deze richtlijn vermelde overeenkomstige verplichtingen, indien dat in een democratische samenleving een noodzakelijke, redelijke en proportionele maatregel vormt om de nationale veiligheid, de landsverdediging en de openbare veiligheid te waarborgen, of om strafbare feiten of onbevoegd gebruik van het elektronischecommunicatiesysteem te

voorkomen, te onderzoeken, op te sporen en te vervolgen. Daartoe kunnen de lidstaten onder meer wettelijke maatregelen treffen om gegevens gedurende een beperkte periode te bewaren indien dat om een van die redenen gerechtvaardigd is.

59. De mogelijkheid om af te wijken van de in de artikelen 5, 6 en 9 van richtlijn 2002/58 vastgestelde rechten en verplichtingen kan echter niet rechtvaardigen dat de uitzondering op de principeverplichting tot waarborging van de vertrouwelijkheid van de elektronische communicatie en van de daarmee verband houdende gegevens en, in het bijzonder, op het verbod om deze gegevens op te slaan de regel wordt (zie in die zin arresten van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punten 89 en 104, en 6 oktober 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 en C-520/18, punt 111).

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

61. Diezelfde vragen rijzen ook voor andere vormen van gegevensverwerking, zoals de doorzending van gegevens aan anderen dan de gebruikers of de toegang tot die gegevens met het oog op het gebruik ervan [zie naar analogie advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punten 122 en 123 en aldaar aangehaalde rechtspraak].

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

63. De in de artikelen 7, 8 en 11 van het Handvest verankerde rechten hebben echter geen absolute gelding, maar moeten worden beschouwd in relatie tot hun functie in de samenleving (zie in die zin arrest van 16 juli 2020, *Facebook Ireland en Schrems*, C-311/18, EU:C:2020:559, punt 172 en aldaar aangehaalde rechtspraak).

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

65. Hieraan dient te worden toegevoegd dat het vereiste dat elke beperking op de uitoefening van grondrechten bij wet wordt gesteld, inhoudt dat de rechtsgrond die de inmenging in die rechten toestaat, zelf de reikwijdte van de beperking op de uitoefening van het betrokken recht moet bepalen (arrest van 16 juli 2020, *Facebook Ireland en Schrems*, C-311/18, EU:C:2020:559, punt 175 en aldaar aangehaalde rechtspraak).

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

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

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

69. Wat de vraag betreft of een nationale regeling als die van het hoofdgeding voldoet aan de vereisten van artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, dient te worden opgemerkt dat de doorzending van verkeers- en locatiegegevens aan anderen dan de gebruikers, zoals de veiligheids- en inlichtingendiensten, afwijkt van het vertrouwelijkheidsbeginsel. Wanneer die bewerking, zoals in casu, op algemene en ongedifferentieerde wijze wordt uitgevoerd, heeft zij tot gevolg dat de afwijking van de principeverplichting tot waarborging van de vertrouwelijkheid van de gegevens de regel wordt, terwijl het bij richtlijn 2002/58 ingevoerde stelsel eist dat die afwijking de uitzondering blijft.

70. Voorts vormt de doorzending van verkeers- en locatiegegevens aan een derde volgens vaste rechtspraak van het Hof een inmenging in de in de artikelen 7 en 8 van het Handvest verankerde grondrechten, ongeacht het latere gebruik van die gegevens. In dit verband is het van weinig belang of de gegevens betreffende het privéleven al dan niet gevoelig zijn en of de betrokkenen door die inmenging enig nadeel hebben ondervonden [zie in die zin advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punten 124 en 126 en aldaar aangehaalde rechtspraak, en arrest van 6 oktober 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 en C-520/18, punten 115 en 116].

71. De inmenging die de doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten vormt in het door artikel 7 van het Handvest gewaarborgde recht, moet als bijzonder ernstig worden beschouwd, met name gelet op het gevoelige karakter van de informatie die deze gegevens kunnen prijsgeven, en op de mogelijkheid om aan de hand van deze gegevens het profiel van de betrokken personen te bepalen, informatie die even gevoelig is als de inhoud zelf van de communicatie. Die inmenging kan bovendien bij de betrokken personen het gevoel opwekken dat hun privéleven constant in de gaten wordt gehouden (zie naar analogie arresten van 8 april 2014, *Digital Rights Ireland e.a.*, C-293/12 en C-594/12, EU:C:2014:238, punten 27 en 37, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punten 99 en 100).

72. Tevens moet worden opgemerkt dat de doorzending van verkeers- en locatiegegevens aan overheidsinstanties voor veiligheidsdoeleinden op zichzelf afbreuk kan doen aan het in artikel 7 van het Handvest verankerde recht op eerbiediging van communicatie, en de gebruikers van elektronischecommunicatiemiddelen kan ontmoedigen om hun door artikel 11 van het Handvest gewaarborgde vrijheid van meningsuiting uit te oefenen. Dit laatste geldt in het bijzonder voor personen van wie de communicatie naar nationaal recht onder het beroepsgeheim valt, en voor klokkenluiders van wie de activiteiten worden beschermd door richtlijn (EU) 2019/1937 van het Europees Parlement en de Raad van 23 oktober 2019 inzake de bescherming van personen die inbreuken op het Unierecht melden (PB 2019, L 305, blz. 17). Dat ontmoedigende effect is bovendien des te ernstiger omdat de bewaarde gegevens talrijk en gevarieerd zijn (zie in die zin arresten van 8 april 2014, *Digital Rights Ireland e.a.*, C-293/12 en C-594/12, EU:C:2014:238, punt 28; 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 101, en 6 oktober 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 en C-520/18, punt 118).

73. Ten slotte is het zo dat, gelet op de aanzienlijke hoeveelheid verkeers- en locatiegegevens die continu kunnen worden bewaard op grond van een algemene bewaringsmaatregel, en op het gevoelige karakter van de informatie die deze gegevens kunnen prijsgeven, het enkele feit dat die gegevens door aanbieders van

elektronischecommunicatiediensten worden bewaard, risico's van misbruik en onrechtmatige toegang tot de gegevens inhoudt.

