Datum van inontvangstneming	:	26/09/2018

Zaak C-520/18

Samenvatting van het verzoek om een prejudiciële beslissing overeenkomstig artikel 98, lid 1, van het Reglement voor de procesvoering van het Hof van Justitie[1]

Datum van indiening:

2 augustus 2018

Verwijzende rechter:

Grondwettelijk Hof (België)

Datum van de verwijzingsbeslissing:

19 juli 2018

Verzoekende partijen:

Ordre des barreaux francophones et germanophone

Académie Fiscale ASBL

UA

Liga voor Mensenrechten ASBL

Ligue des Droits de l'Homme ASBL

VZ

WY

XX

Verwerende partij:

Ministerraad (Belgische regering)

---

[1] Noot van de vertaler: de volledige tekst van het arrest van het Grondwettelijk Hof is beschikbaar in het Nederlands en kan worden geraadpleegd op de website van het Grondwettelijk Hof: http://www.const-court.be/public/n/2018/2018-096n.pdf.

I. Voorwerp en context van het hoofdgeding

1 De Ordre des barreaux francophones et germanophone (hierna: „OBFG”), ASBL „Académie Fiscale”, ASBL „Liga voor Mensenrechten” en ASBL „Ligue des Droits de l'Homme” alsook een aantal natuurlijke personen hebben bij het Grondwettelijk Hof van België (hierna: „verwijzende rechter”) een beroep 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 (*Belgisch Staatsblad*, 2016, blz. 44717; hierna: „bestreden wet”) ingesteld. Deze zaken zijn gevoegd.

2 De bestreden wet wijzigt verschillende bepalingen van de wet van 13 juni 2005 betreffende de elektronische communicatie (*Belgisch Staatsblad,* 20 juni 2005, blz. 28070) (hierna: „wet van 13 juni 2005”), van het Wetboek van strafvordering, en van de organieke wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst (*Belgisch Staatsblad*, 18 december 1998, blz. 40312) (hierna: „wet van 30 november 1998”).

3 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 90decies van het Wetboek van strafvordering (*Belgisch Staatsblad*, 23 augustus 2013, blz. 56109; hierna „wet van 30 juli 2013”), had het Koninkrijk België 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 (PB 2006, L 105, blz. 54) gedeeltelijk in Belgisch recht omgezet, alsook 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) (PB 2002, L 201, blz. 37) (hierna: „richtlijn 2002/58”).

4 In zijn arrest van 8 april 2014, Digital Rights Ireland e.a. (C-293/12 en C-594/12, EU:C:2014:238) (hierna: „arrest Digital Rights Ireland e.a.”), heeft het Hof richtlijn 2006/24 ongeldig verklaard.

5 Bij arrest nr. 84/2015 van 11 juni 2015 heeft de verwijzende rechter artikel 126 van de wet van 13 juni 2005, zoals gewijzigd bij de wet van 30 juli 2013, vernietigd om redenen die identiek zijn aan die welke het Hof ertoe hebben gebracht richtlijn 2006/24 ongeldig te verklaren.

6 Met de bestreden wet is de wetgever willen tegemoetkomen aan die vernietiging.

II. Voorwerp en rechtsgrondslag van het prejudiciële verzoek

7 De bestreden wet wijzigt de wet van 13 juni 2005, waarbij verschillende richtlijnen, waaronder richtlijn 2005/58, in Belgisch recht zijn omgezet.

III. Rechtskader van de prejudiciële vragen

1. Unierecht

A. Verdrag betreffende de Europese Unie (hierna: „VEU")

8 Artikel 5, lid 4, TUE bepaalt:

„Krachtens het evenredigheidsbeginsel gaan de inhoud en de vorm van het optreden van de Unie niet verder dan wat nodig is om de doelstellingen van de Verdragen te verwezenlijken.

De instellingen van de Unie passen het evenredigheidsbeginsel toe overeenkomstig het protocol betreffende de toepassing van de beginselen van subsidiariteit en evenredigheid."

9 Artikel 6 VEU bepaalt:

„1. De Unie erkent de rechten, vrijheden en beginselen die zijn vastgesteld in het Handvest van de grondrechten van de Europese Unie van 7 december 2000, als aangepast op 12 december 2007 te Straatsburg, dat dezelfde juridische waarde als de Verdragen heeft.

De bepalingen van het Handvest houden geenszins een verruiming in van de bevoegdheden van de Unie zoals bepaald bij de Verdragen.

De rechten, vrijheden en beginselen van het Handvest worden uitgelegd overeenkomstig de algemene bepalingen van titel VII van het Handvest betreffende de uitlegging en toepassing ervan, waarbij de in het Handvest bedoelde toelichtingen, waarin de bronnen van deze bepalingen vermeld zijn, terdege in acht genomen worden.

2. De Unie treedt toe tot het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden. Die toetreding wijzigt de bevoegdheden van de Unie, zoals bepaald in de Verdragen, niet. [...]"

B. Handvest van de grondrechten van de Europese Unie (hierna: „Handvest")

10 Artikel 4 van het Handvest bepaalt het volgende:

„Het verbod van folteringen en van onmenselijke of vernederende behandelingen of bestraffingen

Niemand mag worden onderworpen aan folteringen of aan onmenselijke of vernederende behandelingen of bestraffingen.”

11 Artikel 6 van het Handvest luidt als volgt:

„Het recht op vrijheid en veiligheid

Eenieder heeft recht op vrijheid en veiligheid van zijn persoon.”

12 In artikel 7 van het Handvest is het volgende bepaald:

„De eerbiediging van het privéleven en van het familie- en gezinsleven

Eenieder heeft recht op eerbiediging van zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn communicatie.”

13 Artikel 8 van het Handvest bepaalt:

„De bescherming van persoonsgegevens

1. Eenieder heeft recht op bescherming van zijn persoonsgegevens.

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

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

14 Artikel 11 van het Handvest luidt als volgt:

„Artikel 11

De vrijheid van meningsuiting en van informatie

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

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

15 In artikel 47 van het Handvest valt het volgende te lezen:

„Recht op een doeltreffende voorziening in rechte en op een onpartijdig gerecht

Eenieder wiens door het recht van de Unie gewaarborgde rechten en vrijheden zijn geschonden, heeft recht op een doeltreffende voorziening in rechte, met inachtneming van de in dit artikel gestelde voorwaarden.

Eenieder heeft recht op een eerlijke en openbare behandeling van zijn zaak, binnen een redelijke termijn, door een onafhankelijk en onpartijdig gerecht dat vooraf bij wet is ingesteld. Eenieder heeft de mogelijkheid zich te laten adviseren, verdedigen en vertegenwoordigen.

Rechtsbijstand wordt verleend aan degenen die niet over toereikende financiële middelen beschikken, voor zover die bijstand noodzakelijk is om de daadwerkelijke toegang tot de rechter te waarborgen."

16 Artikel 52 van het Handvest bepaalt het volgende:

„Reikwijdte en uitlegging van de gewaarborgde rechten en beginselen

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

C. Richtlijn 2002/58/EG

17 Artikel 15, lid 1, van richtlijn 2002/58 bepaalt het volgende:

„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".

D. Verordening (EU) 2016/679 [van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG (algemene verordening gegevensbescherming)] (hierna: „verordening 2016/679")

18 In artikel 95 van verordening 2016/679 is bepaald:

„Verhouding tot richtlijn 2002/58/EG

Deze verordening legt natuurlijke personen of rechtspersonen geen aanvullende verplichtingen op met betrekking tot verwerking in verband met het verstrekken van openbare elektronische-communicatiediensten in openbare communicatienetwerken in de Unie, voor zover zij op grond van Richtlijn 2002/58/EG onderworpen zijn aan specifieke verplichtingen met dezelfde doelstelling."

2. Nationaal recht

19 De voornaamste bepalingen van de relevante nationale wetgeving, zoals gewijzigd door de bestreden wet, zijn de volgende:

A. Wet van 13 juni 2005 betreffende de elektronische communicatie

20 De wet van 13 juni 2005, zoals gewijzigd bij de bestreden wet, luidt als volgt:

„[...]

Artikel 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.

[...]

§ 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 46bis en 88bis 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 [...];

3° elke officier van gerechtelijke politie van het [Belgisch Instituut voor postdiensten en telecommunicatie (hierna: „Instituut")], met het oog op het opsporen, het onderzoek en de vervolging van inbreuken op de [voorschriften inzake netwerkbeveiliging] 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 [...] 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 [...]. 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.

[...]

Artikel 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 46bis, 88bis en 90ter van het Wetboek van strafvordering en de artikelen 18/7, 18/8, 18/16 en 18/17 van de wet van 30 november 1998 [...].

[...].

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.

[...]

§ 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.

[...]

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:

[...]

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.

Artikel 127:

§ 1. De Koning bepaalt, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de technische en administratieve maatregelen die aan de operatoren, aan de aanbieders bedoeld in artikel 126, § 1, eerste lid, of aan de eindgebruikers worden opgelegd om:

1° in het kader van een noodoproep de oproeplijn te kunnen identificeren;

2° de eindgebruiker te kunnen identificeren en het opsporen, lokaliseren, afluisteren, kennisnemen en opnemen van privé-communicatie mogelijk te maken onder de voorwaarden bepaald door de artikel en 46bis, 88bis en 90ter tot 90decies van het Wetboek van strafvordering en door de wet van 30 november 1998 [...]

[...]

[...].

§ 2. De levering of het gebruik van een dienst of van apparatuur die de uitvoering bemoeilijkt of verhindert van de in § 1 bedoelde verrichtingen, zijn verboden, met uitzondering van encryptiesystemen die kunnen worden gebruikt om de vertrouwelijkheid van de communicatie en de veiligheid van betalingen te garanderen.

