Voorlopige editie

CONCLUSIE VAN ADVOCAAT-GENERAAL
M. CAMPOS SÁNCHEZ-BORDONA
van 15 januari 2020 (1)

Zaak C-520/18

Ordre des barreaux francophones et germanophone,
Académie Fiscale ASBL,
UA,
Liga voor Mensenrechten ASBL,
Ligue des Droits de l'Homme ASBL,
VZ,
WY,
XX
tegen
Ministerraad,
in tegenwoordigheid van:
Child Focus

[verzoek van het Grondwettelijk Hof (België) om een prejudiciële beslissing]

„Prejudiciële verwijzing – Verwerking van persoonsgegevens en bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie – Richtlijn 2002/58/EG – Werkingssfeer – Artikel 1, lid 3 – Artikel 15, lid 1 – Artikel 4, lid 2, VEU – Handvest van de grondrechten van de Europese Unie – Artikelen 4, 6, 7, 8 en 11 en artikel 52, lid 1 – Verplichting tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens – Doeltreffendheid van het strafrechtelijk onderzoek en andere doelstellingen van algemeen belang"

1. Het Hof heeft de afgelopen jaren een vaste lijn aangehouden in zijn rechtspraak met betrekking tot de bewaring van en de toegang tot persoonsgegevens, met als belangrijkste mijlpalen:

– het arrest van 8 april 2014, Digital Rights Ireland e.a.(2), waarbij richtlijn 2006/24/EG(3) ongeldig is verklaard omdat die een onevenredige inmenging in de in de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie neergelegde rechten mogelijk maakte;

– het arrest van 21 december 2016, Tele2 Sverige en Watson e.a.(4), waarin het uitlegging heeft gegeven aan artikel 15, lid 1, van richtlijn 2002/58/EG(5), en

– het arrest van 2 oktober 2018, Ministerio Fiscal(6), waarin het de uitlegging van diezelfde bepaling van richtlijn 2002/58 heeft bevestigd.

2. Deze arresten (in het bijzonder het tweede) baren de autoriteiten van bepaalde lidstaten zorgen, omdat zij hun een instrument zouden ontnemen dat zij noodzakelijk achten om de nationale veiligheid te waarborgen en criminaliteit en terrorisme te bestrijden. Sommige van deze lidstaten pleiten er daarom voor dat het Hof terugkomt die rechtspraak of deze rechtspraak nuanceert.

3. Enkele rechterlijke instanties van de lidstaten hebben diezelfde bezorgdheid geuit in vier prejudiciële verwijzingen(7), waarin ik heden conclusie neem.

4. In die vier zaken rijst allereerst de vraag of richtlijn 2002/58 van toepassing is op activiteiten die verband houden met de nationale veiligheid en de strijd tegen terrorisme. Als deze richtlijn in die context van toepassing is, moet vervolgens worden opgehelderd in hoeverre de lidstaten de door de richtlijn beschermde privacyrechten kunnen beperken. Tot slot moet worden geanalyseerd in welke mate de verschillende nationale regelingen ter zake (de Britse(8), de Belgische(9) en de Franse(10)) verenigbaar zijn met het Unierecht, zoals dat door het Hof is uitgelegd.

5. Nadat het Hof arrest had gewezen in de zaak Digital Rights verklaarde het Grondwettelijk Hof (België) de nationale regeling nietig waarbij gedeeltelijk uitvoering was gegeven aan richtlijn 2006/24, die bij dat arrest ongeldig was verklaard. De Belgische wetgever stelde vervolgens een nieuwe regeling vast, waarvan de verenigbaarheid met het Unierecht echter in twijfel werd getrokken naar aanleiding van het arrest Tele2 Sverige en Watson.

6. Specifiek voor deze prejudiciële verwijzing is dat de mogelijkheid wordt geopperd om tijdelijk de gevolgen te handhaven van een nationale regeling die door de nationale rechters nietig moet worden verklaard omdat zij onverenigbaar is met het Unierecht.

I. Toepasselijke bepalingen

A. Unierecht

7. Ik verwijs naar het desbetreffende deel van mijn conclusie in de gevoegde zaken C-511/18 en C-512/18.

B. Nationaal recht. Wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie

8. In artikel 4 van de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie(11) is bepaald dat artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie(12) komt te luiden als volgt:

„§ 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 houdende regeling van de inlichtingen- en veiligheidsdiensten[(13)] te vervullen en volgens de voorwaarden vastgelegd in die wet;

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.

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

Die statistieken omvatten met name:

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

2° de tijd die is verstreken tussen de datum waarop de gegevens zijn bewaard en de datum waarop de bevoegde autoriteiten om de overdracht ervan verzochten;

3° de gevallen waarin verzoeken om gegevens niet konden worden ingewilligd.

Die statistieken mogen geen persoonsgegevens omvatten.

[...]"

9. Bij artikel 5 wordt in de wet van 2005 een artikel 126/1 ingevoegd, dat luidt:

„§ 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 1998].

[...]

§ 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.

[...]

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.

[...]

§ 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.

[...]"

10. Artikel 8 herformuleert artikel 46bis, § 1, van het Wetboek van strafvordering als volgt:

„§ 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 [...].

[...]

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."

11. Overeenkomstig artikel 9 komt artikel 88bis van het Wetboek van strafvordering te luiden als volgt:

„§ 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 [...] 2005 [...], 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, gebruikmaken 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. [...] 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.

§ 4. [...]”

12. Overeenkomstig artikel 12 wordt artikel 13 van de wet van 1998 geherformuleerd als volgt:

„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.”

13. Bij artikel 14 wordt artikel 18/3 van de wet van 1998 gewijzigd. In artikel 18/3 is nu bepaald:

„§ 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."

14. Artikel 18/8 van de wet van 1998 wordt vervangen als volgt:

„§ 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 [...] 2005 [...], 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.

[...]"

II. Feiten van het hoofdgeding en prejudiciële vragen

15. Bij zijn arrest van 11 juni 2015(14) heeft het Grondwettelijk Hof de nieuwe versie van artikel 126 van de wet van 2005 vernietigd om redenen die identiek zijn aan die welke het Hof ertoe hadden gebracht richtlijn 2006/24 ongeldig te verklaren in het arrest Digital Rights.

16. In het licht van die vernietiging heeft de nationale wetgever de wet van 29 mei 2016 vastgesteld (voordat het arrest Tele2 Sverige en Watson werd gewezen).

17. VZ e.a., de Ordre des barreaux francophones et germanophone (hierna: „Ordre des barreaux"), de Liga voor Mensenrechten ASBL (hierna: „Liga"), de Ligue des Droits de l'Homme ASBL (hierna: „Ligue") en de Académie Fiscale ASBL (hierna: „Académie Fiscale") hebben bij de verwijzende rechter verschillende beroepen ingesteld tot vaststelling dat die wet ongrondwettig is. Daarbij stellen zij in wezen dat de wet verder gaat dan strikt noodzakelijk is en onvoldoende waarborgen voor bescherming biedt.

18. Binnen deze context verzoekt het Grondwettelijk Hof het Hof van Justitie om een prejudiciële beslissing over 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 [‚Handvest'], en het recht op eerbiediging van de persoonsgegevens, zoals gewaarborgd bij de artikelen 7 en 8 en artikel 52, lid 1, van het Handvest [...], 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 [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) (PB 2016, L 119, blz. 1)] 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 en 11 en artikel 52, lid 1, van het Handvest [...], 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 [bestreden] wet [...] 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?"

III. Procedure bij het Hof

19. De prejudiciële verwijzing is ter griffie van het Hof ingekomen op 2 augustus 2018.

20. VZ e.a., de Académie Fiscale, de Liga, de Ligue, de Ordre des barreaux, de Stichting voor Vermiste en Seksueel Uitgebuite Kinderen (Child Focus), de Belgische, de Cypriotische, de Deense, de Duitse, de Estse, de Franse, de Hongaarse, de Ierse, de Nederlandse, de Poolse, de Spaanse, de Tsjechische en de Zweedse regering, de regering van het Verenigd Koninkrijk alsmede de Commissie hebben schriftelijke opmerkingen ingediend.

21. Op 9 september 2019 werd een gezamenlijke openbare terechtzitting gehouden voor de onderhavige zaak en de zaken C-511/18, C-512/18 en C-623/17, waaraan de partijen bij de vier prejudiciële verwijzingen, de voornoemde regeringen en de regering van Noorwegen, alsmede de Commissie en de Europese Toezichthouder voor gegevensbescherming hebben deelgenomen.

IV. Analyse

22. De eerste vraag van deze verwijzing komt grotendeels overeen met de vragen die zijn gesteld in de zaken C-511/18 en C-512/18. Zij verschilt echter van die vragen uit het oogpunt van de doelstellingen van de nationale regeling, die niet alleen bestaan in het bestrijden van terrorisme en de meest ernstige vormen van criminaliteit of het waarborgen van de nationale veiligheid, maar ook in „de verdediging van het grondgebied en van de openbare veiligheid, het onderzoeken, opsporen en vervolgen van andere feiten dan die van zware criminaliteit" en, in het algemeen, alle doelen omvatten zoals opgenomen in artikel 23, lid 1, van verordening 2016/679.

23. De tweede vraag sluit aan bij de eerste, maar vormt er ook een aanvulling op in die zin dat de verwijzende rechter wenst te vernemen of de op de overheid rustende positieve verplichtingen ten aanzien van het onderzoek en de bestraffing van seksueel misbruik van minderjarigen de bestreden maatregelen kunnen rechtvaardigen.

24. De derde vraag wordt gesteld voor het geval dat de nationale regeling onverenigbaar is met het Unierecht. De verwijzende rechter wenst te vernemen of de gevolgen van de wet van 29 mei 2016 in dat geval tijdelijk kunnen worden gehandhaafd.

25. Om deze vragen te beantwoorden, zal ik eerst onderzoeken of richtlijn 2002/58 van toepassing is. In dat verband verwijs ik naar mijn conclusie in een andere van deze prejudiciële verwijzingen. Vervolgens zal ik de belangrijkste tendensen in de desbetreffende rechtspraak van het Hof en de mogelijke evolutie daarvan beschrijven. Tot slot buig ik mij over het op elk van de prejudiciële vragen te geven antwoord.

A. Toepasselijkheid van richtlijn 2002/58

26. Net zoals in de drie andere prejudiciële verwijzingen worden ook in deze verwijzing twijfels geuit over de toepasselijkheid van richtlijn 2002/58. Aangezien de standpunten van de lidstaten dienaangaande overeenkomen, verwijs ik wat dit betreft naar mijn conclusie in de gevoegde zaken C-511/18 en C-512/18.(15)

B. Rechtspraak van het Hof over de bewaring van persoonsgegevens en de toegang van de overheid tot die gegevens in het kader van richtlijn 2002/58

1. Beginsel van vertrouwelijkheid van de communicatie en van de daarmee verband houdende gegevens

27. De bepalingen van richtlijn 2002/58 vormen een „specificatie van en een aanvulling op" richtlijn 95/46/EG(16), teneinde te zorgen voor een hoge mate van bescherming van de persoonsgegevens bij de verlening van elektronischecommunicatiediensten.(17)

28. In artikel 5, lid 1, van richtlijn 2002/58 is bepaald dat de lidstaten via nationale wetgeving het vertrouwelijke karakter garanderen van de communicatie die plaatsvindt via openbare communicatienetwerken en via openbare elektronischecommunicatiediensten, alsook van de daarmee verband houdende verkeersgegevens.