74. Wat de doelstellingen betreft die dergelijke inmengingen kunnen rechtvaardigen, meer in het bijzonder de in het hoofdgeding aan de orde zijnde doelstelling van bescherming van de nationale veiligheid, moet om te beginnen worden opgemerkt dat de nationale veiligheid volgens artikel 4, lid 2, VEU tot de uitsluitende verantwoordelijkheid van elke lidstaat behoort. Deze verantwoordelijkheid strookt met het grote belang dat wordt gehecht aan de bescherming van de essentiële staatsfuncties en de fundamentele belangen van de samenleving, en omvat het voorkomen en bestrijden van activiteiten die de fundamentele constitutionele, politieke, economische of sociale structuren van een land ernstig kunnen destabiliseren en, met name, een rechtstreekse bedreiging kunnen vormen voor de samenleving, de bevolking of de staat als zodanig, zoals terroristische activiteiten (arrest van 6 oktober 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 en C-520/18, punt 135).

75. Het belang van de doelstelling van bescherming van de nationale veiligheid, gelezen in het licht van artikel 4, lid 2, VEU, overstijgt dat van de andere doelstellingen die worden genoemd in artikel 15, lid 1, van richtlijn 2002/58, met name de doelstellingen van bestrijding van – zelfs ernstige – criminaliteit in het algemeen, en van bescherming van de openbare veiligheid. Bedreigingen als die waaraan in het voorgaande punt wordt gerefereerd, verschillen door hun aard en hun bijzondere ernst immers van het algemene risico dat zich – zelfs ernstige – spanningen of wanordelijkheden zullen voordoen die de openbare veiligheid ondermijnen. Mits aan de overige in artikel 52, lid 1, van het Handvest geformuleerde vereisten wordt voldaan, kan de doelstelling van bescherming van de nationale veiligheid derhalve maatregelen rechtvaardigen die ernstigere inmengingen in de grondrechten met zich brengen dan die welke door die andere doelstellingen zouden kunnen worden gerechtvaardigd (arrest van 6 oktober 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 en C-520/18, punt 136).

76. Om te voldoen aan het in punt 67 van het onderhavige arrest in herinnering gebrachte evenredigheidsvereiste, dat verlangt dat uitzonderingen op de bescherming van persoonsgegevens en beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven, dient een nationale regeling die een inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten met zich brengt, evenwel in overeenstemming te zijn met de eisen die voortvloeien uit de in de punten 65, 67 en 68 van het onderhavige arrest aangehaalde rechtspraak.

77. Wat in het bijzonder de toegang van een autoriteit tot persoonsgegevens betreft, mag een regeling zich niet ertoe beperken te eisen dat de toegang tot deze gegevens wordt verleend voor het met die regeling beoogde doel, maar moet zij ook de materiële en procedurele voorwaarden voor dit gebruik bepalen [zie naar analogie advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 192 en aldaar aangehaalde rechtspraak].

78. Een nationale regeling die de toegang tot locatie- en verkeersgegevens regelt, moet dus aan de hand van objectieve criteria bepalen in welke omstandigheden en onder welke voorwaarden aan de bevoegde nationale autoriteiten toegang tot de betrokken gegevens moet worden verleend, aangezien een algemene toegang tot alle bewaarde gegevens, los van enig – zelfs maar indirect – verband met het nagestreefde doel, niet kan worden geacht tot het strikt noodzakelijke te zijn beperkt, (zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 119 en aldaar aangehaalde rechtspraak).

79. Die vereisten zijn *a fortiori* van toepassing op een wettelijke maatregel als aan de orde in het hoofdgeding, op grond waarvan de bevoegde nationale autoriteit aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten kan opleggen. Een dergelijke doorzending heeft immers tot gevolg dat die gegevens ter beschikking worden gesteld aan overheidsinstanties [zie naar analogie advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 212].

80. Het feit dat de doorzending van de verkeers- en locatiegegevens geschiedt op algemene en ongedifferentieerde wijze, betekent dat die doorzending algemeen alle personen betreft die gebruikmaken van elektronischecommunicatiediensten, dat wil zeggen zelfs personen voor wie er geen enkele aanwijzing bestaat dat hun gedrag – zelfs maar indirect of van ver – een verband vertoont met de doelstelling van bescherming van de nationale veiligheid. Met name is er geen enkel verband vereist tussen de gegevens die moeten worden doorgezonden en een bedreiging van de nationale veiligheid (zie in die zin arresten van 8 april 2014, *Digital Rights Ireland e.a.*, C-293/12 en C-594/12, EU:C:2014:238, punten 57 en 58, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 105). Gelet op het feit dat de doorzending van dergelijke gegevens aan overheidsinstanties – overeenkomstig de vaststelling in punt 79 van het onderhavige arrest – gelijkstaat aan het verlenen van toegang tot deze gegevens, moet worden geoordeeld dat een regeling die de algemene en ongedifferentieerde doorzending van gegevens aan overheidsinstanties mogelijk maakt, een algemene toegang tot die gegevens impliceert.

81. Daaruit volgt dat een nationale regeling die aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten oplegt, verder gaat dan strikt noodzakelijk is en niet kan worden beschouwd als een regeling die in een democratische samenleving gerechtvaardigd is, zoals artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, eist.

82. Gelet op een en ander moet op de tweede vraag worden geantwoord dat artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van artikel 4, lid 2, VEU en de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, aldus moet worden uitgelegd dat het zich verzet tegen een nationale regeling op grond waarvan een overheidsorgaan ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten kan opleggen ».

In het dictum van het arrest heeft het Hof van Justitie voor recht verklaard :

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

doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten kan opleggen ».

B.14. Bij zijn arrest van 6 oktober 2020, *La Quadrature du Net e.a.* (C-511/18, C-512/18 en C-520/18), uitgesproken in grote kamer, heeft het Hof van Justitie de eerste twee door het Hof bij zijn arrest nr. 96/2018 gestelde vragen als volgt beantwoord :

« *Eerste vraag in de zaken C-511/18 en C-512/18 en eerste en tweede vraag in zaak C-520/18*

81. Met de eerste vraag in de zaken C-511/18 en C-512/18 en de eerste en de tweede vraag in zaak C-520/18, die samen moeten worden onderzocht, wensen de verwijzende rechters in wezen te vernemen of artikel 15, lid 1, van richtlijn 2002/58 aldus moet worden uitgelegd dat het zich verzet tegen een nationale regeling die voor de in deze bepaling genoemde doeleinden aan aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens oplegt.

[…]

Uitlegging van artikel 15, lid 1, van richtlijn 2002/58

105. Vooraf zij eraan herinnerd dat volgens vaste rechtspraak bij de uitlegging van een Unierechtelijke bepaling niet alleen rekening moet worden gehouden met de bewoordingen ervan, maar ook met de context van die bepaling, de doelstellingen van de regeling waarvan zij deel uitmaakt en, met name, de ontstaansgeschiedenis van die regeling (zie in die zin arrest van 17 april 2018, *Egenberger*, C-414/16, EU:C:2018:257, punt 44).