[...]

Artikel 145

§ 1. Met een geldboete van 50 tot 50 000 EUR wordt gestraft de persoon die de artikelen [...] 126, 126/1, 127 en de ter uitvoering van de artikelen [...] 126, 126/1 en 127 genomen besluiten overtreedt.

[...]”.

B. Wetboek van strafvordering

21 Het wetboek van strafvordering, zoals gewijzigd bij de bestreden wet, luidt als volgt:

„[...]

Artikel 46 bis

§ 1. Bij het opsporen van de misdaden en wanbedrijven kan de procureur des Konings bij een gemotiveerde en schriftelijke beslissing, door zo nodig de medewerking van de operator van een elektronisch communicatienetwerk of van de verstrekker van een elektronische communicatiedienst of van een politiedienst aangewezen door de Koning te vorderen, overgaan of doen overgaan op basis van ieder gegeven in zijn bezit of door middel van een toegang tot de klantenbestanden van de operator of van de dienstenverstrekker tot:

1° de identificatie van de abonnee of de gewoonlijke gebruiker van een elektronische communicatiedienst of van het gebruikte elektronische communicatiemiddel;

2° de identificatie van de elektronische communicatiediensten waarop een bepaald persoon geabonneerd is of die door een bepaald persoon gewoonlijk gebruikt worden.

De motivering weerspiegelt de proportionaliteit met inachtneming van de persoonlijke levenssfeer en de subsidiariteit ten opzichte van elke andere onderzoeksdaad.

In geval van uiterst dringende noodzakelijkheid kan iedere officier van gerechtelijke politie, na mondelinge en voorafgaande instemming van de procureur des Konings, bij een gemotiveerde en schriftelijke beslissing deze gegevens opvorderen. De officier van gerechtelijke politie deelt deze gemotiveerde en schriftelijke beslissing en de verkregen informatie binnen vierentwintig uur mee aan de procureur des Konings en motiveert tevens de uiterst dringende noodzakelijkheid.

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.

§ 2. Iedere operator van een elektronisch communicatienetwerk en iedere verstrekker van een elektronische communicatiedienst van wie gevorderd wordt de in paragraaf 1 bedoelde gegevens mee te delen, verstrekt de procureur des Konings of de officier van gerechtelijke politie de gegevens die werden opgevraagd binnen een termijn te bepalen door de Koning, op het voorstel van de Minister van Justitie en de Minister bevoegd voor Telecommunicatie.

[...]

Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

Weigering de gegevens mee te delen, wordt gestraft met geldboete van zesentwintig euro tot tienduizend euro.

Artikel 88 bis

§ 1. 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.

In de gevallen bepaald in het eerste lid wordt voor ieder elektronisch communicatiemiddel waarvan de oproepgegevens worden opgespoord of waarvan de oorsprong of de bestemming van de elektronische communicatie wordt gelokaliseerd, de dag, het uur, de duur, en, indien nodig, de plaats van de oproep vastgesteld en opgenomen in een proces-verbaal.

De onderzoeksrechter doet in een met redenen omkleed bevelschrift opgave van de feitelijke omstandigheden van de zaak die de maatregel rechtvaardigen, van de proportionaliteit met inachtneming van de persoonlijke levenssfeer en de subsidiariteit ten opzichte van elke andere onderzoeksdaad.

Hij vermeldt ook de duur van de maatregel voor de toekomst, die niet langer kan zijn dan twee maanden te rekenen vanaf het bevelschrift, onverminderd een hernieuwing en, in voorkomend geval, de periode in het verleden waarover de vordering zich uitstrekt overeenkomstig paragraaf 2.

[...]

§ 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 Iter, 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 90ter, §§ 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 324bis van het Strafwetboek, of een strafbaar feit dat een hoofdgevangenisstraf van vijf jaar of een zwaardere straf tot gevolg kan hebben, kan de onderzoeksrechter in zijn bevelschrift de gegevens vorderen voor een periode van negen maanden voorafgaand aan het bevelschrift;

- voor andere strafbare feiten kan de onderzoeksrechter de gegevens slechts vorderen voor een periode van zes maanden voorafgaand aan het bevelschrift.

§ 3. De maatregel kan alleen betrekking hebben op de elektronische communicatiemiddelen van een advocaat of een arts, indien deze er zelf van verdacht worden een strafbaar feit bedoeld in paragraaf 1 te hebben gepleegd of eraan deelgenomen te hebben, of, indien precieze feiten doen vermoeden dat derden die ervan verdacht worden een strafbaar feit bedoeld in paragraaf 1 te hebben gepleegd, gebruik maken van diens elektronische communicatiemiddelen.

De maatregel mag niet ten uitvoer worden gelegd, zonder dat, naargelang 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.

[...]

[§ 4.] [...]

Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek

[...]”

C. Wet van 30 november 1998

22 De wet van 30 november 1998, zoals gewijzigd bij de bestreden wet, luidt als volgt:

„[...]

Artikel 13

In het raam van hun opdrachten kunnen de inlichtingen- en veiligheidsdiensten informatie en persoonsgegevens opsporen, verzamelen, ontvangen en verwerken die nuttig kunnen zijn om hun opdrachten te vervullen en een documentatie bijhouden, meer bepaald met betrekking tot de gebeurtenissen, de groeperingen en de personen die een belang vertonen voor de uitoefening van hun opdrachten.

De in de documentatie vervatte inlichtingen moeten in verband staan met de doeleinden van het gegevensbestand en beperkt blijven tot de vereisten die eruit voortvloeien.

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.

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.

Artikel 18/3

§ 1. Rekening houdend met een potentiële bedreiging zoals bedoeld in artikel 18/1 kunnen de in artikel 18/2, § 1, bedoelde specifieke methoden voor het verzamelen van gegevens aangewend worden indien de gewone methoden voor het verzamelen van gegevens ontoereikend worden geacht om de informatie te verzamelen die nodig is om de inlichtingenopdracht te

volbrengen. De specifieke methode moet worden gekozen in functie van de graad van ernst van de potentiële bedreiging waarvoor ze wordt aangewend.

De specifieke methode kan slechts worden aangewend na een schriftelijke en met redenen omklede beslissing van het diensthoofd en na kennisgeving van deze beslissing aan de commissie.

§ 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;

[...]

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;

[...]

§ 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.

Artikel 18/8

§ 1. De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, zo nodig door daartoe de medewerking van de operator van een elektronisch communicatienetwerk of van de verstrekker van een elektronische communicatiedienst te vorderen, overgaan of doen overgaan tot:

1° het opsporen van de verkeersgegevens van elektronische communicatiemiddelen van waaruit of waarnaar elektronische communicaties worden of werden gedaan;

2° het lokaliseren van de oorsprong of de bestemming van elektronische communicaties.

[...]

§ 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.

[...]”

IV. Andere bepalingen en beginselen die zijn ingeroepen door de partijen of vermeld in de beslissing van de verwijzende rechter

23 Naast de bovengenoemde bepalingen zijn de volgende bepalingen en beginselen door de partijen ingeroepen of in de motivering van de beslissing van de verwijzende rechter vermeld:

– de artikelen 5, 6, 8, 9, 10, 11, 14, 15, 17 en 18 van het Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden, ondertekend te Rome op 4 november 1950 (hierna: „EVRM”);

– artikel 17 van het Internationaal Verdrag inzake burgerrechten en politieke rechten, gesloten te New York op 16 december 1966 (hierna: „BUPO”);

– artikel 2, onder a), en artikel 13, lid 1, van 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 (PB 1995, L 281, blz. 31);

– de artikelen 10, 11, 12, 15, 19, 22, 29, 151, lid 1, eerste alinea, van de Belgische Grondwet;

– de volgende algemene beginselen: het rechtszekerheidsbeginsel, het evenredigheidsbeginsel, het wettigheidsbeginsel in strafzaken, het redelijkheidsbeginsel, het beginsel van het vermoeden van onschuld, het beginsel van het recht op een eerlijk proces, het beginsel van het beroepsgeheim, het beginsel van gelijkheid onder burgers en het beginsel van informationele zelfbeschikking.

VI. Wezenlijke argumenten van de partijen

1. Middelen van de verzoekende partijen

24 De verzoekende partijen beroepen zich op schending van verschillende artikelen van de Grondwet, al dan niet in samenhang gelezen met verschillende artikelen van het VEU, het Handvest, richtlijn 2002/58 en andere bepalingen van het recht van de Unie, en met verschillende bepalingen van het EVRM, artikel 17 van het BUPO en met algemene rechtsbeginselen.

25 De bestreden wet legt de operatoren van elektronische-communicatiediensten een veralgemeende verplichting op om de verkeers- en locatiegegevens van gebruikers gedurende bepaalde perioden te bewaren. De bestreden wet regelt ook de toegang van de gerechtelijke autoriteiten en inlichtingen- en veiligheidsdiensten tot deze gegevens.

Verplichting tot het verzamelen en bewaren van gegevens

26 De verzoekende partijen verwijten de bestreden wet dat de gebruikers van telecommunicatie- of elektronische communicatiediensten die aan het beroepsgeheim zijn onderworpen, waaronder met name advocaten, en de andere gebruikers van die diensten daarbij zonder rechtvaardiging op identieke wijze worden behandeld, zonder dat rekening wordt gehouden met het bijzondere statuut van de advocaat, met het fundamentele karakter van het beroepsgeheim waaraan hij is onderworpen en met de noodzakelijke vertrouwensrelatie die hem aan zijn cliënten moet binden, 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 en ten slotte met vertrouwelijkheidsverplichtingen die gelden voor andere personen die niet onderworpen zijn aan het beroepsgeheim in strikte zin.