29. Het vertrouwelijke karakter van de communicatie impliceert onder meer (artikel 5, lid 1, tweede zin, van richtlijn 2002/58) een verbod op de opslag van de met de communicatie verband houdende verkeersgegevens door anderen dan de gebruikers, indien de betrokken gebruikers daarin niet hebben toegestemd. Er wordt een uitzondering gemaakt voor „personen die [...] de wettelijke toelating hebben gekregen, en voor de technische opslag die nodig is voor het overbrengen van informatie".(18)

30. De artikelen 5 en 6 en artikel 9, lid 1, van richtlijn 2002/58 hebben tot doel het vertrouwelijke karakter van de communicatie en van de daarmee verband houdende gegevens te waarborgen en het risico op misbruik tot een minimum te beperken. De draagwijdte ervan dient te worden beoordeeld in het licht van overweging 30 van die richtlijn, die luidt dat „[s]ystemen voor elektronischecommunicatienetwerken en -diensten [...] op dusdanige wijze [moeten] worden ontworpen dat het aantal persoonsgegevens tot het strikt noodzakelijke *minimum* wordt beperkt".(19)

31. Met betrekking tot die gegevens kan een onderscheid worden gemaakt tussen:

– *verkeersgegevens*, waarvan de verwerking en opslag slechts is toegestaan voor zover en zolang dat nodig is voor de facturering en de marketing van de diensten en voor de levering van diensten met toegevoegde waarde (artikel 6 van richtlijn 2002/58). Zodra die periode is verstreken, moeten de verwerkte en opgeslagen gegevens worden gewist of anoniem worden gemaakt.(20)

– andere *locatiegegevens* dan verkeersgegevens, die slechts onder bepaalde voorwaarden mogen worden verwerkt nadat zij anoniem zijn gemaakt of wanneer de gebruikers of abonnees daarvoor hun toestemming hebben gegeven (artikel 9, lid 1, van richtlijn 2002/58).(21)

2. Beperkende clausule in artikel 15, lid 1, van richtlijn 2002/58

32. Artikel 15, lid 1, van richtlijn 2002/58 staat de lidstaten toe om „wettelijke maatregelen [te] 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".

33. Een eventuele beperking moet „in een democratische samenleving noodzakelijk, redelijk en proportioneel [zijn] 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 elektronischecommunicatiesysteem als bedoeld in artikel 13, lid 1, van richtlijn [95/46]".

34. Deze opsomming van doelstellingen is exhaustief(22): bij wijze van voorbeeld („o.a.") kunnen „wetgevingsmaatregelen [worden getroffen] om gegevens gedurende een beperkte periode te bewaren om de redenen die in dit lid worden genoemd".

35. Hoe dan ook „[dienen] alle in dit lid bedoelde maatregelen [...] 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". Artikel 15, lid 1, van richtlijn 2002/58 moet dan ook worden uitgelegd in het licht van de bij het Handvest gewaarborgde grondrechten.(23)

36. Van die in het Handvest erkende rechten heeft het Hof, voor zover hier van belang, het recht op eerbiediging van het privéleven (artikel 7), het recht op bescherming van persoonsgegevens (artikel 8) en het recht op vrijheid van meningsuiting (artikel 11) genoemd.(24)

37. Voorts heeft het Hof, als richtsnoer voor zijn uitlegging van artikel 15, lid 1, richtlijn 2002/58, onderstreept dat de beperkingen van de verplichting tot waarborging van de vertrouwelijkheid van de communicatie en van de daarmee verband houdende verkeersgegevens, strikt moeten worden uitgelegd.

38. Concreet heeft het de mogelijkheid uitgesloten dat de „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".(25)

39. Deze dubbele constatering is mijns inziens bepalend om te begrijpen waarom het Hof heeft geoordeeld dat de algemene en ongedifferentieerde bewaring van met de elektronische communicatie verband houdende verkeers- en locatiegegevens onverenigbaar is met richtlijn 2002/58.

40. Met die vaststelling heeft het Hof gewoon een „strikte"(26) toepassing gegeven aan het evenredigheidscriterium dat het eerder al had gebruikt(27): „de bescherming van het grondrecht op eerbiediging van het privéleven op het niveau van de Unie vereist dat de uitzonderingen op de bescherming van de persoonsgegevens en de beperkingen daarvan binnen de grenzen van het strikt noodzakelijke blijven".(28)

3. Evenredigheid bij de bewaring van gegevens

a) Onevenredig karakter van een algemene en ongedifferentieerde bewaring

41. Het Hof heeft erkend dat de bestrijding van zware criminaliteit, met name van georganiseerde misdaad en terrorisme, van primordiaal belang is om de openbare veiligheid te waarborgen, en dat de doeltreffendheid ervan in aanzienlijke mate kan afhangen van het gebruik van moderne onderzoekstechnieken. Het heeft daaraan toegevoegd dat „een dergelijke doelstelling van algemeen belang, hoe wezenlijk zij ook is, op zich [echter] niet kan rechtvaardigen dat een bewaringsmaatregel zoals die welke door richtlijn 2006/24 is ingevoerd, noodzakelijk wordt geacht voor het voeren van deze strijd".(29)

42. Om te bepalen of een dergelijke maatregel beperkt was tot het strikt noodzakelijke, heeft het Hof vooreerst onderstreept dat hij een bijzonder ernstige inmenging in de in de artikelen 7 en 8 van het Handvest vastgelegde grondrechten vormt.(30) Die bijzondere ernst vloeit precies voort uit het feit dat in de nationale wetgeving was voorzien 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*".(31)

43. De inmenging die deze maatregel vormde in het leven van de burgers blijkt uit de volgende beoordelingen die het Hof heeft gemaakt van de effecten die de bewaring van de gegevens teweegbrengt.

Aan de hand van die gegevens(32):

– „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"(33);

– „kan in het bijzonder worden nagegaan met welke persoon en met welk middel een abonnee of geregistreerde gebruiker heeft gecommuniceerd, hoe lang de communicatie heeft geduurd en vanaf welke plaats zij heeft plaatsgevonden. Bovendien kan aan de hand van deze gegevens worden achterhaald hoe vaak de abonnee of de geregistreerde gebruiker gedurende een bepaalde periode met bepaalde personen heeft gecommuniceerd"(34);

– „kunnen zeer precieze conclusies worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren”(35), en

– „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”.(36)

44. De inmenging kan bovendien bij „de betrokken personen het gevoel opwekken dat hun privéleven constant in de gaten wordt gehouden”, aangezien „de gegevens worden bewaard zonder dat de gebruikers van de elektronischecommunicatiediensten hierover worden ingelicht”.(37)

45. Gelet op de ernst van de ingreep kan alleen de bestrijding van ernstige criminaliteit een maatregel tot bewaring van gegevens met deze kenmerken rechtvaardigen.(38) Die maatregel mag echter niet de regel worden, aangezien „het bij richtlijn 2002/58 ingevoerde stelsel eist dat deze bewaring van gegevens de uitzondering vormt”.(39)

46. Voorts was er sprake van twee kenmerken die voortvloeiden uit het feit dat de aan de orde zijnde maatregel „in geen enkele differentiatie, beperking of uitzondering naargelang van het nagestreefde doel”(40) voorzag en „geen enkel verband” eiste „tussen de gegevens die moeten worden bewaard en een bedreiging van de openbare veiligheid”(41):

– enerzijds had de maatregel „algemeen betrekking op alle personen die gebruikmaken van elektronischecommunicatiediensten zonder dat deze personen zich, al was het maar indirect, in een situatie bevinden die aanleiding kan geven tot strafvervolging. [...] Bovendien bevat [hij] geen uitzonderingen, zodat [hij] zelfs van toepassing is op personen van wie de communicaties naar nationaal recht onder het beroepsgeheim vallen”(42);

– anderzijds „beperkt [hij] de bewaring [...] niet tot gegevens die betrekking hebben op een bepaalde periode en/of een bepaald geografisch gebied en/of een kring van personen die op een of andere wijze betrokken kunnen zijn bij een ernstig strafbaar feit, of op personen van wie de bewaring van de gegevens om andere redenen zou kunnen helpen bij de bestrijding van criminaliteit”.(43)

47. In die omstandigheden ging de geanalyseerde nationale regeling verder dan strikt noodzakelijk was. Zij kon dus niet worden beschouwd als een regeling die in een democratische samenleving gerechtvaardigd is, zoals 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, eist.(44)

b) Haalbaarheid van een gerichte bewaring van de gegevens

48. Het Hof heeft erkend dat het Unierecht niet in de weg staat aan een nationale regeling „op grond waarvan de verkeersgegevens en de locatiegegevens ter bestrijding van zware criminaliteit preventief *gericht* kunnen worden *bewaard*”.(45)

49. Deze gerichte bewaring is slechts geldig op voorwaarde dat zij „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”.

50. De richtsnoeren die het arrest Tele2 Sverige en Watson biedt om te bepalen wanneer aan die voorwaarden is voldaan, zijn niet exhaustief (en konden dat misschien ook niet zijn) en zijn in eerder algemene bewoordingen geformuleerd. Om aan deze voorwaarden te voldoen, moeten de lidstaten:

– duidelijke en nauwkeurige regels voor de draagwijdte en de toepassing van een dergelijke maatregel van bewaring van gegevens vaststellen(46);

– „objectieve criteria [vaststellen] die een verband leggen tussen de te bewaren gegevens en het nagestreefde doel”(47), en

– zich baseren „op objectieve elementen waarmee kan worden gemikt op een groep mensen wier gegevens, althans indirect, een band met handelingen van zware criminaliteit aan het licht kunnen brengen, waarmee op de een of andere wijze kan worden bijgedragen tot de bestrijding van zware criminaliteit of waarmee een ernstig risico voor de openbare veiligheid kan worden voorkomen".(48)

51. Met betrekking tot die objectieve elementen vermeldt het Hof dat bijvoorbeeld gebruik kan worden gemaakt van een geografisch criterium om het doelpubliek en de situaties die onder die maatregel kunnen vallen, af te bakenen. Met de vermelding van dat criterium, waarover sommige lidstaten zich kritisch hebben uitgelaten, heeft het Hof het spectrum van in aanmerking komende factoren om gegevens gericht te bewaren mijns inziens niet louter daartoe willen beperken.