106. Zoals met name uit de overwegingen 6 en 7 van richtlijn 2002/58 volgt, heeft deze richtlijn tot doel om de gebruikers van elektronischecommunicatiediensten te beschermen tegen de gevaren die de nieuwe technologieën en, met name, de steeds grotere mogelijkheden van geautomatiseerde opslag en verwerking van gegevens voor de persoonsgegevens en de persoonlijke levenssfeer van die gebruikers meebrengen. Zoals in overweging 2 van richtlijn 2002/58 wordt verklaard, beoogt deze richtlijn in het bijzonder de volledige eerbiediging van de in de artikelen 7 en 8 van het Handvest bedoelde rechten te waarborgen. Dienaangaande blijkt uit de toelichting bij het voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie [COM(2000) 385 definitief], waaruit richtlijn 2002/58 is voortgekomen, dat de Uniewetgever heeft willen ‘ zorgen voor een hoge mate van bescherming van de persoonsgegevens en van de persoonlijke levenssfeer voor alle elektronischecommunicatiediensten, ongeacht de gebruikte technologie ’.

107. Daartoe legt artikel 5, lid 1, van richtlijn 2002/58 het beginsel van vertrouwelijkheid van zowel de elektronische communicatie als de daarmee verband houdende verkeersgegevens vast en impliceert het met name dat het anderen dan de gebruikers in beginsel moet worden verboden die communicatie en die gegevens op te slaan, indien de gebruikers daarin niet hebben toegestemd.

108. Wat in het bijzonder de verwerking en de opslag van verkeersgegevens door aanbieders van elektronischecommunicatiediensten betreft, blijkt uit artikel 6 en de overwegingen 22 en 26 van richtlijn 2002/58 dat een dergelijke verwerking slechts is toegestaan voor zover en zolang dat nodig is voor de marketing en de facturering van de diensten en voor de levering van diensten met toegevoegde waarde. Zodra die periode is verstreken, moeten de verwerkte en opgeslagen gegevens worden gewist of geanonimiseerd. Wat de andere locatiegegevens dan de verkeersgegevens betreft, bepaalt artikel 9, lid 1, van richtlijn 2002/58 dat die gegevens slechts onder bepaalde voorwaarden mogen worden verwerkt nadat zij zijn geanonimiseerd of wanneer de gebruikers of abonnees daarvoor hun toestemming hebben gegeven (arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 86 en aldaar aangehaalde rechtspraak).

109. Met de vaststelling van richtlijn 2002/58 heeft de Uniewetgever dus de in de artikelen 7 en 8 van het Handvest neergelegde rechten geconcretiseerd, zodat de gebruikers van elektronischecommunicatiemiddelen in beginsel erop mogen vertrouwen dat hun communicatie en de daarmee verband houdende gegevens anoniem blijven en niet mogen worden vastgelegd, tenzij zij daarin hebben toegestemd.

110. Artikel 15, lid 1, van richtlijn staat 2002/58 staat de lidstaten echter toe, te voorzien in uitzonderingen op de in artikel 5, lid 1, van deze richtlijn geformuleerde principeverplichting om de vertrouwelijkheid van de persoonsgegevens te waarborgen, en op de met name in de artikelen 6 en 9 van deze richtlijn vermelde overeenkomstige verplichtingen, indien dat in een democratische samenleving een noodzakelijke, redelijke en proportionele maatregel vormt om de nationale veiligheid, de landsverdediging en de openbare veiligheid te waarborgen, of om strafbare feiten of onbevoegd gebruik van het elektronischecommunicatiesysteem te voorkomen, te onderzoeken, op te sporen en te vervolgen. Daartoe kunnen de lidstaten onder meer wettelijke maatregelen treffen om gegevens gedurende een beperkte periode te bewaren indien dat om een van die redenen gerechtvaardigd is.

111. De mogelijkheid om af te wijken van de in de artikelen 5, 6 en 9 van richtlijn 2002/58 vastgestelde rechten en verplichtingen kan echter niet rechtvaardigen dat de uitzondering op de principeverplichting tot waarborging van de vertrouwelijkheid van de elektronische communicatie en van de daarmee verband houdende gegevens en, in het bijzonder, op het verbod om deze gegevens op te slaan de regel wordt (zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punten 89 en 104).

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

113. Bovendien volgt uit artikel 15, lid 1, derde zin, van richtlijn 2002/58 dat de lidstaten slechts wettelijke maatregelen ter beperking van de omvang van de in de artikelen 5, 6 en 9 van deze richtlijn bedoelde rechten en plichten mogen nemen voor zover deze maatregelen in overeenstemming zijn met de algemene beginselen van het Unierecht, waaronder het

evenredigheidsbeginsel, en met de door het Handvest gewaarborgde grondrechten. In dit verband heeft het Hof reeds geoordeeld dat de door een lidstaat bij een nationale regeling aan aanbieders van elektronischecommunicatiediensten opgelegde verplichting om de verkeersgegevens te bewaren teneinde de bevoegde nationale autoriteiten in voorkomend geval toegang tot die gegevens te kunnen geven, niet alleen vragen doet rijzen betreffende de eerbiediging van de artikelen 7 en 8 van het Handvest, die betrekking hebben op, respectievelijk, de bescherming van het privéleven en de bescherming van persoonsgegevens, maar ook betreffende de eerbiediging van artikel 11 van het Handvest, dat betrekking heeft op de vrijheid van meningsuiting (zie in die zin arresten van 8 april 2014, *Digital Rights Ireland e.a.*, C-293/12 en C-594/12, EU:C:2014:238, punten 25 en 70, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punten 91 en 92 en aldaar aangehaalde rechtspraak).

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

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

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

117. Deze conclusie is des te meer gerechtvaardigd daar verkeers- en locatiegegevens informatie kunnen prijsgeven over een groot aantal aspecten van het privéleven van de betrokken personen, waaronder ook gevoelige informatie, zoals seksuele geaardheid, politieke opvattingen, religieuze, filosofische, maatschappelijke of andersoortige overtuigingen en gezondheid, terwijl dergelijke gegevens bovendien in het Unierecht bijzondere bescherming genieten. Uit deze gegevens, in hun geheel beschouwd, kunnen zeer precieze conclusies worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere

verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren. In het bijzonder kan aan de hand van deze gegevens het profiel van de betrokken personen worden bepaald, informatie die vanuit het oogpunt van het recht op bescherming van het privéleven even gevoelig is als de inhoud zelf van de communicatie (zie in die zin arresten van 8 april 2014, *Digital Rights*, C-293/12 en C-594/12, EU:C:2014:238, punt 27, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 99).