27 De door de bestreden wet in het leven geroepen discriminerende situatie is even nadelig voor de advocaten als voor de rechtzoekenden, aangezien het beroepsgeheim van de advocaat van algemeen belang is. Allen die zich in vertrouwen tot een advocaat wenden, moeten de zekerheid hebben dat het bestaan en de omstandigheden van die raadpleging en de aan hun raadsman toevertrouwde

geheimen niet aan derden zullen worden bekendgemaakt of tegen hen kunnen worden aangevoerd. Het beginsel van het beroepsgeheim van de advocaat heeft rechtstreeks te maken met het recht op een eerlijk proces en met het recht op eerbiediging van het privéleven. Er kan dus slechts afbreuk aan worden gedaan in uitzonderlijke gevallen, mits afdoende en toereikende waarborgen tegen misbruiken in acht worden genomen.

28 De ingezamelde gegevens, zelfs indien zij geen betrekking hebben op de inhoud van de contacten, maken het mogelijk een werkelijke digitale identiteitskaart van de betrokken persoon op te stellen. Zo zal het mogelijk zijn te bepalen of een persoon die ervan verdacht wordt een strafbaar feit te hebben gepleegd, contact heeft opgenomen met een in het strafrecht gespecialiseerde advocaat, de datum, het uur en de duur te kennen van de communicatie, alsook het communicatiemateriaal van de gebruikers, de plaats van gebruik van de mobiele toestellen, enz. Die gegevens zijn nog preciezer dan die welke zijn opgenomen in de professionele agenda van een advocaat, die nochtans een vertrouwelijk stuk is.

29 De ontstentenis van onderscheid tussen de personen wier communicatie aan het beroepsgeheim is onderworpen en de anderen is onlangs door het Hof bekritiseerd in het arrest van 21 december 2016, Tele2 Sverige en Watson e.a. (C-203/15 en C-698/15, EU:C:2016:970) (hierna: „arrest Tele2 Sverige en Watson e.a.”).

30 Uit technisch oogpunt zou het eenvoudig zijn de gewone metagegevens en die welke betrekking hebben op houders van het beroepsgeheim te sorteren door middel van een filtermechanisme bij binnenkomst. De wetgever zou immers de communicatieoperatoren kunnen verplichten om nota te nemen van de hoedanigheid „houder van het beroepsgeheim” van een klant en om die informatie onderling te delen. Aldus zouden de operatoren de metagegevens die worden gegenereerd door de communicatie van advocaten en van andere houders van het beroepsgeheim niet toevoegen aan de samengestelde gegevensbanken.

31 Bovendien is in geen enkel controlemechanisme voorzien om de houders en de begunstigden van het beroepsgeheim de mogelijkheid te bieden zich te verzetten tegen het verzamelen, het bewaren of het kennisnemen van gegevens die gedekt zijn door het beroepsgeheim. Dat kennisnemen van de gegevens, zelfs indien zij achteraf niet worden overgelegd ter staving van een dossier, volstaat echter om afbreuk te doen aan het beroepsgeheim. De bij artikel 6 EVRM en artikel 47 van het Handvest gewaarborgde rechten worden niet in acht genomen, aangezien de bestreden wet niet de mogelijkheid biedt van enigerlei jurisdictionele controle.

32 Voorts worden de rechtzoekenden die het voorwerp uitmaken van een onderzoeks- of vervolgingsmaatregel wegens feiten die aanleiding kunnen geven tot strafrechtelijke veroordelingen en de rechtszoekenden die niet het voorwerp uitmaken van een dergelijke maatregel door de bestreden bepalingen op identieke wijze behandeld. Het strafrecht steunt echter op het beginsel van vermoeden van onschuld met als logisch uitvloeisel dat de bewijslast op het openbaar ministerie rust en dat de vervolgde persoon het voordeel van de twijfel geniet. Het zou

bijgevolg niet relevant zijn het feit aan te voeren dat de maatregel evengoed ten goede kan komen aan het slachtoffer van een strafbaar feit. Daardoor zijn de bij de bestreden wet opgelegde bewaringsverplichtingen buitensporig ten opzichte van de doelstellingen van de wetgever.

33 De veralgemeende bewaring van gegevens, ook voor personen die niets te maken hebben met criminaliteit, schendt dus het evenredigheidsbeginsel. Die schending wordt bevestigd door de arresten van het Hof Digital Rights Ireland e.a. en Tele2 Sverige en Watson e.a. alsook door de conclusie van advocaat-generaal Cruz Villalón in de gevoegde zaken Digital Rights Ireland e.a. (C-293/12 en C-594/12, EU:C:2013:845), en door het arrest van de verwijzende rechter nr. 84/2015 van 11 juni 2015.

34 De verplichting tot algemene en ongedifferentieerde bewaring van identificatiegegevens, van verbindings- en lokalisatiegegevens en van persoonlijke communicatiegegevens die bij de bestreden wet wordt opgelegd, vormt een inmenging in het recht op bescherming van de persoonlijke levenssfeer die in een democratische samenleving niet strikt noodzakelijk is ter waarborging van de nationale veiligheid, met andere woorden de veiligheid van de staat, de landsverdediging, de openbare veiligheid of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronische-communicatiesysteem zoals bepaald in artikel 13, lid 1, van richtlijn 95/46.

35 In het arrest Tele2 Sverige en Watson e.a. heeft het Hof bevestigd dat het Unierecht zich verzette tegen een nationale regeling die in een algemene en ongedifferentieerde bewaring van de gegevens voorziet. Gesteld dat een dergelijke algemene bewaarplicht op zich niet kan worden geacht de grenzen van het strikt noodzakelijke te overschrijden, moet zij in elk geval worden omringd met alle waarborgen die het Hof in het arrest Digital Rights Ireland e.a. en in het arrest Tele2 Sverige en Watson e.a. heeft aangehaald. Die waarborgen zijn dwingend, cumulatief en minimaal (conclusie van advocaat-generaal Saugmandsgaard Øe in de gevoegde zaken Tele2 Sverige e.a., C-203/15 en C-698/15, EU:C:2016:572).

36 De in de bestreden wet bedoelde verplichting tot het bewaren van gegevens stemt grotendeels overeen met de in de richtlijn 2006/24 bedoelde verplichting tot het bewaren van gegevens, zoals het Hof in de punt 97 van het arrest Tele2 Sverige en Watson e.a. heeft vastgesteld.

37 De in de bestreden wet bedoelde algemene verplichting tot het bewaren van gegevens maakt een bijzonder ernstige aantasting van het recht op eerbiediging van het privé- en gezinsleven en van het recht op bescherming van persoonsgegevens uit. Zij heeft ook een weerslag op het gebruik van elektronische communicatiemiddelen en dus op de wijze waarop de gebruikers van die communicatiemiddelen gebruikmaken van hun vrijheid van meningsuiting. Dit heeft tot gevolg dat er ook sprake is van schending van de internationale en grondwetsbepalingen die die vrijheid van meningsuiting waarborgen. Rekening

houdend met de ernst van de aantasting van die grondrechten, zou enkel de bestrijding van zware criminaliteit die maatregel kunnen verantwoorden. De bestrijding van zware criminaliteit kan op zich echter geen algemene en ongedifferentieerde bewaring van alle verkeersgegevens en alle locatiegegevens verantwoorden (arrest Tele2 Sverige en Watson e.a., punt 103). Dat zou immers erop neerkomen dat het bewaren van die gegevens de regel wordt, terwijl, volgens richtlijn 2002/58, het verbod om die gegevens te bewaren de regel is, terwijl de bewaring ervan een uitzondering vormt. Bovendien heeft het arrest Tele2 Sverige en Watson e.a. betrekking op elke nationale regeling ter bestrijding van criminaliteit die voorziet in een algemene verplichting tot het bewaren van gegevens en niet alleen wanneer het gaat om de bestrijding van zware criminaliteit. Hoewel elke burger met dat soort van criminaliteit kan worden geconfronteerd als inverdenkinggestelde, slachtoffer of mogelijke getuige, valt de in het geding zijnde regeling binnen de werkingssfeer van artikel 15 van richtlijn 2002/58. Het arrest Tele2 Sverige en Watson e.a. is er dus op van toepassing.

38 In het arrest Tele2 Sverige en Watson e.a. heeft het Hof gepreciseerd dat een nationale regeling op grond waarvan de verkeersgegevens en de locatiegegevens ter bestrijding van zware criminaliteit preventief gericht kunnen worden bewaard, kan worden aanvaard in de in dat arrest uitgedrukte strikt noodzakelijke mate. De wetgever stelt in de parlementaire voorbereiding dat een dergelijke gerichte bewaring onmogelijk is. De redenering van de Belgische Staat berust in werkelijkheid op een politieke wil om te allen prijze voort te gaan op de weg van de algemene bewaring van gegevens onder het voorwendsel van een context van terroristisch risico en ondanks de ongrondwettigheid van het ingevoerde veralgemeende toezichtsysteem. Gesteld al dat het werkelijk onmogelijk zou zijn a priori categorieën van personen te bepalen die niet door de zware strafbare feiten zouden kunnen worden geraakt of erbij zouden kunnen zijn betrokken, zou dat het niet mogelijk maken een dermate ernstige inmenging in het privéleven van de burgers te verantwoorden. De logische uitkomst zou moeten zijn geen dergelijke maatregel in te voeren.

39 Ten slotte, hoewel in de memorie van toelichting bij de wet wordt verwezen naar het belang van communicatiegegevens voor onderzoeken inzake terrorisme, kinderpornografie, onrustwekkende verdwijningen, de illegale handel in verdovende middelen, de verkoop van namaakgeneesmiddelen op het internet, het aanzetten tot haat of tot geweld, belaging, inbreken op bankrekeningen en identiteitsdiefstal, wordt de noodzaak van een algemene bewaarplicht met het oog op de bestrijding van zware criminaliteit in verschillende studies ter discussie gesteld (conclusie van advocaat-generaal Saugmandsgaard Øe in de gevoegde zaken Tele2 Sverige e.a., C-203/15 en C-698/15, EU:C:2016:572).