4. Evenredigheid bij de toegang tot de gegevens

a) Arrest Tele2 Sverige en Watson

52. Het Hof bekijkt de *toegang* van de nationale instanties tot de gegevens los van de omvang van de aan de aanbieders van elektronischecommunicatiediensten opgelegde verplichting tot *bewaring* en, meer in het bijzonder, los van de algemene of gerichte aard van bewaring van de gegevens.(49)

53. Hoewel de bewaring logischerwijs bedoeld is om de latere toegang tot de gegevens te vergemakkelijken, kunnen bewaring en toegang immers onderscheiden inbreuken op de door het Handvest beschermde grondrechten veroorzaken. Dat onderscheid betekent echter niet dat bepaalde overwegingen met betrekking tot de bewaring niet evenzeer van toepassing zouden zijn op de toegang tot de bewaarde gegevens.

54. In die zin:

– moet de toegang „daadwerkelijk en strikt op een van [de] doelstellingen [...] berusten" die zijn opgenomen in artikel 15, lid 1, eerste zin, van richtlijn 2002/58. Ook moet het nagestreefde doel in verhouding staan tot de ernst van de inmenging. Indien de inmenging als ernstig wordt beschouwd, kan zij alleen worden gerechtvaardigd door de bestrijding van zware criminaliteit(50);

– kan de toegang alleen worden toegestaan binnen de grenzen van wat strikt noodzakelijk is.(51) Bovendien moeten de wettelijke maatregelen „duidelijke en nauwkeurige regels [...] bevatten over de omstandigheden waarin en de voorwaarden waaronder de aanbieders van elektronischecommunicatiediensten aan de bevoegde nationale autoriteiten toegang tot de gegevens moeten verlenen. Een maatregel van een dergelijke aard moet ook wettelijk verbindend zijn naar intern recht"(52);

– moeten de nationale regelingen meer in het bijzonder „de materiële en procedurele voorwaarden voor de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens bepalen".(53)

55. Uit het voorgaande kan worden afgeleid dat „een algemene toegang tot alle bewaarde gegevens los van enig – zelfs ook maar indirect – verband met het nagestreefde doel niet kan worden geacht tot het strikt noodzakelijke te zijn beperkt".(54)

56. Volgens het Hof „moet de betrokken nationale regeling [...] aan de hand van objectieve criteria bepalen in welke omstandigheden en onder welke voorwaarden aan de bevoegde nationale autoriteiten toegang tot de gegevens van de abonnees of de geregistreerde gebruikers moet worden verleend".(55) In dit verband „kan in beginsel voor het doel van bestrijding van de criminaliteit slechts toegang worden verleend *tot de gegevens van personen die ervan worden verdacht een ernstig misdrijf te plannen, te plegen of te hebben gepleegd of op de een of andere wijze betrokken te zijn bij een dergelijk misdrijf*".(56)

57. De nationale regelingen die de bevoegde nationale instanties toegang bieden tot de bewaarde gegevens, moeten met andere woorden een voldoende beperkte draagwijdte hebben. Er moet een verband bestaan tussen de betrokken personen en het nagestreefde doel; de toegang mag dus geen

aanzienlijk aantal personen, of zelfs alle personen, alle elektronischecommunicatiemiddelen of alle opgeslagen gegevens betreffen.

58. Deze regels kunnen in bepaalde omstandigheden echter worden getemperd. Het Hof vermeldt „bijzondere situaties, zoals die waarin vitale belangen van nationale veiligheid, landsverdediging of openbare veiligheid door terroristische activiteiten worden bedreigd". In dergelijke situaties „zou [...] ook toegang tot de gegevens van andere personen kunnen worden verleend, wanneer op grond van objectieve elementen kan worden geoordeeld dat deze gegevens in het concrete geval een daadwerkelijke bijdrage tot de bestrijding van dergelijke activiteiten zouden kunnen leveren".(57)

59. Deze precisering van het Hof maakt het de lidstaten mogelijk om een specifiek stelsel van ruimere toegang tot de gegevens in te stellen voor het uitzonderlijke geval dat dit noodzakelijk is om bedreigingen van de primordiale belangen van de staat (nationale veiligheid, landsverdediging en openbare veiligheid) te bestrijden(58), waardoor de toegang zelfs personen betreft die slechts indirect met deze risico's in verband worden gebracht.

60. De toegang van de nationale instanties tot de opgeslagen gegevens moet hoe dan ook aan drie voorwaarden voldoen:

– hij moet „in beginsel, behalve in gevallen van naar behoren gerechtvaardigde spoedeisendheid, [worden onderworpen] aan een voorafgaand toezicht door een rechterlijke instantie of door een onafhankelijke bestuurlijke entiteit". De beslissing van die rechterlijke instantie of entiteit moet worden gegeven „op een met redenen omkleed verzoek van deze autoriteiten dat met name is ingediend in het kader van procedures ter voorkoming, opsporing of vervolging van strafbare feiten"(59);

– „de bevoegde nationale autoriteiten waaraan toegang tot de bewaarde gegevens is verleend, [brengen] in het kader van de toepasselijke nationale procedures de betrokken personen daarvan op de hoogte [...] wanneer zulks de door deze autoriteiten gevoerde onderzoeken niet in gevaar kan brengen"(60), en

– de lidstaten moeten regels vaststellen betreffende de beveiliging en bescherming van de door de aanbieders van elektronischecommunicatiediensten bewaarde gegevens, teneinde het misbruik van en de onrechtmatige toegang tot die gegevens te voorkomen.(61)

b) Arrest Ministerio Fiscal

61. In deze zaak werd de vraag gesteld of artikel 15, lid 1, van richtlijn 2002/58, gelezen in samenhang met de artikelen 7 en 8 van het Handvest, zich verzet tegen een nationale regeling die voorziet in de toegang van de bevoegde instanties tot de gegevens inzake de burgerlijke identiteit van de houders van bepaalde simkaarten.

62. Het Hof verklaarde dat het bij de doelstelling om strafbare feiten te voorkomen, te onderzoeken, op te sporen en te vervolgen volgens artikel 15, lid 1, eerste zin, van richtlijn 2002/58 gaat om „strafbare feiten" in het algemeen, en niet alleen om de bestrijding van ernstige delicten.(62)

63. Het voegde daaraan toe dat, om de toegang van de nationale bevoegde instanties tot de gegevens te rechtvaardigen, de ernst van de inmenging in verhouding moet staan tot de ernst van de betrokken strafbare feiten. Bijgevolg:

– kan „ernstige inmenging slechts worden gerechtvaardigd door de doelstelling om – eveneens ‚ernstige' – criminaliteit te bestrijden"(63), en

– kan, indien „de inmenging die een dergelijke toegang veroorzaakt daarentegen niet ernstig [is], [...] die toegang worden gerechtvaardigd door de doelstelling van het voorkomen, onderzoeken, opsporen en vervolgen van ‚strafbare feiten' in het algemeen".(64)

64. Uitgaande van deze premisse, en anders dan in het arrest Tele2 Sverige en Watson, heeft het Hof de inmenging in de door de artikelen 7 en 8 van het Handvest beschermde rechten niet als „ernstig"

aangemerkt, aangezien het verzoek om toegang „louter tot doel [had] de houders te identificeren van de simkaarten die gedurende een periode van twaalf dagen met het IMEI-nummer van de gestolen mobiele telefoon zijn geactiveerd".(65)

65. Om te benadrukken dat de inmenging minder ernstig was, legde het Hof uit dat „[het] met de via het toegangsverzoek in het hoofdgeding beoogde gegevens [...] alleen mogelijk [is] om, gedurende een bepaalde periode, de met de gestolen mobiele telefoon geactiveerde simkaart(en) in verband te brengen met de civiele identiteit van de houders van die simkaarten. Zonder aanvullende gegevens over de communicatie die met die simkaarten tot stand is gebracht en over de locatie, kan met die gegevens noch de datum, het uur, de duur of de ontvanger van de met de betrokken simkaart(en) verrichte oproepen worden achterhaald, noch waar die communicatie heeft plaatsgevonden of hoe vaak in een gegeven periode met bepaalde personen is gecommuniceerd. Uit die gegevens kunnen dus geen nauwkeurige conclusies over het privéleven van de betrokken personen worden getrokken."(66)

66. In de zaak waarover in het arrest Ministerio Fiscal uitspraak werd gedaan, was niet aan de orde of de persoonsgegevens waartoe toegang werd verkregen door de aanbieders van elektronischecommunicatiediensten waren bewaard met inachtneming van de voorwaarden van artikel 15, lid 1, van richtlijn 2002/58, gelezen in samenhang met de artikelen 7 en 8 van het Handvest. (67) Evenmin werd ingegaan op de vraag of al dan niet was voldaan aan de overige voorwaarden voor toegang die uit dat artikel voortvloeien.

67. Uit het arrest Ministerio Fiscal kan dan ook geen verandering worden afgeleid in de rechtspraak van het Hof ten aanzien van de onverenigbaarheid met het Unierecht van een nationale regeling die de algemene en ongedifferentieerde opslag van gegevens toestaat in de zin van het arrest Tele2 Sverige en Watson.

68. Ik ben evenwel van oordeel dat het Hof, door de geldigheid te erkennen van een stelsel waarbij slechts toegang wordt gegeven tot bepaalde persoonsgegevens (de gegevens inzake de burgerlijke identiteit van de houders van simkaarten), impliciet aanvaardt dat diezelfde gegevens door de aanbieders van de dienst worden bewaard.

C. Belangrijkste punten van kritiek op de rechtspraak van het Hof

69. Zowel de verwijzende rechter als de meeste van de lidstaten die opmerkingen hebben ingediend, verzoeken het Hof om verschillende aspecten van zijn rechtspraak op dit gebied, waarop hun kritiek is gericht, te preciseren, te nuanceren of zelfs te heroverwegen.

70. Het overgrote deel van die verholen of openlijke kritiek werd reeds geuit ter gelegenheid van het arrest Digital Rights, en werd afgewezen in het arrest Tele2 Sverige en Watson. Nu worden die bezwaren opnieuw geopperd om in wezen te benadrukken dat strikte regels voor de toegang tot de gegevens waarover de aanbieders van elektronischecommunicatiediensten beschikken, zouden volstaan om de ernst van de inmenging die de algemene en ongedifferentieerde bewaring van die gegevens vormt in zekere zin te compenseren.

71. In verschillende van die bedenkingen wordt eveneens onderstreept dat er werkelijk doeltreffende maatregelen moeten worden genomen in de strijd tegen ernstige bedreigingen voor de veiligheid en tegen criminaliteit in het algemeen, en wordt het Hof gevraagd om rekening te houden met het recht op veiligheid (artikel 6 van het Handvest) en met de beoordelingsmarge waarover de lidstaten met betrekking tot het waarborgen van de nationale veiligheid beschikken. In een enkel geval wordt daar nog aan toegevoegd dat het Hof de preventieve aard van het ingrijpen door de veiligheids- en inlichtingendiensten niet heeft meegewogen.

D. Mijn beoordeling van die kritiek en van de nuances die in de rechtspraak van het Hof zouden kunnen worden aangebracht

72. Mijns inziens zou het Hof het principiële standpunt moeten handhaven dat het in zijn vorige arresten heeft ingenomen: een algemene en ongedifferentieerde verplichting om alle verkeers- en locatiegegevens van alle abonnees en geregistreerde gebruikers te bewaren vormt een onevenredige inbreuk op de door de artikelen 7, 8 en 11 van het Handvest beschermde rechten.