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

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

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

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

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

123. Zo heeft ingevolge artikel 6 van het Handvest, waaraan de Conseil d'État en het Grondwettelijk Hof refereren, eenieder niet alleen recht op vrijheid, maar ook op veiligheid, en waarborgt deze bepaling rechten die overeenstemmen met die welke worden gewaarborgd door

artikel 5 EVRM (zie in die zin arresten van 15 februari 2016, *N.*, C-601/15 PPU, EU:C:2016:84, punt 47; 28 juli 2016, *JZ*, C-294/16 PPU, EU:C:2016:610, punt 48, en 19 september 2019, *Rayonna prokuratura Lom*, C-467/18, EU:C:2019:765, punt 42 en aldaar aangehaalde rechtspraak).

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

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

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

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

128. Het EHRM heeft namelijk geoordeeld dat de positieve verplichtingen die voortvloeien uit de artikelen 3 en 8 EVRM, waarin rechten zijn gewaarborgd die corresponderen met de in de artikelen 4 en 7 van het Handvest gewaarborgde rechten, met name impliceren dat materiële en procedurele bepalingen moeten worden vastgesteld en praktische maatregelen moeten worden genomen die het mogelijk maken om criminaliteit gericht tegen personen effectief te bestrijden door middel van doeltreffend onderzoek en doeltreffende vervolging, hetgeen des te belangrijker is wanneer het lichamelijke en geestelijke welzijn van een kind wordt bedreigd. De bevoegde autoriteiten dienen daarbij echter de wettelijk voorgeschreven procedures en de overige waarborgen die de omvang van de strafrechtelijke

onderzoeksbevoegdheden beperken, alsmede de overige vrijheden en rechten volledig in acht te nemen. Met name dient er volgens het EHRM een wettelijk kader te worden ingevoerd dat het mogelijk maakt de verschillende belangen en rechten die moeten worden beschermd, met elkaar te verzoenen (EHRM, 28 oktober 1998, *Osman t. Verenigd Koninkrijk*, CE:ECHR:1998:1028JUD002345294, §§ 115 en 116; 4 maart 2004, *M.C. t. Bulgarije*, CE:ECHR:2003:1204JUD003927298, § 151; 24 juni 2004, *Von Hannover t. Duitsland*, CE:ECHR:2004:0624JUD005932000, §§ 57 en 58, en 2 december 2008, *K.U. t. Finland*, CE:ECHR:2008:1202JUD 000287202, §§ 46, 48 en 49).

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

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

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

132. Om aan het evenredigheidsvereiste te voldoen, dient een regeling duidelijke en nauwkeurige regels te bevatten over de reikwijdte en de toepassing van de betrokken maatregel, zodat degenen van wie de persoonsgegevens aan de orde zijn, over voldoende waarborgen beschikken dat die gegevens doeltreffend worden beschermd tegen het risico van misbruik. Die regeling moet wettelijk verbindend zijn naar intern recht en in het bijzonder aangeven in welke omstandigheden en onder welke voorwaarden een maatregel die voorziet in de verwerking van dergelijke gegevens kan worden genomen, en aldus waarborgen dat de inmenging tot het strikt noodzakelijke wordt beperkt. De noodzaak om over dergelijke waarborgen te beschikken is des te groter wanneer de persoonsgegevens op geautomatiseerde wijze worden verwerkt, met name wanneer er een aanzienlijk risico bestaat dat deze gegevens op onrechtmatige wijze zullen worden geraadpleegd. Deze overwegingen gelden in het bijzonder wanneer het gaat om de bescherming van een bijzondere categorie persoonsgegevens, te weten gevoelige gegevens [zie

in die zin arresten van 8 april 2014, *Digital Rights Ireland e.a.*, C-293/12 en C-594/12, EU:C:2014:238, punten 54 en 55, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 117; advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 141].

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

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

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

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

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

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

op alle gebruikers van elektronischecommunicatiemiddelen, zonder dat er op het eerste gezicht enig verband in de zin van de in punt 133 van het onderhavige arrest bedoelde rechtspraak tussen die gebruikers en een bedreiging voor de nationale veiligheid van de betrokken lidstaat lijkt te bestaan, geoordeeld moet worden dat het bestaan van een dergelijke bedreiging op zichzelf dat verband aantoont.

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

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

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

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

141. Een nationale regeling die voorziet in de algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens ten behoeve van de bestrijding van zware criminaliteit, gaat verder dan strikt noodzakelijk is en kan niet worden beschouwd als een regeling die in een democratische samenleving gerechtvaardigd is, zoals artikel 15, lid 1, van richtlijn 2002/58,

gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, eist (zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 107).

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

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

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

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

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

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

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

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

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

151. Om ervoor te zorgen dat de inmenging die de in de punten 147 tot en met 150 van het onderhavige arrest beschreven maatregelen inzake gerichte gegevensbewaring met zich brengen, in overeenstemming is met het evenredigheidsbeginsel, mogen die maatregelen niet langer gelden dan strikt noodzakelijk is in het licht van het ermee beoogde doel en van de

omstandigheden waardoor zij worden gerechtvaardigd, met dien verstande dat zij eventueel kunnen worden verlengd mocht de noodzaak van een dergelijke bewaring blijven bestaan.

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

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

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

154. Om de op het spel staande rechten en belangen met elkaar te verzoenen, zoals de in punt 130 van het onderhavige arrest aangehaalde rechtspraak verlangt, moet echter in aanmerking worden genomen dat in het geval van een online gepleegd strafbaar feit het IP-adres het enige onderzoeksmiddel kan zijn met behulp waarvan de persoon kan worden geïdentificeerd aan wie dat adres was toegewezen op het moment waarop dat feit werd gepleegd. Bovendien lijkt de bewaring van IP-adressen door aanbieders van elektronischecommunicatiediensten na afloop van de periode waarvoor deze adressen werden toegewezen, in beginsel niet noodzakelijk te zijn met het oog op de facturering van die diensten, met als gevolg dat, zoals verschillende regeringen hebben aangevoerd in de door hen bij het Hof ingediende opmerkingen, het opsporen van online gepleegde strafbare feiten onmogelijk kan blijken zonder gebruik te maken van een wettelijke maatregel als bedoeld in artikel 15, lid 1, van richtlijn 2002/58. Zoals die regeringen hebben betoogd, kan dit met name het geval zijn bij zeer ernstige strafbare feiten op het gebied van kinderpornografie, zoals het online verwerven, verspreiden, uitzenden of ter beschikking stellen van kinderpornografie in de zin van artikel 2, onder c), van richtlijn 2011/93/EU van het Europees Parlement en de Raad van 13 december 2011 ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie, en ter vervanging van kaderbesluit 2004/68/JBZ van de Raad (*PB* 2011, L 335, blz. 1).