40 Subsidiair voeren de verzoekende partijen aan dat het arrest Digital Rights Ireland e.a. op twee manieren kan worden geïnterpreteerd: in een eerste interpretatie zou de onwettigheid van de verplichting tot algemene en ongedifferentieerde bewaring van gegevens voortvloeien uit het ontbreken van voldoende waarborgen met betrekking tot de toegang tot de bewaarde gegevens en de bewaartermijn; in een

tweede interpretatie zou de bewaarplicht onwettig zijn, net door het algemene en ongedifferentieerde karakter ervan. In de memorie van toelichting bij de wet wordt eveneens erkend dat de verplichting tot algemene en ongedifferentieerde bewaring van gegevens niet overeenstemde met dat arrest, maar wordt geoordeeld dat dat kan worden gecompenseerd door een striktere regeling met betrekking tot de andere aspecten, namelijk een differentiatie op grond van de categorieën van bewaarde gegevens en het nut ervan, de regels inzake de toegang van de overheden tot de betrokken gegevens en de regels inzake de beveiliging van de gegevens bij de operatoren. Er moet dus worden vastgesteld dat de verplichting tot algemene bewaring van gegevens evenmin beantwoordt aan de soepele interpretatie die van dat arrest is gemaakt wegens de ontstentenis van waarborgen om die inmenging te beperken tot hetgeen strikt noodzakelijk is.

41 Het is juist dat de operatoren reeds gegevens bewaren om redenen van facturering. De bestreden wet verbiedt hun de bewaarde gegevens te gebruiken voor andere doeleinden dan die welke bij de wet zijn bepaald, inclusief dus voor de facturering van hun diensten. Bovendien legt de bestreden wet hun de verplichting op elementen te bewaren die zij niet zouden bewaren, niet in die vorm en, en in elk geval, niet gedurende dezelfde periode.

42 Daarenboven bestaat er een niet te verwaarlozen risico dat de relevante gegevensbanken lichtzinnig worden beheerd door de operatoren die terughoudend zijn ten opzichte van de controle die die nieuwe verplichting met zich meebrengt.

43 Geen enkele onafhankelijke autoriteit houdt toezicht op de naleving door de operatoren van het niveau van beveiliging en bescherming van de bewaarde gegevens. De verantwoordelijke personen die door de bestreden wet in dit verband zijn aangewezen, zijn alle personeelsleden van de operatoren, die zich in een ondergeschikte positie bevinden.

44 Bovendien biedt de bestreden wet de operatoren de mogelijkheid verzamelde gegevens met het oog op bewaring en om redenen van onderaanneming naar andere lidstaten van de Europese Unie over te dragen, zulks ondanks het gevoelige en vertrouwelijke karakter van sommige gegevens, hetgeen het risico dat zij toegankelijk kunnen zijn voor derden of kunnen worden verspreid aanzienlijk doet toenemen. Bovendien staan de nationale regelingen die van toepassing zijn in andere lidstaten, bijvoorbeeld de Franse regeling, de inlichtingendiensten toe, van operatoren informatie te verkrijgen over de gegevens welke zij verwerken.

– *ii) Duur van de bewaring*

45 Wat de duur van de bewaring van de gegevens betreft, bepaalt de bestreden wet in essentie dat de gegevens gedurende twaalf maanden worden bewaard, welke termijn op zich buitensporig is. Het is juist dat voor de strafbare feiten die geen hoofdgevangenisstraf van een jaar of meer tot gevolg kunnen hebben, de

gevorderde gegevens slechts de zes maanden voorafgaand aan de aanvraag kunnen betreffen. Die strafbare feiten zijn evenwel weinig talrijk.

46 De aanvangspunten van de bewaringstermijnen worden evenmin in verband gebracht met omstandigheden die eventueel de bewaring van de gegevens verantwoorden. Overigens kunnen de identificatiegegevens de facto gedurende een veel langere termijn bewaard kunnen blijven dan twaalf maanden aangezien de bewaartermijn aanvangt „de datum waarop communicatie voor de laatste maal mogelijk is via de gebruikte dienst".

47 In andere Europese landen worden kortere bewaringstermijnen gehanteerd. Er wordt verwezen naar een arrest van het Duitse grondwettelijke hof waarbij de Duitse wet betreffende de bewaring van telecommunicatiegegevens is vernietigd, en naar het arrest Digital Rights Ireland e.a.

48 De bewaartermijn is ook vatbaar voor kritiek, omdat hij voor alle categorieën gegevens gelijk is, terwijl hij moet worden gedifferentieerd naar categorieën van gegevens, het nut ervan voor het nagestreefde doel of de betrokken personen, en voor zover de termijn beperkt is tot het strikt noodzakelijke. Deze gelijke behandeling van ongelijke categorieën van bewaarde gegevens is niet redelijk verantwoord en is bijgevolg discriminerend.

49 Ten slotte verplicht de bestreden wet de overheid die toegang heeft gehad tot gegevens niet tot vernietiging van die gegevens indien zij geen verband houden met het doel waarvoor zij zijn verzameld of wanneer zij niet meer strikt noodzakelijk zijn voor de bestrijding van ernstige criminaliteit.

– *iii) Toegang tot de gegevens*

50 De bestreden wet biedt aan zes verschillende overheden de mogelijkheid om toegang te krijgen tot de bewaarde gegevens en beperkt die toegang niet strikt tot de overheden die betrokken zijn bij de strijd tegen criminaliteit, laat staan zware criminaliteit.

51 De bestreden wet maakt het de autoriteiten mogelijk toegang te krijgen tot de bewaarde gegevens, zonder dat die toegang wordt beperkt tot de zware criminaliteit. De in de bestreden wet vastgestelde aanvullende waarborgen inzake het beroepsgeheim, hebben geen betrekking op andere aan het beroepsgeheim onderworpen personen dan advocaten, artsen en journalisten. Artikel 458 van het Strafwetboek [in welke bepaling de eerbiediging van het beroepsgeheim wordt voorgeschreven] ziet op meer personen dan die welke deze drie beroepen uitoefenen. Bovendien zijn sommige personen, overheden en organisaties niet aan een beroepsgeheim onderworpen zijn terwijl de communicatie met hen toch een zekere vertrouwelijkheid moet kunnen genieten met toepassing van andere bepalingen. Bovendien vormt de procureur des Konings geen rechterlijke instantie of onafhankelijke bestuurlijke autoriteit.

52 De bestreden wet biedt de inlichtingen- en veiligheidsdiensten toegang tot de bewaarde gegevens. Het werkterrein van deze diensten werd te ruim omschreven. De communicatiegegevens van alle burgers kunnen naargelang van het karakter van de potentiële dreiging worden opgevraagd voor een periode van zes, negen of twaalf maanden vóór de beslissing tot toegang. De bestreden wet kan dus leiden tot machtsmisbruik ten nadele van individuen of organisaties die kritisch staan tegenover de regering of het politieke systeem. De persvrijheid zou eveneens in gevaar worden gebracht door het feit dat de inlichtingen- en veiligheidsdiensten alle telefonische en internetcommunicatie kunnen opvragen van journalisten. De bestreden wet zou ook zelfcensuur kunnen uitlokken of versterken bij de burger die het vage gevoel heeft te worden gecontroleerd, hetgeen een invloed kan hebben op de uitoefening van zijn vrijheid van meningsuiting en van informatie en zodoende een inmenging ten aanzien van artikel 11 van het Handvest.

53 Er is geen nauwkeurige beschrijving van de omstandigheden en van de voorwaarden inzake het verlenen van toegang. De toegang is evenmin onderworpen aan enige materiële of procedurele voorwaarde, aangezien de aanbieders eenvoudigweg verplicht zijn elk verzoek van de zes aangeduide overheden in te willigen. In zijn arrest Tele2 Sverige en Watson e.a. heeft het Hof evenwel bevestigd dat de nationale regeling moet voorzien in passende waarborgen, met andere woorden duidelijke en nauwkeurige regels die aangeven in welke omstandigheden en onder welke voorwaarden de aanbieders aan de bevoegde nationale autoriteiten toegang moeten verlenen. In hetzelfde arrest is ook gepreciseerd dat in beginsel enkel toegang kan worden verleend tot de gegevens van personen die ervan worden verdacht een ernstig misdrijf te plannen, te plegen of te hebben gepleegd of op een of andere wijze bij een dergelijk misdrijf betrokken te zijn. Bovendien moet de toegang worden onderworpen aan een voorafgaand toezicht door een rechterlijke instantie of door een onafhankelijke bestuurlijke entiteit. In de bestreden wet is echter geen enkele procedureregel vastgesteld nog enige autoriteit aangewezen die over het verzoek tot het ontvangen van gegevens kan oordelen. De enige controles waarin is voorzien, zijn controles achteraf.

54 Voorts wordt in het arrest Tele2 Sverige en Watson e.a. de term „ernstig risico voor de openbare veiligheid” gebruikt. De bestreden wet neemt dit criterium niet in acht, daar het gaat om de gewone en specifieke methoden van de inlichtingendiensten en deze betrekking hebben op minder ernstige inbreuken op de veiligheid dan de bijzondere methoden.

55 Ten slotte voorziet de bestreden wet niet in enige verplichting om personen ervan op de hoogte te brengen dat toegang tot hun privégegevens is verleend. Dit ontneemt hun ook een doeltreffend en effectief recht van beroep.