73. Omgekeerd zou een nationale wettelijke regeling waarbij passende beperkingen worden gesteld aan de bewaring van bepaalde van die gegevens, die zijn gegenereerd in verband met het aanbieden van elektronischecommunicatiediensten, wél verenigbaar kunnen zijn met het Unierecht. De sleutel ligt dus in de *beperkte bewaring* van die gegevens.

74. Om de redenen die ik hierna zal uiteenzetten, mag die beperkte bewaring niet aldus worden opgevat dat het uitsluitend gaat om de bewaring met betrekking tot een bepaald geografisch gebied of een bepaalde categorie van personen: uit de discussies over die bewaringscriteria blijkt dat zij mogelijk niet toepasbaar zijn, ondoeltreffend kunnen zijn met het oog op de nagestreefde doeleinden of zelfs tot discriminatie kunnen leiden.

75. Om te beginnen ben ik het oneens met de kritiek waarin wordt gepleit voor het binomium „ruimere bewaring in ruil voor beperktere toegang". De redenering van het Hof, waarbij ik mij aansluit, is dat de bewaring van en de toegang tot gegevens twee verschillende soorten vormen van inmenging zijn. Hoewel de bewaring van gegevens zinvol is met het oog op de eventuele latere toegang tot die gegevens door de bevoegde instanties, moet elk van deze inmengingen afzonderlijk worden gerechtvaardigd, middels een specifiek onderzoek in het licht van het nagestreefde doel.

76. Een nationaal stelsel dat voorziet in de algemene en ongedifferentieerde opslag van gegevens kan dan ook niet worden gerechtvaardigd op grond van het feit dat in de regeling ter zake tegelijkertijd strikte materiële en procedurele voorwaarden voor de toegang tot die gegevens zijn vastgesteld.

77. Er moeten dus regels zijn die specifiek verband houden met de bewaring van gegevens, uit hoofde waarvan die bewaring aan bepaalde voorwaarden wordt onderworpen om het algemene en ongedifferentieerde karakter ervan te voorkomen. Alleen zo kan worden gewaarborgd dat de bewaring verenigbaar is met 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.

78. Dat is overigens ook de aanpak die de werkgroepen in de Raad hebben gekozen bij de vaststelling van regels voor de bewaring en toegang die strookten met de rechtspraak van het Hof, waarbij de twee vormen van inmenging naast elkaar werden onderzocht.(68)

79. Door beperkingen te stellen aan elk van beide vormen van inmenging, zal kunnen worden beoordeeld of het eventuele cumulatieve effect ervan, in combinatie met gedegen waarborgen, van die aard is dat het de effecten van de bewaring van gegevens op de door de artikelen 7, 8 en 11 van het Handvest beschermde grondrechten beperkt en tegelijkertijd de doeltreffendheid van de onderzoeken waarborgt.

80. Om die rechten te beschermen, moet het stelsel:

– voorzien in een bewaring van gegevens die bepaalde beperkingen en verschillen omvat naargelang van het nagestreefde doel;

– de toegang tot die gegevens slechts regelen voor zover dat strikt noodzakelijk is voor het beoogde doel en onder toezicht van een rechter of een onafhankelijke bestuurlijke autoriteit.

81. De rechtvaardiging van het feit dat aanbieders van elektronischecommunicatiediensten bepaalde gegevens bewaren – en niet alleen in het kader van het beheer van hun contractuele verplichtingen met de gebruikers – neemt toe parallel aan de technologische vooruitgang. Als wordt aangenomen dat die bewaring nuttig is om criminaliteit te voorkomen en te bestrijden (wat moeilijk te weerleggen is(69)), zou het niet logisch zijn de omvang ervan te beperken tot de loutere exploitatie van de gegevens die de operatoren bewaren voor de verrichting van hun commerciële activiteiten en tot de tijd die daarvoor nodig is.

82. Wanneer wordt erkend dat het dienstig is te voorzien in een verplichting tot bewaring van gegevens om de nationale veiligheid te waarborgen en criminaliteit te bestrijden, die verder gaat dan de bewaring die door de operatoren mag worden toegepast met het oog op hun technische en commerciële behoeften, is het absoluut noodzakelijk om de contouren van die verplichting af te bakenen.

83. Elke bewaringsregeling moet strikt zijn afgestemd op het nagestreefde doel, zodat zij niet kan verworden tot een ongedifferentieerde bewaring.(70) Voorts moet worden uitgesloten dat de som van deze gegevens een *beeld* geeft van de betrokken persoon (d.w.z. van zijn gebruikelijke activiteiten en zijn sociale relaties) dat het beeld benadert of evenaart dat zou worden verkregen als de inhoud van de communicatie bekend zou zijn.

84. Om een aantal misverstanden weg te nemen en een zeker onbegrip te verhelpen, is het belangrijk rekening te houden met wat het Hof in zijn arresten Digital Rights en Tele2 Sverige en Watson *niet heeft verklaard*. In die arresten werd het bestaan als zodanig van een regeling voor de bewaring van gegevens als nuttig instrument in de strijd tegen criminaliteit niet veroordeeld. Integendeel, de legitimiteit van de doelstelling strafbare feiten te voorkomen en te bestraffen werd erin erkend alsook het nut van een stelsel voor de bewaring van gegevens om die doelstelling te bereiken.

85. Wat, zoals ik al zei, wél duidelijk werd verworpen, is dat de Unie of haar lidstaten met een beroep op die doelstelling de ongedifferentieerde bewaring van *alle* in het kader van de verrichting van elektronischecommunicatiediensten gegenereerde gegevens en de algemene toegang tot die gegevens kunnen opleggen.

86. Er moeten derhalve manieren voor gegevensbewaring worden gevonden die niet beantwoorden aan die kwalificaties („algemeen en ongedifferentieerd"), die onverenigbaar zijn met de uit hoofde van de artikelen 7, 8 en 11 van het Handvest geëiste bescherming.

87. Eén van die manieren is een *gerichte* bewaring van gegevens, met betrekking tot ofwel een specifiek publiek (in theorie het publiek dat bepaalde meer of minder directe verbanden vertoont met de meest ernstige bedreigingen), ofwel een bepaald geografisch gebied.

88. Die benadering levert echter enkele problemen op:

– de identificatie van een groep potentiële daders zou waarschijnlijk ontoereikend zijn als die daders anonimiseringstechnieken gebruiken of hun identiteit vervalsen. Bovendien zou de selectie van die groepen ertoe kunnen leiden dat een algemene verdenking komt te rusten op bepaalde segmenten van de bevolking en zou die selectie als discriminerend kunnen worden beschouwd, naargelang van het gebruikte algoritme;

– de selectie op basis van geografische criteria (die, om doeltreffend te zijn, niet al te sterk beperkte gebieden zou moeten betreffen) levert dezelfde problemen op en creëert er nog andere, zoals de Europese Toezichthouder voor gegevensbescherming ter terechtzitting aangaf, aangezien bepaalde gebieden gestigmatiseerd zouden kunnen worden.

89. Bovendien zou er een zekere tegenspraak kunnen bestaan tussen het preventieve karakter van een bewaring die gericht is op een specifiek publiek of een bepaald geografisch gebied en het feit dat noch de daders van de strafbare feiten, noch de plek en het tijdstip waarop die feiten worden begaan vooraf bekend zijn.

90. Hoe dan ook mag niet worden uitgesloten dat er op deze criteria gebaseerde formules voor gerichte bewaring bestaan die nuttig zijn om voornoemde doelstellingen te bereiken. Het staat aan de wetgevende macht, in elke lidstaat of voor de gehele Unie, om die formules te ontwerpen, met eerbied voor de door het Hof gewaarborgde bescherming van de grondrechten.

91. Het zou fout zijn te denken dat de gerichte bewaring van gegevens met betrekking tot een specifiek publiek of een bepaald geografisch gebied de enige formule is die het Hof verenigbaar acht met artikel 15, lid 1, van richtlijn 2002/58, gelezen tegen de achtergrond van de artikelen 7 en 8 van het Handvest.

92. Zoals gezegd kunnen er ook andere manieren worden gevonden om gegevens gericht te bewaren, naast bewaring gericht op specifieke groepen van personen of geografische gebieden. Zo hebben ook de eerder genoemde werkgroepen in de Raad het begrepen: als te onderzoeken mogelijkheden hebben zij met name gekeken naar de beperking van de categorieën van bewaarde gegevens(71); de pseudonimisering van gegevens(72); de invoering van beperkte

bewaringstermijnen(73); de uitsluiting van bepaalde categorieën van aanbieders van elektronischecommunicatiediensten(74); vernieuwbare vergunningen voor de opslag(75); de verplichting om de opgeslagen gegevens binnen de Unie te bewaren of het stelselmatige en regelmatige toezicht door een onafhankelijk bestuursorgaan op de door de aanbieders van elektronischecommunicatiediensten geboden waarborgen ter voorkoming van misbruik van de gegevens.

93. Om verenigbaar te zijn met de rechtspraak van het Hof zou mijns inziens de voorkeur moeten worden gegeven aan een tijdelijke bewaring van bepaalde *categorieën* van verkeers- en locatiegegevens, die beperkt moeten worden tot wat strikt noodzakelijk is voor de veiligheid en die het, samen bezien, niet mogelijk mogen maken dat een nauwkeurig en gedetailleerd beeld wordt verkregen van het leven van de betrokken personen.

94. In de praktijk komt dit erop neer dat voor de twee belangrijkste gegevenscategorieën (verkeersgegevens en locatiegegevens), door toepassing van passende filters, alleen de *minimumgegevens* mogen worden bewaard die worden geacht absoluut noodzakelijk te zijn voor de preventie van en de doeltreffende controle op de criminaliteit en het waarborgen van de nationale veiligheid.

95. Het staat aan de lidstaten of aan de instellingen van de Unie om, via de wetgeving (met de hulp van hun eigen deskundigen), die selectie te maken, waarbij zij moeten afzien van enige poging om een algemene en ongedifferentieerde opslag van alle verkeers- en locatiegegevens op te leggen.

96. Naast deze beperking per categorie mogen de gegevens slechts voor een bepaalde termijn worden bewaard, zodat zij geen gedetailleerd beeld van het leven van de betrokken personen kunnen geven. Die bewaringstermijn moet bovendien worden aangepast naargelang van de aard van de gegevens, om ervoor te zorgen dat gegevens die nadere informatie verschaffen over de levensstijl en de gewoonten van die personen minder lang worden opgeslagen.(76)

97. De differentiëring van de bewaartermijn naar categorieën van gegevens, op basis van het nut ervan voor het nagestreefde veiligheidsdoel, is met andere woorden een mogelijkheid die verder moet worden onderzocht. Door de termijn te beperken waarin bepaalde gegevenscategorieën gelijktijdig mogen worden bewaard (en dus kunnen worden gebruikt om correlaties te vinden waaruit de levensstijl van de betrokken personen blijkt), wordt de bescherming uitgebreid van het recht dat is vastgelegd in artikel 8 van het Handvest.