155. In deze omstandigheden moet worden vastgesteld dat, ook al zou een wettelijke maatregel die voorziet in de bewaring van de IP-adressen van alle natuurlijke personen die eigenaar zijn van eindapparatuur die internettoegang mogelijk maakt, personen betreffen bij wie op het eerste gezicht een verband met de nagestreefde doelstellingen in de zin van de in punt 133 van het onderhavige arrest aangehaalde rechtspraak ontbreekt, en ook al moeten internetgebruikers, zoals in punt 109 van het onderhavige arrest is vastgesteld, op grond van de

artikelen 7 en 8 van het Handvest erop kunnen vertrouwen dat hun identiteit in beginsel niet wordt onthuld, een wettelijke maatregel die voorziet in de algemene en ongedifferentieerde bewaring van uitsluitend de aan de bron van een verbinding toegewezen IP-adressen, in beginsel niet in strijd is met artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, voor zover die mogelijkheid afhankelijk wordt gesteld van de strikte naleving van de materiële en procedurele voorwaarden die het gebruik van die gegevens dienen te regelen.

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

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

158. Hieruit volgt dat, overeenkomstig hetgeen is uiteengezet in punt 140 van het onderhavige arrest, wettelijke maatregelen die betrekking hebben op de verwerking van die gegevens als zodanig, in het bijzonder op de bewaring van en de toegang tot die gegevens met als enige doel de betrokken gebruiker te identificeren, zonder dat de gegevens in verband kunnen worden gebracht met informatie over de tot stand gebrachte communicatie, kunnen worden gerechtvaardigd door de in artikel 15, lid 1, eerste zin, van richtlijn genoemde doelstelling strafbare feiten in het algemeen te voorkomen, te onderzoeken, op te sporen en te vervolgen (zie in die zin arrest van 2 oktober 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, punt 62).

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

- Wettelijke maatregelen die voorzien in de spoedbewaring van verkeers- en locatiegegevensten behoeve van de bestrijding van zware criminaliteit

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

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

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

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

164. Aangezien het doel van een dergelijke spoedbewaring niet meer overeenkomt met de doelen waarvoor de gegevens oorspronkelijk zijn vergaard en bewaard, en aangezien ingevolge artikel 8, lid 2, van het Handvest iedere verwerking van gegevens bepaalde doelen moet dienen, moeten de lidstaten in hun wetgeving duidelijk maken voor welk doel spoedbewaring van gegevens mogelijk is. Gelet op het feit dat een dergelijke bewaring een ernstige inmenging inhoudt in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten, kunnen

enkel de bestrijding van zware criminaliteit en, *a fortiori*, de bescherming van de nationale veiligheid die inmenging rechtvaardigen. Om ervoor te zorgen dat de inmenging die een dergelijke maatregel met zich brengt, tot het strikt noodzakelijke wordt beperkt, moet bovendien om te beginnen de bewaarplicht uitsluitend gelden voor verkeers- en locatiegegevens die kunnen helpen bij het ophelderen van het betrokken ernstige strafbare feit of de betrokken verstoring van de nationale veiligheid. Bovendien mag de bewaartermijn niet langer zijn dan strikt noodzakelijk, zij het dat die termijn kan worden verlengd wanneer de omstandigheden en het met de betrokken maatregel beoogde doel dit rechtvaardigen.

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

166. Hieraan moet nog worden toegevoegd dat, zoals met name uit de punten 115 en 133 van het onderhavige arrest volgt, de toegang tot verkeers- en locatiegegevens die door aanbieders van elektronischecommunicatiediensten worden bewaard op grond van een krachtens artikel 15, lid 1, van richtlijn 2002/58 vastgestelde maatregel, in beginsel enkel kan worden gerechtvaardigd door de doelstelling van algemeen belang met het oog waarop de verplichting tot bewaring van die gegevens aan die aanbieders is opgelegd. Hieruit volgt met name dat in geen geval toegang tot dergelijke gegevens mag worden verleend met het oog op de vervolging en bestraffing van een gewoon strafbaar feit, wanneer de bewaring van die gegevens haar rechtvaardiging vindt in de doelstelling van bestrijding van zware criminaliteit of, a fortiori, de doelstelling van bescherming van de nationale veiligheid. Overeenkomstig het evenredigheidsbeginsel zoals dit is verduidelijkt in punt 131 van het onderhavige arrest, kan daarentegen de toegang tot gegevens die zijn bewaard met het oog op de bestrijding van zware criminaliteit, worden gerechtvaardigd door de doelstelling van bescherming van de nationale veiligheid, mist de in het voorgaande punt bedoelde materiële en procedurele voorwaarden voor een dergelijke toegang in acht worden genomen.

167. In zoverre staat het de lidstaten vrij om in hun wetgeving te bepalen dat met inachtneming van diezelfde materiële en procedurele voorwaarden toegang tot verkeers- en locatiegegevens kan worden verleend met het oog op de bestrijding van zware criminaliteit of

de bescherming van de nationale veiligheid, wanneer die gegevens door een aanbieder zijn bewaard in overeenstemming met de artikelen 5, 6 en 9 of met artikel 15, lid 1, van richtlijn 2002/58.

168. Gelet op een en ander moet op de eerste vraag in de zaken C-511/18 en C-512/18 en op de eerste en de tweede vraag in zaak C-520/18 worden geantwoord dat artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, aldus moet 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, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, 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 ».

In het dictum van het arrest heeft het Hof van Justitie verklaard voor recht :

« 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.15. Uit het voormelde arrest van het Hof van Justitie van 6 oktober 2020 in zake *La Quadrature du Net e.a.*, blijkt dat artikel 15, lid 1, van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8 en 11 alsook van artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, aldus moet worden uitgelegd dat het zich verzet tegen wettelijke maatregelen die voor de in dat artikel 15, § 1, genoemde doeleinden preventief voorzien in een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens, behalve in de in het voormelde arrest beschreven beperkte gevallen.