56 Wat de toegangstermijn betreft, maakt de wet enkel een onderscheid naar de aard van de inbreuk en dreiging, maar niet naar de aard van de bewaarde gegevens.

2. Middelen van de Belgische Staat

57 De Ministerraad is van mening dat de bestreden wet een antwoord biedt op de kritiek die door het Hof en door de verwijzende rechter is geformuleerd met betrekking tot de vroeger van toepassing zijnde regelgeving.

58 Het beroepsgeheim van de advocaat, hoewel het onder de openbare orde valt, is niet absoluut. Het evenredigheidsbeginsel „moet het mogelijk maken de grenzen te beoordelen die worden gesteld door de noodzakelijkheid of andere beginselen of waarden die in voorkomend geval met dat beroepsgeheim in strijd zijn".

59 Wat de toegang tot de gegevens betreft, voorziet de bestreden wet in grenzen met betrekking tot het beroepsgeheim, inzonderheid dat van de advocaat. De wet beoogt slechts de metagegevens, met uitsluiting van de inhoud van de communicatie. Zij raakt bijgevolg niet echt de vertrouwelijkheid van de contacten tussen de advocaat en zijn cliënt. Het zou daarentegen onevenredig zijn de communicatie van en naar de beoefenaars van beroepen die aan het beroepsgeheim onderworpen zijn, volledig aan de wettelijke regeling te onttrekken. Het is immers niet omdat een e-mailadres door een houder van het beroepsgeheim wordt gebruikt dat alle boodschappen die op dat adres terechtkomen of er vandaan komen daadwerkelijk door het beroepsgeheim worden beschermd. De houders van het beroepsgeheim kunnen zelf zware strafbare feiten plegen.

60 Ten aanzien van de rechtzoekenden die hun advocaat niet langer in vertrouwen zouden kunnen nemen, heeft de wetgever alle voorzorgen genomen opdat aan de nagestreefde doelstelling, waarvan de legitimiteit niet wordt betwist, kan worden voldaan zonder op onevenredige wijze afbreuk te doen aan het recht op privéleven en aan het recht op een eerlijk proces.

61 Met betrekking tot het al dan niet bewaren van gegevens naargelang de betrokkene al dan niet houder van een beroepsgeheim is, werden in de parlementaire voorbereiding van de wet de technische moeilijkheden van dergelijke oplossingen onderstreept alsook het feit dat andere lidstaten van de Unie geen technische formule hebben kunnen vinden om een onderscheid te maken. Bovendien zou een dergelijk onderscheid niet zozeer het beroepsgeheim zelf beschermen dan wel de persoon van diegene die, door zijn beroep, houder is van geheimen. Dat onderscheid zou tot gevolg hebben dat niet alleen datgene wat onder het beroepsgeheim valt, maar ook datgene wat er helemaal niet onder valt, van het toepassingsgebied van de wet wordt uitgesloten onder het voorwendsel dat voor de verzamelde informatie hetzelfde kanaal zou worden gebruikt als voor de informatie die onder het beroepsgeheim zou vallen.

62 Wat betreft de ontstentenis van mogelijkheid van beroep tegen de beslissing waarbij de maatregel van raadpleging van de bewaarde gegevens wordt voorgeschreven, alsook tegen de maatregelen genomen op basis van die beslissing, maakt de toegang tot de bewaarde gegevens daadwerkelijk het

voorwerp uit van een jurisdictionele controle in het kader van het strafonderzoek, die wordt uitgevoerd door de BIM Commissie [bestuurlijke Commissie belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten], samengesteld uit onafhankelijke magistraten, in het geval dat het de inlichtingendiensten zijn die toegang hebben tot de informatie. De procureur des Konings is van zijn kant wel degelijk een onafhankelijke entiteit is wanneer hij zijn onderzoeksbevoegdheden in het kader van het Wetboek van strafvordering uitoefent en de waarborg biedt dat de uitoefening van zijn bevoegdheden niet op onredelijke wijze afbreuk doet aan het recht op bescherming van de persoonlijke levenssfeer.

63 Wat de termijn betreft gedurende welke de gegevens worden bewaard, wordt bij de wet in een gradatie voorzien die in essentie gebaseerd is op de ernst van het strafbare feit. De bewaringsverplichting gaat logischerwijs vooraf aan de toegang tot de bewaarde informatie. Alleen het verzoek om toegang zal het mogelijk maken de ernst te bepalen van het strafbare feit of de dreiging. Aangezien de wet bepaalt dat de toegang tot de betrokken informatie wordt gemoduleerd door de ernst van het strafbare feit of van de dreiging, is het moeilijk, informatiecategorie per informatiecategorie, a priori te bepalen wat het nut ervan zal zijn voor een specifiek onderzoek. Tot slot geeft de verzoekende partij niet aan waarom de aldus bij de wet bepaalde termijnen op zich onevenredig zouden zijn.

64 De wetgever heeft alle mogelijkheden onderzocht om tegemoet te komen aan de rechtspraak van het Hof. Een verdere differentiatie op het vlak van de bewaringstermijn van de gegevens is na een grondig onderzoek van die kwestie onmogelijk gebleken. Het is gebleken dat een termijn van twaalf maanden noodzakelijk is om terroristische misdrijven te bestrijden.

65 Met betrekking tot de ontstentenis van een onderscheid onder de rechtsonderhorigen naargelang zij al dan niet het voorwerp uitmaken van een onderzoek of vervolging, biedt het dispositief van de bestreden wet de speurders net de mogelijkheid biedt toegang te hebben tot bepaalde metagegevens over een persoon die het voorwerp uitmaakt van een dergelijk onderzoek. Dat veronderstelt dat die metagegevens voorafgaandelijk aan het onderzoek en dus op een ogenblik dat het niet mogelijk was het onderscheid te maken, werden bewaard.

66 Wat het risico betreft dat de operatoren de bewaarde gegevens lichtzinnig behandelen, maakt de naleving door de operatoren van hun wettelijke verplichtingen het voorwerp uit van controle door de sectorale regulator, waarbij die controle gepaard gaat met sancties die kunnen gaan tot de intrekking van een licentie. De bestreden wet voorziet in een groot aantal waarborgen betreffende de beveiliging van gegevens.

67 Geen enkel ander preventief systeem zou kunnen vermijden dat gegevens die onder het beroepsgeheim vallen, worden bewaard en dat men toegang ertoe kan hebben. Om te bepalen of informatie onder het beroepsgeheim valt, dient zij noodzakelijkerwijs vooraf te worden verwerkt.

68 De nationale wetgevingen in Zweden en het Verenigd Koninkrijk die door het Hof in zijn arrest Tele2 Sverige en Watson e.a. zijn onderzocht, hadden de strijd tegen zware criminaliteit ten doel, terwijl de bestreden wet een ruimere doelstelling heeft. Bijgevolg kan de door het Hof geconstateerde onaangepastheid of onevenredigheid van een nationale wetgeving ten opzichte van de doelstelling van bestrijding van de zware criminaliteit niet mutatis mutandis worden toegepast op een nationale wetgeving waarvan de doelstelling verschillend is.

69 Het is juist dat het Hof heeft geoordeeld dat een regeling die het verzamelen en het bewaren van de gegevens met betrekking tot de elektronische communicatie en de toegang van de bevoegde nationale autoriteiten daartoe zou toestaan, niet in strijd zou zijn met het Unierecht, indien die regeling gericht was. Die deur die door het Hof wordt opengezet, zou echter theoretisch zijn. Het Hof is in dat arrest immers niet ertoe gebracht de overeenstemming te onderzoeken van een concrete regeling die in die zin gericht zou zijn. Het is twijfelachtig of een dergelijk systeem kan worden ingevoerd zonder een schending van het beginsel van gelijkheid onder burgers met zich mee te brengen.

70 Uit de parlementaire voorbereiding blijkt dat het doel van de bestreden wet verschilt van de concrete situatie die door het Hof is onderzocht in de arresten Digital Rights Ireland e.a. en Tele2 Sverige en Watson e.a. In die arresten diende het Hof zich immers uit te spreken over de vraag of de verplichting tot het bewaren van algemene en ongedifferentieerde gegevens noodzakelijk en evenredig was ten aanzien van de bestrijding van zware criminaliteit. De bestreden wet streeft een ander doel na. Het gaat erom de integriteit van het strafrechtsysteem te waarborgen, alsook het vertrouwen van de burger in de werking van justitie te verbeteren door het zoeken naar de waarheid, in het belang van het slachtoffer, van de inverdenkinggestelde en van alle betrokken personen.

71 Er bestaat een redelijk verband van evenredigheid tussen de algemene verplichting tot het bewaren van gegevens en het door de wetgever nagestreefde doel dat bovendien volledig in overeenstemming zou zijn met artikel 15, lid 1, van richtlijn 2002/58. Hoewel niet elke burger immers potentieel een crimineel is, kan elke burger wel potentieel met criminaliteit worden geconfronteerd, zowel als slachtoffer, als beklaagde of als getuige, en bijgevolg een belang hebben bij de waarheidsvinding. Ondanks de algemene verplichting tot het bewaren van gegevens, zijn de nodige waarborgen ter bescherming van de privacy ingevoerd op het gebied van de bewaring van de gegevens en op het gebied van de toegang tot de gegevens. Rekening houdend met die waarborg, heeft de bij de wet voorgeschreven verplichting, geen onevenredig karakter. De bestreden wet is niet strijdig met de rechtspraak van het Hof.

72 Wat de vroegere wetgeving betreft, was geoordeeld dat het recht op eerbiediging van de persoonlijke levenssfeer onevenredig was aangetast wegens de combinatie van vier elementen: het feit dat de bewaring van gegevens betrekking had op alle personen, de ontstentenis van een verschil in behandeling op grond van de categorieën van bewaarde gegevens en het nut ervan, het gebrek aan of de

ontoereikendheid van regels, hetgeen een inmenging in het recht op bescherming van de persoonlijke levenssfeer zou uitmaken.