98. In die zin heeft de Europese Toezichthouder voor gegevensbescherming zich ter terechtzitting uitgelaten: hoe meer categorieën van metagegevens worden opgeslagen en hoe langer de bewaringstermijn, des te gemakkelijker wordt het om een gedetailleerd profiel van een persoon te bepalen, en omgekeerd.(77)

99. Voorts is het, zoals tijdens de terechtzitting ook is vermeld, moeilijk om een grens te trekken tussen bepaalde metagegevens over de elektronische communicatie en de inhoud van die communicatie. Sommige metagegevens kunnen net zoveel onthullen als de inhoud van die communicatie, of zelfs meer: dat kan bijvoorbeeld het geval zijn bij adressen (URL's) van bezochte webpagina's.(78) Met betrekking tot dit soort gegevens en andere soortgelijke gegevens moet er dus bijzonder nauw op worden toegezien dat de noodzaak van de bewaring en de duur ervan zoveel mogelijk worden beperkt.

100. Het is niet gemakkelijk om een evenwichtige oplossing te vinden, aangezien de onderzoeks- en beveiligingsdiensten door de opgeslagen gegevens te kruisen en met elkaar in verband te brengen in staat zijn een verdachte of een bedreiging aan te wijzen, al naargelang van het geval. Toch bestaat er een onderscheid tussen de bewaring van gegevens om die verdachte of die dreiging op te sporen en de bewaring die ertoe leidt dat een gedetailleerd beeld van het leven van een persoon kan worden gevormd.

101. In afwachting van een gemeenschappelijke regeling voor de hele Unie op dit specifieke gebied, denk ik niet dat van het Hof kan worden verlangd dat het een regelgevende functie op zich neemt en in detail specificeert welke categorieën van gegevens mogen worden bewaard en hoelang. Het staat aan

de instellingen van de Unie en aan de lidstaten om, zodra de grenzen vaststaan die volgens het Hof voortvloeien uit het Handvest, het juiste evenwicht te vinden tussen de handhaving van de veiligheid en de door het Handvest beschermde grondrechten.

102. Niet beschikken over de informatie die kan worden afgeleid uit een groter aantal opgeslagen gegevens zou het in sommige vallen moeilijker kunnen maken om potentiële bedreigingen te bestrijden. Dat is echter de prijs die de overheid, zoals wel vaker, moet betalen wanneer zij zichzelf de verplichting oplegt de grondrechten te waarborgen.

103. Net zoals niemand een ex ante-verplichting tot algemene en ongedifferentieerde bewaring van de *inhoud* van de private elektronische communicatie zou steunen (zelfs niet wanneer bij wet zou worden gegarandeerd dat later slechts een beperkte toegang tot die inhoud wordt gegeven), mogen ook de metagegevens over die communicatie, die even gevoelige informatie kunnen bevatten als de eigenlijke inhoud ervan, niet op algemene en ongedifferentieerde wijze worden opgeslagen.

104. Dat het moeilijk is om in de wetgeving nauwkeurig vast te stellen in welke gevallen en onder welke voorwaarden voor gerichte bewaring moet worden gekozen – hetgeen ik erken –, rechtvaardigt niet dat de lidstaten van de uitzondering de regel maken en van de algemene bewaring van persoonsgegevens het centrale beginsel in hun wetgeving maken. Indien dat wel zo zou zijn, zou immers worden aanvaard dat het recht op bescherming van de persoonsgegevens voor onbepaalde duur met voeten wordt getreden.

105. Ik moet hieraan toevoegen dat niets belet dat in echt *uitzonderlijke* omstandigheden, waarin sprake is van een onmiddellijke dreiging die of een buitengewoon risico dat rechtvaardigt dat de noodtoestand wordt uitgeroepen in een lidstaat, in de nationale wetgeving wordt voorzien in de mogelijkheid om voor bepaalde tijd een verplichting tot gegevensbewaring op te leggen die zo ruim en algemeen is als noodzakelijk wordt geacht.

106. In dat geval zou een regeling kunnen worden ingevoerd die de ruimere bewaring van gegevens (en de toegang daartoe) expliciet toestaat, overeenkomstig voorwaarden en procedures die moeten verzekeren dat de maatregelen een uitzonderlijk karakter hebben wat hun materiële omvang en de duur ervan betreft, en dat de overeenkomstige juridische waarborgen worden geboden.

107. Uit het vergelijkend onderzoek van de regelgevingsstelsels waarbij de situaties zijn geregeld die als een noodsituatie worden beschouwd, blijkt dat het niet onmogelijk is om te bepalen in welke feitelijke omstandigheden een specifiek regelgevingsstelsel kan worden toegepast, waarbij moet worden vastgesteld welke instantie de beslissing daartoe kan nemen, onder welke omstandigheden en onder wiens toezicht.(79)

E. Specifieke antwoorden op de drie prejudiciële vragen

1. Opmerking vooraf

108. De verwijzende rechter verzoekt om uitlegging van artikel 15, lid 1, van richtlijn 2002/58 met betrekking tot verschillende door het Handvest gewaarborgde rechten: het recht op eerbiediging van het privéleven en van het familie- en gezinsleven (artikel 7), het recht op bescherming van persoonsgegevens (artikel 8) en het recht op vrijheid van meningsuiting en van informatie (artikel 11).

109. Zoals ik in mijn conclusie in de gevoegde zaken C-511/18 en C-512/18 uiteenzet, zijn dit immers de rechten die volgens het Hof in dergelijke gevallen zouden kunnen worden aangetast.

110. Het Grondwettelijk Hof vermeldt echter eveneens de artikelen 4 en 6 van het Handvest, waarop respectievelijk de tweede en de eerste prejudiciële vraag betrekking hebben.

111. Over de relevantie van artikel 6 van het Handvest, waarbij het recht op vrijheid en veiligheid wordt gewaarborgd en dat eveneens wordt ingeroepen in de zaken C-511/18 en C-512/18, heb ik me reeds uitgesproken in de conclusie in die zaken, waarnaar ik hier verwijs.(80)

112. Wat artikel 4 van het Handvest betreft, lijkt het mij dienstig om de desbetreffende vraag eerst te beantwoorden, aangezien het antwoord niet zozeer afhankelijk is van de beoordeling van de nationale wetgeving, met het oog op de toetsing aan het Unierecht, als wel van de uitlegging van deze bepaling.

2. Tweede prejudiciële vraag

113. Naar het verbod van folteringen en van onmenselijke of vernederende behandelingen of bestraffingen, dat gewaarborgd wordt bij artikel 4 van het Handvest, wordt alleen in deze prejudiciële verwijzing verwezen, hetgeen mij ertoe verplicht er aandacht aan te besteden.

114. Door een beroep te doen op artikel 4 van het Handvest wil de verwijzende rechter duidelijk maken dat de nationale regeling eveneens tot doel heeft te voldoen aan de *positieve verplichting* die op de overheid rust 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".(81)

115. Mijns inziens verschilt deze concrete *positieve verplichting* niet zo sterk van elk van de specifieke taken die de afkondiging van een lijst van grondrechten met zich brengt voor de staat. De rechten op leven (artikel 2 van het Handvest), op lichamelijke integriteit (artikel 3 van het Handvest) of op bescherming van persoonsgegevens (artikel 8 van het Handvest), behelzen net zoals de vrijheid van meningsuiting (artikel 11 van het Handvest) of van gedachte, geweten en godsdienst (artikel 10 van het Handvest) een verplichting voor de staat om een regelgevingskader op te zetten waarin het effectieve genot van die rechten en vrijheden wordt gewaarborgd, in voorkomend geval middels de uitoefening van de door de staat gemonopoliseerde macht jegens eenieder die tracht dat genot te beletten of te bemoeilijken.(82)

116. Wat seksueel misbruik van minderjarigen betreft, is het Europees Hof voor de Rechten van de Mens (EHRM) van oordeel dat kinderen en andere kwetsbare personen een versterkt recht hebben op bescherming door de staat, middels de vaststelling van strafrechtelijke regels om dergelijke strafbare feiten doeltreffend te bestraffen en te ontmoedigen.(83)

117. Dit versterkt recht op bescherming is niet alleen in artikel 4 van het Handvest neergelegd – uiteraard zou ook artikel 1 (menselijke waardigheid) of artikel 3 (recht op lichamelijke en geestelijke integriteit) daartoe kunnen worden ingeroepen.

118. Hoewel de positieve verplichting van de overheid om de bescherming van kinderen en andere kwetsbare personen te waarborgen niet buiten beschouwing mag worden gelaten in de weging van de belangen die door de nationale regeling worden geschaad(84), mag deze verplichting evenmin leiden tot een „buitensporige last" voor de overheid(85) en mag zij niet worden vervuld buiten de legaliteit of zonder eerbiediging van de overige grondrechten.(86)

3. Eerste prejudiciële vraag

119. De verwijzende rechter wenst in essentie te vernemen of het Unierecht zich verzet tegen de nationale wet waarover hij zich moet uitspreken in het kader van een beroep tot vernietiging ervan wegens ongrondwettigheid.

120. Aangezien het Hof richtlijn 2002/58 reeds in overeenstemming met de overeenkomstige bepalingen van het Handvest heeft uitgelegd, moet in het antwoord op de prejudiciële vraag rekening worden gehouden met de rechtspraak die is vervat in het arrest Tele2 Sverige en Watson, in voorkomend geval met de nuances die nu worden aangebracht.

121. In deze optiek moeten de uitleggingscriteria die aan het Grondwettelijk Hof kunnen worden aangereikt om het in staat te stellen zelf te toetsen of de nationale regeling strookt met het Unierecht, de bewaring van en de toegang tot gegevens, zoals vastgelegd in die nationale regeling, afzonderlijk beschouwen.

a) Voorwaarden voor het bewaren van de gegevens

122. De Belgische regering onderstreept dat zij een duidelijk rechtskader wenste op te zetten dat de waarborgen zou omvatten die nodig zijn om de persoonlijke levenssfeer te beschermen, in plaats van zich te baseren op de praktijk van de operatoren van elektronischecommunicatiediensten met betrekking tot de bewaring van de gegevens voor facturering of voor de behandeling van verzoeken om inlichtingen van klanten.

123. Volgens deze regering heeft de algemene en preventieve verplichting om de gegevens te bewaren niet alleen ten doel feiten van zware criminaliteit te onderzoeken, op te sporen en te vervolgen, maar ook de nationale veiligheid te waarborgen, het grondgebied en de openbare veiligheid te verdedigen, andere feiten dan zware criminaliteit te onderzoeken, op te sporen en te vervolgen, en het verboden gebruik van de elektronische communicatiesystemen te voorkomen(87), of een andere in artikel 23, lid 1, van verordening 2016/679 genoemde doelstelling te verwezenlijken.