In zoverre zij principieel en zonder beperking tot die gevallen voorziet in een algemene en ongedifferentieerde bewaring, door de operatoren en aanbieders van elektronische communicatiediensten, van de identificatiegegevens, de toegangs- en verbindingsgegevens, alsook van de communicatiegegevens beoogd in artikel 126, § 3, van de wet van 13 juni 2005, schendt de bestreden wet bijgevolg artikel 15, lid 1, van de richtlijn 2002/58/EG, gelezen in het licht van de voormelde bepalingen van het Handvest van de grondrechten van de Europese Unie, en in samenhang met de artikelen 10 en 11 van de Grondwet.

B.16.1. In het dictum van het voormelde arrest van 6 oktober 2020, in zake *La Quadrature du Net e.a.*, preciseert het Hof van Justitie echter dat artikel 15, lid 1, van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8 en 11 alsook van artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, zich niet verzet tegen verschillende soorten wettelijke maatregelen die het Hof opsomt. Toelaatbaar zijn aldus, met name, wettelijke maatregelen « die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de IP-adressen die zijn

toegewezen aan de bron van een verbinding, voor een periode die niet langer is dan strikt noodzakelijk », of nog wettelijke maatregelen « die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van criminaliteit en de bescherming van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronische communicatiemiddelen ». Die wettelijke maatregelen moeten, « door het gebruik van duidelijke en nauwkeurige regels, verzekeren dat de betrokken gegevens slechts worden bewaard indien aan de daarvoor geldende materiële en procedurele voorwaarden wordt voldaan, en dat de betrokken personen beschikken over effectieve waarborgen tegen het risico van misbruik ».

B.16.2. Op grond van die preciseringen van het Hof van Justitie betoogt de Ministerraad in zijn aanvullende memories dat de bestreden wet in elk geval niet dient te worden vernietigd in zoverre zij voorziet in de algemene en ongedifferentieerde verplichting tot bewaring, door de operatoren en aanbieders van elektronische communicatiediensten, van de IP-adressen die zijn toegewezen aan de bron van een verbinding, enerzijds, en van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronische communicatiemiddelen, anderzijds.

De Ministerraad besluit daaruit dat, in voorkomend geval, enkel het tweede en het derde lid van artikel 126, § 3, van de wet van 13 juni 2005 dienen te worden vernietigd, waarin respectievelijk de verbindings- en locatiegegevens en de communicatiegegevens worden beoogd. Hij is van mening dat het eerste lid van het voormelde artikel 126, § 3, waarin de identificatiegegevens worden beoogd, daarentegen niet dient te worden vernietigd, net zomin als de andere bepalingen van de bestreden wet, aangezien zij de nodige waarborgen bevatten op het vlak van bewaring van en toegang tot de gegevens.

B.17. Te dezen dient te worden vastgesteld dat de bestreden wet, wat het beginsel zelf ervan betreft, berust op een verplichting tot algemene en ongedifferentieerde bewaring van alle gegevens beoogd in artikel 126, § 3, van de wet van 13 juni 2005, en dat zij, in het algemeen, zoals in B.3 en B.4 is vermeld, ruimere doelstellingen nastreeft dan de bestrijding van zware criminaliteit of het risico van aantasting van de openbare veiligheid.

Het onderscheid dat bij artikel 126, § 3, van de wet van 13 juni 2005 wordt gemaakt tussen drie categorieën van gegevens (te weten : identificatiegegevens, toegangs- en verbindingsgegevens, alsook communicatiegegevens) heeft slechts een weerslag op het

startpunt van de bewaringstermijn van de gegevens - in elk geval twaalf maanden -, en eventueel op de mogelijkheden voor de gemachtigde instanties om toegang tot die gegevens te hebben (zie artikel 46*bis* van het Wetboek van strafvordering en artikel 126, §2, van de wet van 13 juni 2005). Die categorisering stemt daarenboven niet overeen met het onderscheid dat door het Hof van Justitie in zijn arrest van 6 oktober 2020 wordt gemaakt voor wat betreft de verschillende categorieën van gegevens die het voorwerp kunnen uitmaken van een verplichting tot algemene en ongedifferentieerde bewaring, mits verscheidene voorwaarden in acht worden genomen (te weten, te dezen : de IP-adressen die zijn toegewezen aan de bron van een verbinding en de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronische communicatiemiddelen).

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

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

B.20. Rekening houdend met hetgeen voorafgaat, dienen de artikelen 2, b), 3 tot 11 en 14 van de bestreden wet, die onlosmakelijk met elkaar verbonden zijn, te worden vernietigd.

B.21. De andere middelen in de zaken nrs. 6599 en 6601 betreffen ook de algemene en ongedifferentieerde bewaring van gegevens met betrekking tot elektronische communicatie en de toegang tot die gegevens. Aangezien zij niet tot een ruimere vernietiging kunnen leiden, dienen zij niet te worden onderzocht.

Ten aanzien van de handhaving van de gevolgen

B.22. In zijn memories van wederantwoord verzoekt de Ministerraad het Hof in uiterst ondergeschikte orde de gevolgen te handhaven van de bepalingen die in voorkomend geval zouden worden vernietigd, teneinde het door de politie- en inlichtingendiensten verrichte werk inzake opsporing en vervolging van misdrijven niet in gevaar te brengen.

B.23.1. Artikel 8, derde lid, van de bijzondere wet van 6 januari 1989 op het Grondwettelijk Hof bepaalt :

« Zo het Hof dit nodig oordeelt, wijst het, bij wege van algemene beschikking, die gevolgen van de vernietigde bepalingen aan welke als gehandhaafd moeten worden beschouwd of voorlopig gehandhaafd worden voor de termijn die het vaststelt ».

B.23.2. Het Hof dient ter zake rekening te houden met de beperkingen die uit het recht van de Europese Unie voortvloeien inzake de handhaving van de gevolgen van nationale normen die dienen te worden vernietigd omdat zij in strijd zijn met dat recht (HvJ, grote kamer, 8 september 2010, C-409/06, *Winner Wetten*, punten 53-69; HvJ, grote kamer, 28 februari 2012, C-41/11, *Inter-Environnement Wallonie en Terre wallonne*, punten 56-63).

In de regel kan dit enkel onder de voorwaarden die door het Hof van Justitie in antwoord op een prejudiciële vraag worden vastgesteld.

B.24.1. In antwoord op de door het Hof gestelde derde prejudiciële vraag over een eventuele handhaving van de gevolgen van de bestreden wet, heeft het Hof van Justitie geoordeeld :

« *Derde vraag in zaak C-520/18*

213. Met de derde vraag in zaak C-520/18 wenst de verwijzende rechter in wezen te vernemen of een nationale rechterlijke instantie een bepaling van haar nationale recht mag toepassen die haar machtigt om de werking in de tijd van een onwettigverklaring te beperken wanneer hij op grond van dit recht een nationale wettelijke regeling die ten behoeve van onder meer de bescherming van de nationale veiligheid en de bestrijding van criminaliteit aan aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens oplegt, onwettig dient te verklaren omdat zij onverenigbaar is met artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest.