73 Noch het Hof, noch de verwijzende rechter heeft evenwel geoordeeld dat een van die vier elementen kon volstaan om tot het onevenredige karakter van de maatregel te besluiten. De toetsing van het evenredigheidsbeginsel houdt immers een globale aanpak in. De veralgemeende verplichting tot het bewaren van gegevens gaat gepaard met voldoende waarborgen op het vlak van de toegang tot de gegevens, de bewaartermijnen, de bescherming en de beveiliging van de gegevens, zodat de inmenging wordt beperkt tot hetgeen strikt noodzakelijk is.

74 De bestreden wet is in overeenstemming met artikel 15, lid 1, van richtlijn 2002/58, ook wanneer het erom gaat gegevens te bewaren en ze mee te delen aan de bevoegde overheden voor het onderzoeken, opsporen en vervolgen van andere vormen van criminaliteit dan zware criminaliteit, wanneer het leven of de fysieke integriteit van personen of goederen in gevaar is, of wanneer onrechtmatig gebruik wordt gemaakt van systemen voor elektronische communicatie.

75 Het arrest Tele2 Sverige en Watson e.a. vereist niet dat die waarborgen een cumulatief karakter hebben en zet die vaststelling geenszins op de helling.

76 Ten slotte verwijst de Belgische Staat naar de parlementaire voorbereiding van de bestreden wet.

VII. Korte uiteenzetting van de motivering van de verwijzing

77 De vroegere wetgeving, die bij de bestreden wet is vervangen, is door de verwijzende rechter vernietigd in zijn arrest nr. 84/2015 van 11 juni 2015, waarvan de motivering uitvoerig wordt aangehaald in het onderhavige verzoek om een prejudiciële beslissing. Dit arrest is beschikbaar op de website van het Grondwettelijk Hof van België: http://www.const-court.be/public/n/2015/2015-084n.pdf.

78 De verwijzende rechter verwijst voorts naar de parlementaire voorbereiding van de wet (Doc. parl. Kamer, 2015-2016, DOC 54-1567, die beschikbaar is op: https://www.lachambre.be/kvvcr/showpage.cfm?section=/flwb&language=nl&cfm=/site/wwwcfm/flwb/flwbn.cfm?lang=N&legislat=54&dossierID=1567).

79 De verwijzende rechter wijst erop dat uit de parlementaire voorbereiding van de bestreden wet blijkt dat de wetgever zowel zijn voormelde arrest nr. 84/2015 van 11 juni 2015 als het daaraan ten grondslag liggende arrest van het Hof Tele2 Sverige en Watson e.a. grondig heeft onderzocht.

80 Daaruit blijkt dat het doel dat de wetgever met de bestreden wet nastreeft erin bestaat 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.

81 De wetgever heeft een gerichte en gedifferentieerde bewaarplicht in het licht van de vooropgestelde doelstelling niet mogelijk geacht en ervoor 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 dit verband is erop gewezen dat een a priori differentiatie naar personen, periodes en geografische zones eenvoudigweg niet mogelijk zou zijn. In de parlementaire voorbereiding werd deze onmogelijkheid omstandig toegelicht (zie document 1, punten 7-10, http://www.lachambre.be/FLWB/PDF/54/1567/54K1567001.pdf).

82 Met zijn arrest van 21 december 2016, Tele2 Sverige en Watson e.a. (C-203/15 en C-698/15, EU:C:2016:970), dat dus dateert van nadat de bestreden wet is aangenomen, heeft het Hof twee prejudiciële vragen beantwoord met betrekking tot de uitlegging van artikel 15, lid 1, van richtlijn 2002/58.

83 Het Hof komt in punt 78 van dat arrest tot de conclusie dat „een wettelijke maatregel waarbij een lidstaat op grond van artikel 15, lid 1, van richtlijn 2002/58, ter verwezenlijking van de in die bepaling vermelde doelstellingen, aan de aanbieders van elektronische communicatiediensten de verplichting oplegt om de nationale autoriteiten onder de in een dergelijke maatregel genoemde voorwaarden toegang te verlenen tot de door die aanbieders bewaarde gegevens, betrekking [heeft] op de verwerking van persoonsgegevens door die aanbieders, en [dat] deze verwerking [...] binnen de werkingssfeer van die richtlijn [valt]”.

84 Het Hof brengt in herinnering dat artikel 5, lid 1, van de richtlijn bepaalt dat de lidstaten via nationale wetgeving het vertrouwelijke karakter van de communicatie via openbare communicatienetwerken en via openbare elektronische communicatiediensten en van de daarmee verband houdende verkeersgegevens moeten waarborgen. Het beginsel van vertrouwelijkheid impliceert een verbod voor derden om zonder toestemming van de gebruikers verkeersgegevens betreffende hun elektronische communicatie op te slaan (punten 84 en 85).

85 Het Hof brengt eveneens in herinnering dat artikel 15, lid 1, van de richtlijn de lidstaten toestaat te voorzien in uitzonderingen op de in het voormelde artikel 5, lid 1, geformuleerde principeverplichting, die volgens vaste rechtspraak van het Hof strikt moeten worden uitgelegd. „[Artikel 15] kan dus niet rechtvaardigen dat de in artikel 5 van deze richtlijn bepaalde uitzondering op deze principeverplichting en, in het bijzonder, op het verbod om deze gegevens op te slaan de regel wordt, omdat laatstgenoemde bepaling in dat geval grotendeels haar inhoud zou verliezen” (punten 88 en 89).

86 In dat verband „[bepaalt] artikel 15, lid 1, eerste zin, van richtlijn 2002/58 [...] dat de aldaar bedoelde wettelijke maatregelen die afwijken van het beginsel van

vertrouwelijkheid van de communicaties en van de daarmee verband houdende verkeersgegevens, tot doel moeten hebben de ‚waarborging van de nationale [veiligheid], d.w.z. de staatsveiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronischecommunicatiesysteem', of een van de andere doelen genoemd in artikel 13, lid 1, van richtlijn 95/46, waarnaar artikel 15, lid 1, eerste zin, van richtlijn 2002/58 verwijst (zie in die zin arrest van 29 januari 2008, Promusicae, C-275/06, EU:C:2008:54, punt 53). Een dergelijke opsomming van doelstellingen is exhaustief, zoals blijkt uit artikel 15, lid 1, tweede zin, van deze richtlijn, volgens welke de wettelijke maatregelen moeten worden gerechtvaardigd door ‚de redenen' die in artikel 15, lid 1, eerste zin, van die richtlijn worden genoemd. Bijgevolg mogen de lidstaten dergelijke maatregelen niet treffen voor andere doeleinden dan die welke in laatstgenoemde bepaling worden genoemd" (punt 90).

87 Met betrekking tot de draagwijdte van artikel 15, lid 1, van de richtlijn komt het Hof tot de slotsom dat:

„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 bepalingen genoemde doelstellingen. In overweging 11 van deze richtlijn wordt gepreciseerd dat een dergelijke maatregel ‚strikt' evenredig moet zijn met het nagestreefde doel. Wat in het bijzonder de bewaring van gegevens betreft, eist artikel 15, lid 1, tweede zin, van deze richtlijn dat deze gegevens slechts ‚gedurende een beperkte periode' worden bewaard ‚om de redenen' die in artikel 15, lid 1, eerste zin, van die richtlijn worden genoemd" (punt 95).

88 Het Hof onderzoekt vervolgens of een nationale regeling zoals die welke van toepassing is op de eerste zaak die aanleiding heeft gegeven tot de prejudiciële vragen die bij het Hof aanhangig zijn gemaakt, aan die voorwaarden voldoet. Het Hof stelt vast dat de in het geding zijnde nationale regeling voorziet in een algemene en ongedifferentieerde bewaring van alle verkeersgegevens en locatiegegevens van alle abonnees en geregistreerde gebruikers betreffende alle elektronischecommunicatiemiddelen, en de aanbieders van elektronischecommunicatiediensten verplicht die gegevens stelselmatig en voortdurend te bewaren zonder enige uitzondering. Aan de hand van de aldus bewaarde gegevens kunnen de bron en de bestemming van een communicatie worden opgespoord en geïdentificeerd en kunnen de datum, het tijdstip en de duur van die communicatie, de communicatieapparatuur van de gebruikers en de locatie van de mobiele communicatieapparatuur worden bepaald (punten 97 en 98).

89 Volgens het Hof kunnen uit die gegevens, in hun geheel beschouwd, zeer precieze conclusies worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard. Aan de hand van die gegevens kan het profiel van de

betrokken personen worden bepaald, informatie die, wat het recht op bescherming van het privéleven betreft, even gevoelig is als de inhoud zelf van de communicaties.

90 De verwijzende rechter citeert de punten 100 tot en met 112 van het arrest Tele2 Sverige en Watson e.a. integraal.

91 Op de tweede prejudiciële vraag in de zaak C-203/15 en de eerste prejudiciële vraag in de zaak C-698/15 antwoordt het Hof dat artikel 15, lid 1, van richtlijn 2002/58, gelezen tegen de achtergrond van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, in die zin moet worden uitgelegd dat het zich verzet tegen een nationale regeling die de bescherming en de beveiliging van de verkeersgegevens en van de locatiegegevens en in het bijzonder de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens regelt zonder, in het kader van de bestrijding van criminaliteit, te bepalen dat die toegang alleen wordt verleend ter bestrijding van ernstige criminaliteit, dat die toegang aan een voorafgaand toezicht door een rechterlijke instantie of een onafhankelijke bestuurlijke autoriteit is onderworpen, en dat de betrokken gegevens op het grondgebied van de Unie moeten worden bewaard (punt 125).