124. Volgens de Belgische regering:

– kunnen uit de bewaring van gegevens als dusdanig geen zeer precieze conclusies worden getrokken over het privéleven van de betrokken personen. Dergelijke conclusies kunnen alleen worden getrokken wanneer ook toegang tot de bewaarde gegevens wordt gegeven;

– bevat de wet waarborgen om de privacy te beschermen. Zo betreft de bewaring van gegevens niet de inhoud van de communicatie, zijn de waarborgen met betrekking tot de rechtvaardiging van de bewaring, het recht van toegang, het recht van rectificatie en andere rechten volledig van toepassing, en moeten de aanbieders en operatoren de bewaarde gegevens aan dezelfde verplichtingen en beveiligings- en beschermingsmaatregelen onderwerpen als de gegevens in het netwerk, waarbij zij onbedoelde of onwettige vernietiging en onbedoeld verlies of wijziging dienen te voorkomen;

– kunnen de gegevens gedurende twaalf maanden worden opgeslagen (waarna zij moeten worden vernietigd), en wel uitsluitend op het grondgebied van de Unie;

– moeten de aanbieders en operatoren maatregelen van technologische beveiliging treffen die de bewaarde gegevens vanaf de registratie ervan onleesbaar en onbruikbaar maken voor elke persoon die niet gemachtigd is om er toegang toe te hebben;

– staan die activiteiten hoe dan ook onder toezicht van de Belgische post- en telecomregulator en de gegevensbeschermingsautoriteit.

125. Ondanks die garanties legt de Belgische wettelijke regeling de operatoren en aanbieders van elektronischecommunicatiediensten wel degelijk een algemene verplichting op om de verkeers- en locatiegegevens in de zin van richtlijn 2002/58, die bij het verlenen van die diensten worden verwerkt, zonder onderscheid te bewaren. Zoals gezegd bedraagt de bewaringstermijn gewoonlijk twaalf maanden: er is niet voorzien in enige beperking in de tijd naargelang van de categorieën van bewaarde gegevens.

126. Deze algemene en ongedifferentieerde verplichting geldt voortdurend en zonder onderbreking. Hoewel een dergelijke verplichting bedoeld is om alle vormen van strafbare feiten te voorkomen, te onderzoeken en te vervolgen (van feiten in verband met de nationale veiligheid of de landsverdediging dan wel bijzonder zware feiten tot feiten waarop gevangenisstraffen van minder dan een jaar staan), strookt zij niet met de rechtspraak van het Hof, en kan zij dus niet worden geacht verenigbaar te zijn met het Handvest.

127. Om de verplichting met die rechtspraak in overeenstemming te brengen, zal de Belgische wetgever andere mogelijkheden moeten verkennen (zoals die welke ik eerder al heb genoemd), waarmee formules voor een beperkte bewaring worden ingevoerd. Die formules, die kunnen variëren volgens de categorieën van gegevens, moeten voldoen aan het beginsel dat alleen het noodzakelijke *minimum* aan gegevens wordt bewaard, naargelang van het risico of de bedreiging, en gedurende een beperkte termijn, die zal afhangen van de aard van de opgeslagen informatie. Hoe dan ook mag de bewaring het privéleven, de gewoonten, het gedrag of de sociale relaties van de betrokkenen niet nauwkeurig *in kaart brengen*.

b) Voorwaarden voor de toegang van de overheidsinstanties tot de bewaarde gegevens

128. Mijns inziens blijven de in het arrest Tele2 Sverige en Watson(88) vermelde voorwaarden ook voor de toegang relevant: de nationale regeling moet de materiële en procedurele voorwaarden bepalen waaronder de bevoegde autoriteiten toegang hebben tot de bewaarde gegevens.(89)

129. De Belgische regering specificeert dat in artikel 126, § 2, van de wet van 2005 (betreffende de elektronische communicatie)(90) restrictief is bepaald welke overheden de gegevens mogen ontvangen die krachtens § 1 van dat artikel worden bewaard.

130. Het betreft de eigenlijke gerechtelijke autoriteiten en het openbaar ministerie; de Staatsveiligheid; de Algemene Dienst Inlichting en Veiligheid, onder toezicht van onafhankelijke commissies; de officieren van gerechtelijke politie van het Belgisch Instituut voor postdiensten en telecommunicatie; de hulpdiensten; de officieren van gerechtelijke politie van de Cel Vermiste Personen van de federale politie; de Ombudsdienst voor telecommunicatie en het toezichtsorgaan voor de financiële sector.

131. In algemene zin verklaart de Belgische regering dat de nationale wettelijke regeling niet toestaat dat de verschillende diensten toegang hebben tot de gegevens om bedreigingen die niet zijn vastgesteld of waarvoor geen concrete aanwijzingen bestaan actief te vervolgen. De nationale autoriteiten zouden dus niet zonder meer toegang kunnen krijgen tot de ruwe communicatiegegevens en die gegevens niet automatisch kunnen verwerken om informatie te verkrijgen en risico's voor de veiligheid actief te voorkomen.

132. Volgens diezelfde regering gelden voor de toegang tot de gegevens strikte voorwaarden, naargelang van de status van elk van de bevoegde nationale autoriteiten.

133. Het antwoord op de eerste prejudiciële vraag behoeft volgens mij geen uitvoerige analyse door het Hof van de voorwaarden waaronder elk van deze autoriteiten toegang kan krijgen tot de bewaarde gegevens. Dat staat eerder aan de verwijzende rechter, die deze taak moet uitvoeren in het licht van de richtsnoeren die het arrest Tele2 Sverige en Watson en het arrest Ministerio Fiscal aanreiken.

134. Voorts bestaan er volgens de door de Belgische regering verstrekte inlichtingen aanzienlijke verschillen tussen de toegangsvoorwaarden voor de gerechtelijke autoriteiten of het openbaar ministerie(91) met het oog op het onderzoek, de opsporing of de vervolging van strafbare feiten, overeenkomstig de artikelen 46bis(92) en 88bis(93) van het Belgische Wetboek van strafvordering, enerzijds, en de voorwaarden die gelden voor andere autoriteiten, anderzijds.

135. Wat de inlichtingen- en veiligheidsdiensten betreft, moet het verzoek om toegang tot de verkeers- en locatiegegevens in het bezit van de operatoren overeenkomstig de wet van 1998 gebaseerd zijn op objectieve criteria om te waarborgen dat de toegang wordt beperkt tot het strikt noodzakelijke, op basis van een vooraf bepaalde dreiging.(94) Er is voorzien in verschillende termijnen voor de toegang (zes, negen of twaalf maanden) naargelang van de potentiële dreiging, en de vordering moet voldoen aan de principes van proportionaliteit en subsidiariteit. Voorts is een mechanisme voor toezicht door een onafhankelijke autoriteit opgezet.(95)

136. Officieren van gerechtelijke politie van de regulator van de Belgische post- en telecommunicatiesector (BIPT) krijgen slechts in bijzonder beperkte concrete gevallen toegang tot de door de telecomoperatoren bewaarde gegevens, onder toezicht van het openbaar ministerie(96), zonder dat hun activiteiten volgens de Belgische regering de personen bereiken van wie de gegevens worden bewaard.

137. De hulpdiensten die hulp ter plaatse bieden, kunnen, wanneer zij naar aanleiding van een noodoproep, van de aanbieder of operator niet de identificatiegegevens van de oproeper ontvangen of onvolledige of onjuiste gegevens krijgen, om de gegevens van de oproeper verzoeken.

138. De officieren van gerechtelijke politie van de Cel Vermiste Personen van de federale politie kunnen bij de operator de gegevens vorderen die nodig zijn om een vermiste te vinden van wie de fysieke integriteit in onmiddellijk gevaar is. De toegang, waarvoor strikte voorwaarden gelden, is beperkt tot de gegevens ter identificatie van de gebruiker, 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. Het gaat hierbij enkel om gegevens die zijn bewaard in de 48 uur voorafgaand aan het verzoek.

139. De Ombudsdienst voor telecommunicatie kan enkel de identificatiegegevens opvragen van de persoon die kwaadwillig gebruik heeft gemaakt van een elektronischecommunicatienetwerk of -dienst. In dit geval is er geen sprake van voorafgaand toezicht door een rechterlijke instantie of een onafhankelijke bestuurlijke autoriteit (buiten de Ombudsdienst zelf).

140. Met het oog op de bestrijding van financiële criminaliteit, tot slot, kan het toezichtsorgaan voor de financiële sector toegang tot de verkeers- en locatiegegevens krijgen na machtiging door de onderzoeksrechter.

141. Uit de uiteenzetting van deze wijzen van en voorwaarden voor toegang tot de bewaarde gegevens voor elk van de autoriteiten die gemachtigd zijn om die gegevens te verkrijgen, blijkt dat er uiteenlopende situaties en waarborgen bestaan waarvan de verwijzende rechter nauwkeurig moet onderzoeken of zij stroken met de criteria die het Hof hanteert in zijn rechtspraak.(97)

142. Ik stel bijvoorbeeld vast dat uit de bestreden wettelijke regeling niet blijkt dat de bevoegde nationale autoriteiten de betrokken personen er stelselmatig van op de hoogte moeten brengen dat hun gegevens zijn geraadpleegd (behalve wanneer dat een lopend onderzoek in gevaar brengt). Verder lijken er – op zijn minst in enkele gevallen, bijvoorbeeld met betrekking tot financiële inbreuken, – geen vooraf bepaalde regels over de ernst van die inbreuken te bestaan om de toegang tot de betrokken gegevens te rechtvaardigen. Het verband tussen de intensiteit van de inmenging en de ernst van het onderzochte feit, in de zin van het arrest Ministerio Fiscal, is niet in alle gevallen duidelijk.

143. Hoe dan ook, ik ben van oordeel dat de overwegingen met betrekking tot de toegang van de autoriteiten tot de gegevens naar de achtergrond verdwijnen wanneer, gelet op het voorgaande, de algemene en ongedifferentieerde bewaring van die gegevens zelf de belangrijkste reden is waarom de in deze verwijzing aan de orde zijnde nationale wettelijke regeling niet strookt met het Unierecht.

4. Derde prejudiciële vraag

144. Het Grondwettelijk Hof wenst te vernemen of de gevolgen van de nationale wettelijke regeling tijdelijk kunnen worden gehandhaafd voor het geval dat in het licht van het antwoord van het Hof zou komen vast te staan dat die regeling onverenigbaar is met het Unierecht. Zo zou rechtsonzekerheid worden voorkomen en zouden de voorheen verzamelde en bewaarde gegevens alsnog voor de beoogde doeleinden kunnen worden gebruikt.