214. Het beginsel van het primaat van het Unierecht houdt in dat dit recht voorrang heeft op het recht van de lidstaten. Dit beginsel verplicht dus alle instanties van de lidstaten om volle werking te verlenen aan de verschillende normen van de Unie, aangezien het recht van de lidstaten niet kan afdoen aan de werking die op het grondgebied van die staten aan deze verschillende normen is verleend [arrest van 15 juli 1964, *Costa*, 6/64, EU:C:1964:66, blz. 1219 en 1220, en 19 november 2019, *A. K. e.a*. (*Onafhankelijkheid van de tuchtkamer van de Sąd Najwyższy*), C-585/18, C-624/18 en C-625/18, EU:C:2019:982, punten 157 en 158 en aldaar aangehaalde rechtspraak].

215. Het voorrangsbeginsel brengt mee dat, indien de nationale regelgeving niet in overeenstemming met de vereisten van het Unierecht kan worden uitgelegd, de nationale rechter die in het kader van zijn bevoegdheid is belast met de toepassing van de bepalingen van het Unierecht, verplicht is de volle werking van deze bepalingen te verzekeren en daarbij zo nodig, op eigen gezag, elke, zelfs latere, strijdige bepaling van de nationale wettelijke regeling buiten toepassing te laten, zonder dat hij de voorafgaande opheffing hiervan via de wetgeving of enige andere constitutionele procedure hoeft te vragen of af te wachten [arresten van 22 juni 2010, *Melki en Abdeli*, C-188/10 en C-189/10, EU:C:2010:363, punt 43 en aldaar aangehaalde rechtspraak; 24 juni 2019, *Popławski*, C-573/17, EU:C:2019:530, punt 58, en 19 november 2019, *A. K. e.a.* (*Onafhankelijkheid van de tuchtkamer van de Sąd Najwyższy*), C-585/18, C-624/18 en C-625/18, EU:C:2019:982, punt 160].

216. Enkel het Hof kan, bij wijze van uitzondering en om dwingende redenen van rechtszekerheid, een voorlopige opschorting toestaan van het effect dat een regel van het Unierecht op het daarmee strijdige nationale recht heeft, namelijk de terzijdestelling daarvan. Een dergelijke beperking in de tijd van de werking van de door het Hof aan het Unierecht gegeven uitlegging kan slechts worden vastgesteld in het arrest waarin de gevraagde uitlegging wordt gegeven [zie in die zin arresten van 23 oktober 2012, *Nelson e.a.*, C-581/10 en C-629/10, EU:C:2012:657, punten 89 en 91; 23 april 2020, *Herst*, C-401/18, EU:C:2020:295, punten 56 en 57, en 25 juni 2020, *A e.a.* (*Windturbines in Aalter en Nevele*), C-24/19, EU:C:2020:503, punt 84 en aldaar aangehaalde rechtspraak].

217. Aan de voorrang en de uniforme toepassing van het Unierecht zou afbreuk worden gedaan indien de nationale rechterlijke instanties bevoegd waren om, al was het maar tijdelijk, aan nationale bepalingen voorrang te geven boven het Unierecht waarmee deze bepalingen in strijd zijn (zie in die zin arrest van 29 juli 2019, *Inter-Environnement Wallonie en Bond Beter Leefmilieu Vlaanderen*, C-411/17, EU:C:2019:622, punt 177 en aldaar aangehaalde rechtspraak).

218. Het Hof heeft evenwel in een zaak waarin het draaide om de rechtmatigheid van maatregelen die waren vastgesteld in strijd met de Unierechtelijke verplichting om een voorafgaande beoordeling te verrichten van de gevolgen van een project voor het milieu of voor een beschermd gebied, geoordeeld dat een nationale rechterlijke instantie, indien het nationale recht dat toestaat, bij wijze van uitzondering de gevolgen van dergelijke maatregelen kan handhaven indien deze handhaving wordt gerechtvaardigd door dwingende redenen die verband houden met de noodzaak om het reële en ernstige risico af te wenden dat de elektriciteitsbevoorrading van de betrokken lidstaat wordt onderbroken, en aan dit risico niet het hoofd zou kunnen worden geboden met andere middelen en alternatieven, met name in het kader van de interne markt, met dien verstande dat die handhaving niet langer kan duren dan strikt noodzakelijk is om een einde te maken aan die onrechtmatigheid (zie in die zin arrest van 29 juli 2019, *Inter-Environnement Wallonie en Bond Beter Leefmilieu Vlaanderen*, C-411/17, EU:C:2019:622, punten 175, 176, 179 en 181).

219. Anders dan de niet-nakoming van een procedurele verplichting als de voorafgaande beoordeling van de gevolgen van een project op het specifieke terrein van de milieubescherming, kan een schending van artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, niet worden geregulariseerd via een procedure die vergelijkbaar is met die waaraan in het voorgaande punt wordt gerefereerd. Handhaving van de gevolgen van een nationale wettelijke regeling als in het hoofdgeding aan de orde is, zou immers betekenen dat die regeling aan aanbieders van elektronischecommunicatiediensten verplichtingen blijft opleggen die in strijd zijn met het Unierecht en leiden tot een ernstige inmenging in de grondrechten van de personen van wie de gegevens zijn bewaard.

220. Hieruit volgt dat de verwijzende rechter geen bepaling van zijn nationale recht mag toepassen die hem machtigt om de werking in de tijd te beperken van een door hem op grond van dit recht uit te spreken onwettigverklaring van de in het hoofdgeding aan de orde zijnde nationale wettelijke regeling.

221. VZ, WY en XX stellen in hun bij het Hof ingediende schriftelijke opmerkingen dat de derde vraag impliciet maar noodzakelijkerwijs de vraag opwerpt of het Unierecht zich ertegen verzet dat in het kader van een strafrechtelijke procedure wordt gebruikgemaakt van informatie en bewijzen die zijn verkregen door middel van een met dit recht onverenigbare algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens.

222. Om de verwijzende rechter een nuttig antwoord te verstrekken, zij er in dit verband aan herinnerd dat het bij de huidige stand van het Unierecht uitsluitend een zaak van het nationale recht is om de regels vast te stellen met betrekking tot de aanvaarding en de beoordeling van door middel van een dergelijke met het Unierecht strijdige gegevensbewaring verkregen informatie en bewijzen in het kader van een strafrechtelijke procedure tegen personen die worden verdacht van ernstige strafbare feiten.