92 Het Europees Hof voor de Rechten van de Mens (hierna: „EHRM") van zijn kant heeft de Zweedse wetgeving inzake het massief onderscheppen van elektronische communicatie inmiddels in overeenstemming bevonden met artikel 8 EVRM (EHRM, 19 juni 2018, Centrum för Rättvisa tegen Zweden, CE:ECHR:2018:0619JUD003525208). Dat Hof hanteert daarvoor de criteria die het in zijn vroegere rechtspraak heeft ontwikkeld (EHRM, 4 december 2015, Roman Zakharov tegen Rusland, CE:ECHR:2015:1204JUD004714306)). Het merkte inzonderheid op:

„Het Hof heeft uitdrukkelijk erkend dat de nationale overheden over een ruime beoordelingsmarge beschikken bij de keuze hoe zij het legitieme doel van vrijwaring van de nationale veiligheid het best kunnen bereiken (zie Weber and Saravia, hogervermeld, § 106). In Weber and Saravia en Liberty and Others aanvaardde het Hof dat de regels inzake het massief onderscheppen niet per se buiten die marge vielen. Gelet op de redenering van het Hof in die arresten en rekening houdend met de dreigingen waarmee vele verdragsluitende Staten geconfronteerd worden (met name wereldwijd terrorisme en andere ernstige vormen van criminaliteit zoals drugshandel, mensenhandel, seksuele uitbuiting van kinderen en cybercriminaliteit), met de technologische evoluties waardoor terroristen en criminelen gemakkelijker kunnen ontkomen aan hun opsporing via het internet en met de onvoorspelbaarheid van de kanalen via welke elektronische communicatie wordt doorgegeven, is het Hof van oordeel dat de beslissing om een regeling inzake het massief onderscheppen in te voeren teneinde tot dusver onbekende dreigingen voor de nationale veiligheid te identificeren een beslissing is die nog steeds onder de beoordelingsmarge van de Staten valt" (EHRM, 19 juni 2018, Centrum för Rättvisa tegen Zweden, CE:ECHR:2018:0619JUD003525208, § 112)

93 OBFG 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.

Dezelfde verzoekende 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.

94 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.

95 ASBL Académie fiscale en een particulier 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.

96 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.

97 Liga voor Mensenrechten en Ligue des Droits de l'Homme 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.

98 Een aantal natuurlijke personen die in België wonen en verschillende elektronischecommunicatiediensten gebruiken in het kader van een met een operator gesloten overeenkomst, klagen 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.

99 De wetgever heeft drie categorieën van metagegevens willen vaststellen die moeten worden bewaard – de identificatiegegevens, de toegangs- en verbindingsgegevens en de communicatiegegevens –, de voorwaarden voor de toegang tot de gegevens door de bevoegde overheden willen verstrengen en de beveiliging van de door de operatoren bewaarde gegevens willen versterken, in de interpretatie van de arresten van het Hof volgens welke een veralgemeende verplichting tot het bewaren van gegevens zou kunnen worden toegestaan indien die verplichting gepaard gaat met dergelijke waarborgen.

100 Artikel 95 van verordening 2016/679 bepaalt dat die verordening natuurlijke personen of rechtspersonen geen aanvullende verplichtingen oplegt met betrekking tot verwerking in verband met het verstrekken van openbare elektronische-communicatiediensten in openbare communicatienetwerken in de Unie, voor zover zij op grond van richtlijn 2002/58 onderworpen zijn aan specifieke verplichtingen met dezelfde doelstelling.

101 Artikel 15, lid 1, van richtlijn 2002/58 bepaalt dat de lidstaten onder andere wetgevingsmaatregelen kunnen treffen om gegevens gedurende een beperkte periode te bewaren om redenen die in dat lid worden genoemd, met name de nationale veiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronische-communicatiesysteem, onder de voorwaarden die in die bepaling worden gepreciseerd.

102 De bestreden wet bepaalt onder meer de voorwaarden waaronder de inlichtingen- en veiligheidsdiensten gegevens mogen ontvangen van de aanbieders en operatoren.

103 In dit verband dient te worden vastgesteld dat in de zaak Privacy International, C-623/17, een rechterlijke instantie van de Unie de volgende vragen heeft voorgelegd aan het Hof:

„Overwegende hetgeen volgt:

a. de capaciteiten (van de veiligheids- en inlichtingendiensten) om de aan hen geleverde bulkcommunicatiegegevens te gebruiken zijn essentieel voor de bescherming van de nationale veiligheid van het Verenigd Koninkrijk, waaronder op het gebied van terrorismebestrijding, contraspionage en de bestrijding van nucleaire proliferatie;

b. een fundamenteel element van het gebruik van bulkcommunicatiegegevens door de veiligheids- en inlichtingendiensten is om voorheen onbekende bedreigingen voor de nationale veiligheid te ontdekken door middel van niet-gerichte bulktechnieken die afhankelijk zijn van de aggregatie van bulkcommunicatiegegevens op één plaats. Het belangrijkste nut ervan ligt in een snelle identificatie en ontwikkeling van het doelwit, alsook het voorzien van een grond voor actie in geval van een onmiddellijke bedreiging;

c. de leverancier van een elektronischecommunicatienetwerk is daarna niet verplicht om de bulkcommunicatiegegevens te bewaren (na de periode van hun gebruikelijke bedrijfsmatige vereisten); deze worden enkel bewaard door de Staat (veiligheids- en inlichtingendiensten);

d. de nationale rechter heeft vastgesteld dat de waarborgen die betrekking hebben op het gebruik van bulkcommunicatiegegevens door de veiligheids- en inlichtingendiensten (onder voorbehoud van enkele buiten beschouwing gelaten kwesties) in overeenstemming zijn met het EVRM; en

e. de nationale rechter heeft vastgesteld dat de oplegging van de vereisten die gespecifieerd zijn in de punten 119 tot en met 125 van het arrest [Tele2 Sverige en Watson e.a.], indien van toepassing, de maatregelen van de veiligheids- en inlichtingendiensten om de nationale veiligheid te beschermen zullen dwarsbomen en daardoor de nationale veiligheid van het Verenigd Koninkrijk in gevaar brengen;

1. Valt een vereiste in een aanwijzing van een minister aan een leverancier van een elektronische communicatienetwerk dat bulkcommunicatiegegevens verstrekt worden aan de veiligheids- en inlichtingendiensten van een lidstaat, gezien artikel 4 VEU en artikel 1, lid 3, van richtlijn 2002/58/EG betreffende de persoonlijke levenssfeer en elektronische communicatie, binnen de werkingssfeer van het Unierecht en de e-privacyrichtlijn?

2. Indien het antwoord op de eerste vraag bevestigend is: zijn de in het arrest Watson geformuleerde vereisten of andere vereisten, naast de vereisten die worden opgelegd door het EVRM, van toepassing op een dergelijke aanwijzing van een minister? Zo ja, hoe en in welke mate zijn deze vereisten van toepassing,

rekening houdende met de essentiële noodzaak voor de veiligheids- en inlichtingendiensten om bulkverwerving en automatische verwerkingstechnieken te gebruiken voor de bescherming van de nationale veiligheid en met de mate waarin dergelijke mogelijkheden op kritieke wijze belemmerd kunnen worden door dergelijke vereisten, voor zover zij verder in overeenstemming zijn met het EVRM?"

104 De verwijzende rechter zal met het antwoord op die prejudiciële vragen rekening moeten houden bij zijn onderzoek.

105 De bestreden wet bepaalt ook de voorwaarden waaronder de gerechtelijke autoriteiten met het oog op het opsporen, het onderzoek en de vervolging van inbreuken gegevens mogen ontvangen.

106 Bijgevolg dient ook het antwoord afgewacht te worden dat het Hof zal geven op de prejudiciële vraag in de zaak Ministerio Fiscal, C-207/16:

„Geldt als criterium om te bepalen of een delict voldoende ernstig is om inmenging in de door de artikelen 7 en 8 van het Handvest erkende grondrechten te rechtvaardigen, uitsluitend de straf die kan worden opgelegd ter zake van het onderzochte delict of is het bovendien noodzakelijk dat door de strafbaar gestelde gedraging individuele en/of collectieve rechtsgoederen in bijzondere mate worden aangetast?

Indien het verenigbaar is met de constitutionele beginselen van de Unie die het Hof heeft toegepast in zijn arrest Digital Rights als maatstaven voor de strikte toetsing van de richtlijn, dat de ernst van het delict uitsluitend wordt vastgesteld op basis van de op te leggen straf, wat zou dan het minimumniveau van de straf moeten zijn? Zou een algemeen vereiste van minimaal drie jaar gevangenisstraf voldoen?"

Uit de conclusie van advocaat-generaal Saugmandsgaard Øe in deze zaak (C-207/16, EU:C:2018:300) blijkt dat de relevante bepalingen voor meerdere interpretaties vatbaar zijn.

107 De partijen voor de verwijzende rechter verschillen voorts van mening over de interpretatie die moet gegeven worden aan meerdere bepalingen die de verwijzende rechter in zijn toetsing van de bestreden wet dient te betrekken, inzonderheid artikel 15, lid 1, van richtlijn 2002/58 en de artikelen 7, 8, 11 en 52 van het Handvest.