145. Het is vaste rechtspraak dat „enkel het Hof, bij wijze van uitzondering en om dwingende redenen van rechtszekerheid, een voorlopige opschorting kan toestaan van het effect dat een [...] regel van het recht van de Unie op het daarmee strijdige nationale recht heeft, namelijk de terzijdestelling daarvan". Indien „de nationale rechterlijke instanties bevoegd zouden zijn voorrang te geven aan de nationale bepalingen boven het [...] Unierecht [waarmee zij in strijd zijn], al ware het slechts tijdelijk, zou immers afbreuk worden gedaan aan de uniforme toepassing van het Unierecht".(98)

146. De Commissie is van mening dat deze vraag van de verwijzende rechter ontkennend moet worden beantwoord, aangezien het Hof de gevolgen van de uitlegging van artikel 15, lid 1, van richtlijn 2002/58 niet in de tijd heeft beperkt.(99)

147. Niettemin heeft het Hof in het arrest van 28 februari 2012, Inter-Environnement Wallonie en Terre wallonne(100), verklaard dat het een nationale rechterlijke instantie, gelet op het bestaan van een dwingende overweging van bescherming van het milieu, bij uitzondering kon worden toegestaan een nationaal voorschrift toe te passen op grond waarvan zij bepaalde gevolgen kon handhaven van een nationale handeling die wegens schending van een regel van de Unie was vernietigd.(101)

148. Die lijn in de rechtspraak is bevestigd door het arrest van 29 juli 2019, Inter-Environnement Wallonie en Bond Beter Leefmilieu Vlaanderen.(102) Of die rechtspraak nu tot stand is gekomen op het gebied van milieubescherming dan wel is gebaseerd op de continuïteit van de

elektriciteitsvoorziening, ik zie geen redenen om de toepassing ervan uit te sluiten op andere gebieden van het Unierecht, in het bijzonder het gebied dat hier aan de orde is.

149. Indien een „dwingende overweging van bescherming van het milieu" kan rechtvaardigen dat de nationale rechters bij uitzondering bepaalde gevolgen handhaven van een nationale handeling die onverenigbaar is met het Unierecht, is dat omdat milieubescherming „een van de wezenlijke doelstellingen van de Unie is en een zowel sectoroverschrijdend als fundamenteel karakter heeft".(103)

150. Tot die doelstellingen van de Unie behoort ook de totstandbrenging van een ruimte van veiligheid (artikel 3 VEU), met eerbiediging van de essentiële staatsfuncties, en in het bijzonder de functies die de handhaving van de openbare orde en de bescherming van de nationale veiligheid ten doel hebben (artikel 4 VEU, lid 2). Dat is een doelstelling die niet minder „sectoroverschrijdend en fundamenteel" is dan milieubescherming, aangezien de verwezenlijking ervan een noodzakelijke voorwaarde is voor de totstandbrenging van een regelgevingskader dat het effectieve genot van de grondrechten en fundamentele vrijheden kan garanderen.

151. Mijns inziens zouden dwingende redenen in verband met de bescherming van de nationale veiligheid in deze zaak kunnen rechtvaardigen dat het Hof de verwijzende rechter bij uitzondering toestaat om op zijn minst bepaalde gevolgen van de bestreden wet te handhaven.

152. Voor die handhaving zou de verwijzende rechter, in het licht van de uitspraak van het Hof, moeten oordelen dat de nationale regeling onverenigbaar is met het Unierecht en dat het al te ontwrichtende gevolgen zou hebben voor de openbare veiligheid of de staatsveiligheid dat de regeling onmiddellijk zou worden vernietigd (indien die onverenigbaarheid in het nationale recht tot vernietiging leidt) of buiten toepassing zou worden gelaten.

153. Om de gevolgen van de nationale regeling (geheel of gedeeltelijk) tijdelijk te handhaven, zou het bovendien noodzakelijk zijn dat de verlenging:

– bedoeld is om een juridische leemte te voorkomen die even schadelijke gevolgen als de toepassing van de bestreden regeling zou hebben, die niet anderszins zou kunnen worden opgevuld en waardoor de lidstaten een waardevol instrument voor de waarborging van de staatsveiligheid zou worden ontnomen, en

– slechts zolang geldt als absoluut noodzakelijk is om de maatregelen te treffen waarmee de vastgestelde onverenigbaarheid met het Unierecht kan worden verholpen.(104)

154. Deze oplossing vindt bovendien steun in het feit dat de nationale regelingen moeilijk zijn af te stemmen op de rechtspraak in de zaak Tele2 Sverige en Watson(105) en dat de Belgische wetgever zijn bereidheid om zich te schikken naar het arrest Digital Rights heeft getoond door zijn wettelijke regeling te wijzigen. Dit doet vermoeden dat hij de wet van 29 mei 2016 (die is uitgevaardigd vóór het arrest Tele2 Sverige en Watson werd gewezen) eveneens zal aanpassen aan dit laatste arrest.

V. Conclusie

155. Gelet op het voorgaande geef ik het Hof in overweging om het Grondwettelijk Hof (België) als volgt te antwoorden:

„1) Artikel 15, lid 1, van richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), gelezen in samenhang met de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, moet aldus worden uitgelegd dat:

– het zich verzet tegen een nationale regeling die de operatoren en aanbieders van elektronischecommunicatiediensten de verplichting oplegt om de verkeers- en

locatiegegevens van alle abonnees en gebruikers betreffende alle elektronischecommunicatiemiddelen op algemene en ongedifferentieerde wijze te bewaren;

– aan het voorgaande niet wordt afgedaan door het feit dat die nationale regeling niet alleen ten doel heeft feiten van al dan niet zware criminaliteit te onderzoeken, op te sporen en te vervolgen, maar ook de nationale veiligheid te waarborgen, het grondgebied en de openbare veiligheid te verdedigen, het verboden gebruik van de elektronische communicatiesystemen te voorkomen, of een andere doelstelling te verwezenlijken als vermeld in artikel 23, lid 1, van 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);

– aan het voorgaande evenmin wordt afgedaan door het feit dat de toegang tot de bewaarde gegevens onderworpen is aan nauwkeurig geregelde waarborgen. Het staat aan de verwijzende rechter na te gaan of de nationale regeling waarin de voorwaarden voor die toegang door de bevoegde autoriteiten zijn vastgesteld, de toegang beperkt tot specifieke gevallen waarvan de ernst inmenging noodzakelijk maakt; de toegang afhankelijk stelt van voorafgaand toezicht (behalve in gevallen van spoedeisendheid) door een rechterlijke instantie of een onafhankelijke bestuurlijke autoriteit, en voorschrijft dat de betrokken personen van die toegang op de hoogte worden gesteld, voor zover dat het optreden van die autoriteiten niet in gevaar brengt.

2) De artikelen 4 en 6 van het Handvest van de grondrechten van de Europese Unie beïnvloeden de uitlegging van artikel 15, lid 1, van richtlijn 2002/58, gelezen in samenhang met de overige reeds genoemde artikelen van het Handvest, niet in die zin dat zij het onmogelijk maken om vast te stellen dat een nationale regeling zoals die in het hoofdgeding onverenigbaar is met het Unierecht.

3) Een nationale rechterlijke instantie kan, indien het nationale recht dit toestaat, de gevolgen van een regeling zoals die in het hoofdgeding bij wijze van uitzondering tijdelijk handhaven – ook wanneer die regeling onverenigbaar is met het Unierecht – voor zover die handhaving gerechtvaardigd wordt door dwingende redenen in verband met bedreigingen van de openbare veiligheid of de nationale veiligheid waaraan niet het hoofd zou kunnen worden geboden met andere middelen en alternatieven. De gevolgen kunnen niet langer worden gehandhaafd dan strikt noodzakelijk is om een einde te maken aan de onverenigbaarheid met het Unierecht."

---

1 Oorspronkelijke taal: Spaans.

---

2 Gevoegde zaken C-293/12 en C-594/12, EU:C:2014:238; hierna: „arrest Digital Rights".

---

3 Richtlijn 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 elektronischecommunicatiediensten of van openbare communicatienetwerken en tot wijziging van richtlijn 2002/58/EG (PB 2006, L 105, blz. 54).

---

4 Gevoegde zaken C-203/15 en C-698/15, EU:C:2016:970; hierna: „arrest Tele2 Sverige en Watson".

---

5 Richtlijn 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).

---

6 Zaak C-207/16, EU:C:2018:788; hierna: „arrest Ministerio Fiscal”.

7 Naast deze zaak (zaak C-520/18, Ordre des barreaux francophones et germanophone e.a.), betreft het de gevoegde zaken C-511/18 en C-512/18, La Quadrature du Net e.a., en zaak C-623/17, Privacy International.

8 Zaak Privacy International, C-623/17.

9 Zaak Ordre des barreaux francophones et germanophone e.a., C-520/18.

10 Gevoegde zaken La Quadrature du Net e.a., C-511/18 en C-512/18.

11 Hierna: „wet van 29 mei 2016” (*Belgisch Staatsblad* van 18 juli 2016, blz. 44717).

12 Hierna: „wet van 2005” (*Belgisch Staatsblad* van 20 juni 2005, blz. 28070).

13 Hierna: „wet van 1998” (*Belgisch Staatsblad* van 18 december 1998, blz. 40312).

14 Arrest nr. 84/2015, *Belgisch Staatsblad* van 11 augustus 2015.

15 Punten 40 e.v.

16 Richtlijn 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). Zie artikel 1, lid 2, van richtlijn 2002/58. Richtlijn 95/46 is met ingang van 25 mei 2018 ingetrokken bij verordening 2016/679. Voor zover richtlijn 2002/58 naar richtlijn 95/46 verwijst of niet zelf regels voorschrijft, moet dus absoluut rekening worden gehouden met de bepalingen van verordening 2016/679 (zie artikel 94, leden 1 en 2, ervan).

17 Arrest Tele2 Sverige en Watson, punten 82 en 83.

18 Ibidem, punt 85 en aldaar aangehaalde rechtspraak.

19 Ibidem, punt 87. Cursivering van mij.

20 Ibidem, punt 86 en aldaar aangehaalde rechtspraak.

21 Ibidem, punt 86, in fine.

22 Ibidem, punt 90.

23 Ibidem, punt 91 en aldaar aangehaalde rechtspraak.

24 Ibidem, punt 93 en aldaar aangehaalde rechtspraak.

25 Ibidem, punt 89.

26 Het gebruik van deze term in het arrest Tele2 Sverige en Watson, punt 95, gaat terug op overweging 11 van richtlijn 2002/58.

27 Arrest Digital Rights, punt 48: „Gelet op de belangrijke rol die de bescherming van persoonsgegevens speelt in het licht van het fundamentele recht op bescherming van het privéleven, alsook op de omvang en de ernst van de door richtlijn 2006/24 veroorzaakte inmenging in dit recht is de beoordelingsbevoegdheid van de Uniewetgever [...] beperkt, zodat een strikt toezicht moet worden uitgeoefend."

28 Arrest Tele2 Sverige en Watson, punt 96 en aldaar aangehaalde rechtspraak.

29 Arrest Digital Rights, punt 51. Zie in die zin ook het arrest Tele2 Sverige en Watson, punt 103.

30 Arresten Digital Rights, punt 65, en Tele2 Sverige en Watson, punt 100.

31 Arrest Tele2 Sverige en Watson, punt 97. Cursivering van mij.

32 Waaronder de naam en het adres van de abonnee of van de geregistreerde gebruiker, het telefoonnummer van de oproeper en het opgeroepen nummer en een IP-adres voor de internetdiensten.