223. Het is immers vaste rechtspraak dat het bij gebreke van Unieregelgeving ter zake krachtens het beginsel van procedurele autonomie een aangelegenheid van de interne rechtsorde van elke lidstaat is om de procedureregels vast te stellen voor rechtsvorderingen die ertoe strekken de rechten die de justitiabelen aan het Unierecht ontlenen, te beschermen, op voorwaarde evenwel dat die regels niet ongunstiger zijn dan die welke voor soortgelijke situaties naar nationaal recht gelden (gelijkwaardigheidsbeginsel) en de uitoefening van de door het Unierecht verleende rechten in de praktijk niet onmogelijk of uiterst moeilijk maken

(doeltreffendheidsbeginsel) (zie in die zin arresten van 6 oktober 2015, *Târşia*, C-69/14, EU:C:2015:662, punten 26 en 27; 24 oktober 2018, *XC e.a.*, C-234/17, EU:C:2018:853, punten 21 en 22 en aldaar aangehaalde rechtspraak, en 19 december 2019, *Deutsche Umwelthilfe*, C-752/18, EU:C:2019:1114, punt 33).

224. Wat het gelijkwaardigheidsbeginsel betreft, staat het aan de nationale rechter bij wie een strafrechtelijke procedure is aangebracht die gebaseerd is op informatie of bewijzen die in strijd met de uit richtlijn 2002/58 voortvloeiende vereisten zijn verkregen, om na te gaan of het op die procedure van toepassing zijnde nationale recht minder gunstige regels bevat voor de aanvaarding en het gebruik van dergelijke informatie en bewijzen dan voor de aanvaarding en het gebruik van informatie en bewijzen die zijn verkregen in strijd met het interne recht.

225. Met betrekking tot het doeltreffendheidsbeginsel moet worden opgemerkt dat nationale regels inzake de aanvaarding en het gebruik van informatie en bewijzen tot doel hebben om in overeenstemming met de in het nationale recht gemaakte keuzen te voorkomen dat onrechtmatig verkregen informatie en bewijzen ongerechtvaardigd nadeel toebrengen aan een persoon die ervan wordt verdacht strafbare feiten te hebben gepleegd. Dat doel kan naar nationaal recht niet alleen worden bereikt door middel van een verbod op het gebruik van dergelijke informatie en bewijzen, maar ook door middel van nationale regels en praktijken met betrekking tot de beoordeling en de weging van de informatie en de bewijzen, of door de inaanmerkingneming van het onrechtmatige karakter ervan bij de straftoemeting.

226. Uit de rechtspraak van het Hof volgt dat bij de beoordeling of informatie en bewijzen die in strijd met de voorschriften van het Unierecht zijn verkregen, moeten worden uitgesloten, met name moet worden nagegaan of de aanvaarding van dergelijke informatie en bewijzen schending van het beginsel van hoor en wederhoor en dus ook van het recht op een eerlijk proces tot gevolg kan hebben (zie in die zin arrest van 10 april 2003, *Steffensen*, C-276/01, EU:C:2003:228, punten 76 en 77). Een rechterlijke instantie die van oordeel is dat een partij niet in de gelegenheid is om doeltreffend commentaar te leveren op een bewijsmiddel dat betrekking heeft op een gebied waarvan de rechters geen kennis hebben en dat een doorslaggevende invloed kan hebben op de beoordeling van de feiten, moet vaststellen dat het recht op een eerlijk proces hierdoor wordt geschonden, en dat bewijsmiddel uitsluiten om die schending te voorkomen (zie in die zin arrest van 10 april 2003, *Steffensen*, C-276/01, EU:C:2003:228, punten 78 en 79).

227. Bijgevolg brengt het doeltreffendheidsbeginsel voor de nationale strafrechter de verplichting mee om informatie en bewijzen die door middel van een met het Unierecht onverenigbare algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens zijn verkregen, in het kader van een strafrechtelijke procedure tegen personen die worden verdacht van strafbare handelingen buiten beschouwing te laten indien die personen niet in de gelegenheid zijn om doeltreffend commentaar te leveren op die informatie en die bewijzen, die betrekking hebben op een gebied waarvan de rechter geen kennis heeft en een doorslaggevende invloed kunnen hebben op de beoordeling van de feiten.

228. Gelet op een en ander moet op de derde vraag in zaak C-520/18 worden geantwoord dat een nationale rechterlijke instantie geen bepaling van haar nationale recht mag toepassen die haar machtigt om de werking in de tijd te beperken van de door haar op grond van dit recht uit te spreken onwettigverklaring van een nationale wettelijke regeling waarbij ten behoeve van met name de bescherming van de nationale veiligheid en de bestrijding van criminaliteit aan aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en

ongedifferentieerde bewaring van verkeers- en locatiegegevens wordt opgelegd die onverenigbaar is met artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest. Op grond van artikel 15, lid 1, uitgelegd in het licht van het doeltreffendheidsbeginsel, dient de nationale strafrechter informatie en bewijzen die door middel van een met het Unierecht onverenigbare algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens zijn verkregen, in het kader van een strafrechtelijke procedure tegen personen die worden verdacht van strafbare handelingen buiten beschouwing te laten indien die personen niet in de gelegenheid zijn om doeltreffend commentaar te leveren op die informatie en die bewijzen, die betrekking hebben op een gebied waarvan de rechter geen kennis heeft en een doorslaggevende invloed kunnen hebben op de beoordeling van de feiten ».

In het dictum van het arrest heeft het Hof van Justitie voor recht verklaard :

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

B.24.2. Uit het voormelde arrest blijkt dat het Hof geen gegronde redenen heeft om de gevolgen van de vernietigde bepalingen voorlopig te handhaven.

B.24.3. Het staat aan de bevoegde strafrechter, in voorkomend geval, uitspraak te doen over de toelaatbaarheid van de bewijzen die werden verzameld bij de tenuitvoerlegging van de vernietigde bepalingen, overeenkomstig artikel 32 van de voorafgaande titel van het Wetboek van stafvordering en in het licht van de door het Hof van Justitie in het voormelde arrest van 6 oktober 2020 aangebrachte preciseringen.

Om die redenen,

het Hof

vernietigt 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 » en verwerpt de beroepen voor het overige.

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 22 april 2021.

De griffier, De voorzitter,

F. Meersschaut F. Daoût