108 Het Hof heeft evenwel, zo geven de verzoekende partijen aan, bij zijn arrest Tele2 Sverige en Watson e.a. geoordeeld dat artikel 5, lid 1, van richtlijn 2002/58 een principeverplichting bevat tot waarborging van de vertrouwelijkheid van de communicatie en van de daarmee verband houdende verkeersgegevens, en dat artikel 15, lid 1, van dezelfde richtlijn, die uitzonderingen op dat principe bevat, strikt moet worden uitgelegd, om te vermijden dat de in artikel 5 van de richtlijn

bepaalde uitzondering op de principeverplichting de regel wordt, omdat laatstgenoemde bepaling in dat geval grotendeels haar inhoud zou verliezen.

109 Het Hof heeft eveneens beklemtoond dat enkel de in artikel 15 vermelde doelstellingen een maatregel kunnen verantwoorden die afwijkt van het beginsel van vertrouwelijkheid van de communicaties en van de daarmee verband houdende verkeersgegevens, aangezien artikel 15 in dat verband vereist dat de gegevens slechts gedurende een beperkte periode worden bewaard om de redenen die erin worden opgesomd.

110 Bijgevolg vormt, zo onderstrepen de verzoekende partijen, een nationale regeling die voorziet in een algemene en ongedifferentieerde bewaring van alle verkeersgegevens en locatiegegevens van alle abonnees en geregistreerde gebruikers betreffende alle elektronischecommunicatiemiddelen zonder dat de gebruikers erover worden ingelicht, volgens het Hof, een bijzonder ernstige inmenging in de in de artikelen 7 en 8 van het Handvest vastgelegde grondrechten uit, zodat alleen de bestrijding van ernstige criminaliteit een dergelijke maatregel kan rechtvaardigen. Het Hof voegt eraan toe dat, hoewel die doelstelling van algemeen belang is, zij op zich niet kan rechtvaardigen dat een nationale regeling die voorziet in algemene en ongedifferentieerde bewaring van alle verkeersgegevens en alle locatiegegevens, noodzakelijk wordt geacht voor het voeren van die strijd.

111 Op grond daarvan oordeelt het Hof dat een nationale regeling die in geen enkele differentiatie, beperking of uitzondering naargelang van het nagestreefde doel voorziet, en die algemeen betrekking heeft op alle personen die gebruik maken van elektronischecommunicatiediensten, zonder geografisch onderscheid of onderscheid in de tijd, zonder dat rekening wordt gehouden met het feit dat die personen zich, al was het maar indirect, in een situatie bevinden die aanleiding kan geven tot strafvervolging of dat de communicatie van de gegevens betrekking heeft op personen van wie de communicaties onder het beroepsgeheim vallen, of zonder enig verband tussen de gegevens die moeten worden bewaard en een bedreiging van de openbare veiligheid te vereisen, de grenzen van het strikt noodzakelijke overschrijdt en niet kan worden beschouwd als een regeling die in een democratische samenleving gerechtvaardigd is, zoals artikel 15 van de richtlijn, gelezen tegen de achtergrond van de artikelen 7, 8, 11 en 52, lid 1, van het Handvest, vereist.

112 Het Hof geeft volgens de verzoekende partijen weliswaar aan dat artikel 15, lid 1, van richtlijn 2002/58 niet in de weg staat aan een nationale regeling op grond waarvan de verkeersgegevens en de locatiegegevens ter bestrijding van zware criminaliteit gericht kunnen worden bewaard, op voorwaarde dat de bewaring van die gegevens, wat de categorieën van te bewaren gegevens, de betrokken communicatiemiddelen, de betrokken personen en de duur van de bewaring betreft, tot het strikt noodzakelijke wordt beperkt. Zulks houdt in dat de nationale regeling duidelijke en nauwkeurige regels bevat, en dat de personen op wie de bewaring van gegevens betrekking heeft, voldoende garanties genieten dat hun

persoonsgegevens doeltreffend worden beschermd tegen het risico van misbruik. Het Hof voegt eraan toe dat de nationale regeling in het bijzonder moet aangeven in welke omstandigheden en onder welke voorwaarden een maatregel van bewaring van gegevens preventief kan worden genomen. Een dergelijke regeling moet worden gebaseerd op objectieve elementen waarmee kan worden gemikt op een groep mensen wier gegevens een band met zware criminaliteit aan het licht kunnen brengen of die een ernstig risico voor de openbare veiligheid vertonen, waarbij die afbakening aan de hand van een geografisch criterium kan worden verricht wanneer de bevoegde nationale autoriteiten, op basis van objectieve elementen, van mening zijn dat er in een of meer geografische zones een hoog risico bestaat dat dergelijke handelingen worden voorbereid of gepleegd.

113 De wetgever streeft, met het aannemen van de bestreden wet, evenwel ruimere doelstellingen na dan de bestrijding van zware criminaliteit of het risico van een ernstige aantasting van de openbare veiligheid.

114 De wetgever heeft in de parlementaire voorbereiding eveneens meermaals aangegeven dat hij, met betrekking tot het beginsel zelf van de verplichting tot het bewaren van gegevens, alle personen beoogde, ook al zijn zij nog niet betrokken bij een onderzoek; hij heeft daarenboven geen onderscheid gemaakt naargelang de periode, de geografische zone of een kring van personen en heeft evenmin voorzien in een uitzondering ten aanzien van de personen wier communicaties onder het beroepsgeheim vallen.

115 Hoewel de voorwaarden voor de toegang tot de bewaarde gegevens aanzienlijk werden verstrengd in de bestreden wet, beantwoordt de algemene verplichting tot het bewaren van gegevens waarin zij voorziet, volgens de verzoekende partijen, niet aan de vereisten die zijn voorgeschreven bij artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8, 11 en 52, lid 1, van het Handvest, volgens de uitlegging die het Hof bij zijn arrest Tele2 Sverige en Watson e.a. eraan heeft gegeven. Een dergelijke verplichting overschrijdt immers de grenzen van het strikt noodzakelijke is en kan niet worden beschouwd als een verplichting die in een democratische samenleving gerechtvaardigd is, zoals de voormelde Europese bepalingen vereisen.

116 De Ministerraad van zijn kant beklemtoont dat het doel van de bestreden regeling meervoudig is. De wetgever beoogt in de eerste plaats de reeds jaar en dag bestaande situatie waarbij toegang tot gegevens in de telecommunicatiesector verkregen wordt in het kader van strafrechtelijke onderzoeken te bestendigen door het creëren van een wetgevend kader dat de nodige waarborgen omvat op het vlak van de bescherming van de persoonlijke levenssfeer. De bewaarplicht wordt ook ingevoerd met het oog op de waarheidsvinding van vele vormen van criminaliteit en beoogt hiermee de integriteit van het strafrechtsysteem te waarborgen. Die waarheidsvinding is in het belang van zowel het slachtoffer, de beschuldigde (die bijvoorbeeld kan aantonen dat hij ergens anders was op het ogenblik van de feiten), als alle andere betrokken personen. De bewaarplicht is eveneens ingegeven vanuit de doelstellingen die erin bestaan actie te ondernemen om

gevolg te geven aan een oproep naar een nooddienst of een vermiste persoon op te sporen wiens fysieke integriteit in onmiddellijk gevaar is. Dat element zou een belangrijk verschil zijn ten opzichte van de situaties die aan de orde waren in voormelden arresten van het Hof. Bijgevolg zou er een band van evenredigheid bestaan tussen de algemene bewaarplicht en het door de wetgever vooropgestelde doel.

117 De Ministerraad beklemtoont nog 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 bescherming van de persoonlijke levenssfeer tot een minimum zou worden beperkt. In dit verband wijst de Ministerraad erop dat een a priori differentiatie naar personen, periodes en geografische zones eenvoudigweg niet mogelijk is. In dat verband verwijst hij nog naar de conclusie van advocaat-generaal Saugmandsgaard Øe in de gevoegde zaken Tele2 Sverige e.a., C-203/15 en C-698/15, EU:C:2016:572.

118 Uit de aan de verwijzende rechter ter beschikking staande gegevens blijkt dat het merendeel van de lidstaten overigens grote moeilijkheden blijken te kennen om hun wetgeving inzake de bewaring van telecommunicatiegegevens in overeenstemming te brengen met de eisen die door het Hof in zijn rechtspraak zijn gesteld (zie: Data retention across the EU, http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention; Brief van de Nederlandse minister van Justitie en Veiligheid van 26 maart 2018 aan de voorzitter van de Tweede Kamer der Staten-Generaal, Tweede Kamer, vergaderjaar 2017-2018, 34 537, nr. 7).

119 Bijgevolg is het aangewezen de eerste in het dictum vermelde prejudiciële vraag te stellen aan het Hof.

120 De bestreden wet beoogt ook een effectief strafrechtelijk onderzoek en een daadwerkelijke bestraffing van seksueel misbruik van minderjarigen mogelijk te maken en het effectief mogelijk te maken om de pleger van zodanig misdrijf te identificeren, ook wanneer gebruik wordt gemaakt van elektronische communicatiemiddelen. Ter terechtzitting is in dit verband gewezen op de positieve verplichtingen die volgen uit de artikelen 3 en 8 EVRM inzake de bescherming van de fysieke en morele integriteit van minderjarigen en andere kwetsbare personen, zoals geïnterpreteerd door het EHRM (EHRM, 2 december 2008, K.U. tegen Finland, CE:ECHR:2008:1202JUD000287202, §§46-49). Die verplichtingen zouden ook kunnen volgen uit de overeenstemmende bepalingen van het Handvest en zulks zou gevolgen kunnen hebben voor de uitlegging van artikel 15, lid 1, van richtlijn 2002/58.

121 Bijgevolg is het aangewezen de tweede in het dictum vermelde prejudiciële vraag te stellen.

122 Het is tot slot aangewezen de derde in het dictum vermelde prejudiciële vraag te stellen.

VIII. Prejudiciële vragen

123 Het Grondwettelijk Hof stelt aan het Hof van Justitie van de Europese Unie de volgende vragen:

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?