33 Arrest Tele2 Sverige en Watson, punt 98.

34 Ibidem, punt 98.

35 Ibidem, punt 99.

36 Ibidem, punt 99, in fine.

37 Ibidem, punt 100.

38 Ibidem, punt 102.

39 Ibidem, punt 104.

40 Ibidem, punt 105.

41 Ibidem, punt 106.

42 Ibidem, punt 105.

43 Ibidem, punt 106.

44 Ibidem, punt 107.

45 Ibidem, punt 108. Cursivering van mij.

46 Ibidem, punt 109. Zij moet in het bijzonder aangeven „in welke omstandigheden en onder welke voorwaarden een maatregel van bewaring van gegevens preventief kan worden genomen, en aldus waarborgen dat een dergelijke maatregel tot het strikt noodzakelijke wordt beperkt".

47 Ibidem, punt 110.

48 Ibidem, punt 111.

49 Ibidem, punt 113.

50 Ibidem, punt 115.

51 Ibidem, punt 116.

52 Ibidem, punt 117.

53 Ibidem, punt 118.

54 Ibidem, punt 119.

55 Idem.

56 Idem. Cursivering van mij.

57 Idem.

58 Deze uitzondering zou niet alleen kunnen worden gerechtvaardigd door terroristische activiteiten, maar ook door andere omstandigheden, zoals een grootschalige cyberaanval op kritieke infrastructuur van de lidstaat of een bedreiging in verband met nucleaire proliferatie.

59 Arrest Tele2 Sverige en Watson, punt 120.

60 Ibidem, punt 121.

61 Ibidem, punt 122.

62 Arrest Ministerio Fiscal, punt 53.

63 Ibidem, punt 56.

64 Ibidem, punt 57.

65 Ibidem, punt 59. Het ging om de toegang „tot de telefoonnummers die overeenstemmen met die simkaarten en tot de civiele-identiteitsgegevens van de houders van die kaarten, zoals hun naam, voornaam en, in voorkomend geval, adres. Zoals zowel de Spaanse regering als het openbaar ministerie ter terechtzitting heeft bevestigd, gaat het daarbij echter niet over de communicatie die met de gestolen mobiele telefoon tot stand is gebracht of over de locatie van die telefoon."

66 Ibidem, punt 60.

67 Arrest Ministerio Fiscal, punt 49.

68 De lidstaten nemen sinds 2017 deel aan een werkgroep die tot doel heeft hun wetgeving af te stemmen op de criteria die zijn vastgesteld in de desbetreffende rechtspraak van het Hof [Groep informatie-uitwisseling en gegevensbescherming (Dapix)].

69 Hoe dan ook staat het aan de lidstaten om de opsporingstechnieken te bepalen en de doeltreffendheid ervan te beoordelen.

70 Arrest Digital Rights, punt 57, en arrest Tele2 Sverige en Watson, punt 105.

71 Gegevens die niet strikt en objectief noodzakelijk zijn voor het voorkomen en vervolgen van strafbare feiten en het beschermen van de openbare veiligheid zouden worden uitgesloten van de bewaringsverplichting. Er zou in het bijzonder moeten worden aangegeven welke soorten gegevens van abonnees, verkeersgegevens en locatiegegevens overeenkomstig de nagestreefde doelstelling absoluut moeten worden bewaard om die doelstelling te verwezenlijken. Met name gegevens die niet absoluut noodzakelijk worden geacht voor het onderzoeken en vervolgen van de strafbare feiten, zouden worden uitgesloten.

72 Een methode waarbij de namen worden vervangen door een alias, en de gegevens dus niet langer aan een naam zijn gekoppeld. In tegenstelling tot anonimisering kunnen de gegevens bij pseudonimisering later opnieuw aan de naam van de betrokkene worden gekoppeld.

73 Een mogelijkheid die zou kunnen worden bestudeerd, is dat de bewaringstermijnen zouden worden aangepast naargelang van de verschillende categorieën van gegevens, rekening houdend met het meer of minder ingrijpende karakter in het privéleven van de personen. Voorts zou erin moeten worden voorzien dat de gegevens permanent worden gewist aan het einde van de bewaringstermijn.

74 Er zou kunnen worden overwogen om niet alle aanbieders van elektronischecommunicatiediensten te verplichten om gegevens te bewaren, maar om die verplichting op te leggen op basis van de omvang van die aanbieders en het soort diensten dat zij aanbieden, waarbij bijvoorbeeld aanbieders die bijzonder gespecialiseerde diensten verlenen, zouden kunnen worden vrijgesteld.

75 De vergunningsstelsels zouden gebaseerd kunnen worden op periodieke evaluaties van de bedreigingen in elke lidstaat. Er moet worden gewaarborgd dat het verband tussen de bewaarde gegevens en de nagestreefde doelstelling wordt vastgesteld en wordt aangepast aan de specifieke situatie van elke lidstaat. De aan de aanbieders verleende bewaringsvergunningen zouden derhalve aanleiding kunnen geven tot de bewaring van bepaalde soorten gegevens gedurende een bepaalde termijn, afhankelijk van de evaluatie van de dreiging. Deze vergunningen zouden kunnen worden verleend door een rechter of een onafhankelijk bestuursorgaan en zouden aanleiding geven tot een periodieke herziening van wat absoluut noodzakelijk is bij deze bewaring.

76 Dit lijkt het systeem te zijn dat wordt toegepast in de Bondsrepubliek Duitsland, waarvan de regering tijdens de terechtzitting aangaf dat verkeersgegevens overeenkomstig haar wetgeving tien weken worden bewaard, terwijl de bewaringstermijn voor locatiegegevens slechts vier weken bedraagt. Volgens de Franse Republiek is het daarentegen noodzakelijk dat verkeers- en locatiegegevens een jaar worden bewaard. Volgens die lidstaat zou het verkorten van die termijn tot minder dan een jaar de diensten van de gerechtelijke politie minder doeltreffend maken.

77 Uiteraard moet worden gegarandeerd dat de aanbieders van elektronischecommunicatiediensten de gegevens na afloop van de bewaringstermijn permanent wissen (met uitzondering van de gegevens die zij mogen blijven opslaan voor commerciële doeleinden, overeenkomstig richtlijn 2002/58).

78 Tijdens de terechtzitting verklaarde de Franse regering dat URL's waren uitgesloten van de verbindingsgegevens waarvoor in haar wetgeving een algemene bewaringsverplichting geldt.

79 Ackerman, B., „The Emergency Constitution", *Yale Law Journal*, deel 113, 2004, blz. 1029-1092; Ferejohn, J. en Pasquino, P., „The Law of the Exception: A typology of Emergency Powers", *International Journal of Constitutional Law*, deel 2, 2004, blz. 210-239.

80 Conclusie in de gevoegde zaken C-511/18 en C-512/18, punten 95 e.v.

81 Formulering van de tweede vraag in fine. Die verwijzing naar elektronischecommunicatiemiddelen verklaart dat in de vraag wordt gesproken van een tweede *positieve verplichting* die op de lidstaten rust, namelijk de bij artikel 8 van het Handvest opgelegde verplichting met betrekking tot de bescherming van persoonsgegevens. De dubbele verwijzing naar artikel 8 van het Handvest geeft aan dat de rechten uit het Handvest volgens de verwijzende rechter twee functies vervullen naargelang van hun aard: die van *beperking* van de bestreden verplichting, en die van *rechtvaardiging* van die verplichting.

82 Deze doeltreffendheidsplicht houdt een resultaatsverplichting in voor de overheid in de welvaartsstaat of de op prestaties gebaseerde staat, waarin naast de formele erkenning van de rechten vooral de praktische verwezenlijking van de feitelijke inhoud ervan van belang is.

83 EHRM, arrest van 2 december 2008, K.U. tegen Finland (ECHR:2008:1202JUD000287202, § 46).

84 Wat dat betreft, ben ik van mening dat aan de rechten die de verwijzende rechter vermeldt (als *beperkingen* van de bestreden verplichting, niet als *rechtvaardiging* ervan), ook het recht op een doeltreffende voorziening in rechte (artikel 47 van het Handvest) of het recht van verdediging (artikel 48 van het Handvest) kan worden toegevoegd, waarvan de schending eveneens aan de orde is gesteld in de hoofdgedingen. In het beschikkend gedeelte van de verwijzingsbeslissing wordt echter uitsluitend verwezen naar de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest.

85 EHRM, arrest van 28 oktober 1998, Osman tegen Verenigd Koninkrijk (CE:ECHR:1998:1028JUD002345294, § 116).

86 Ibidem, § 116 in fine: „er moet worden verzekerd dat de politie haar bevoegdheid om criminaliteit te bestrijden en te voorkomen uitoefent met volledige inachtneming van de juridische wegen en de overige waarborgen die de reikwijdte van haar strafrechtelijke onderzoekshandelingen op legitieme wijze beperken". Zie in die zin EHRM, arrest van 2 december 2008, K.U. tegen Finland (CE:ECHR:2008:1202JUD000287202, § 48). Op vergelijkbare wijze heeft het Hof in het arrest van 29 juli 2019, Gambino en Hyka (C-38/18, EU:C:2019:628, punt 49), geoordeeld dat de rechten die toekomen aan het slachtoffer geen afbreuk mogen doen aan het effectieve genot van de rechten die aan de verdachte zijn toegekend.

87 De bewaarplicht is eveneens gerechtvaardigd om gevolg te geven aan een oproep naar een nooddienst of om een vermiste persoon op te sporen wiens fysieke integriteit in onmiddellijk gevaar is.

88 Zie punt 60 van deze conclusie.

89 Arrest Tele2 Sverige en Watson, punt 118.

90 Artikel 126, zoals gewijzigd bij de wet van 29 mei 2016.

91 Of het openbaar ministerie de gepaste instantie is om dit soort maatregelen uit te vaardigen, wordt ter discussie gesteld in prejudiciële verwijzing C-746/18, HK/Prokuratur, die nog in behandeling is.

92 Het vorderen van de identificatiegegevens bij de operatoren is de bevoegdheid van het openbaar ministerie, dat die gegevens opvraagt bij een met redenen omklede en schriftelijke (of in dringende gevallen mondelinge) beslissing, die aantoont dat de maatregel proportioneel is, gelet op de eerbiediging van de persoonlijke levenssfeer, en subsidiair ten opzichte van elke andere onderzoeksdaad. Voor strafbare feiten die geen correctionele hoofdgevangenisstraf van een jaar of een zwaardere straf tot gevolg kunnen hebben, kan het openbaar ministerie de gegevens slechts vorderen voor een periode van zes maanden voorafgaand aan zijn beslissing.

93 Het doen opsporen van elektronische communicatie door de operatoren of het vorderen van de bewaarde verkeers- en locatiegegevens is de bevoegdheid van de onderzoeksrechter, die deze maatregel middels een met redenen omklede schriftelijke (of in dringende gevallen mondelinge) beschikking kan treffen indien er ernstige aanwijzingen zijn voor strafbare feiten waarop bepaalde straffen staan. Dezelfde proportionaliteits- en subsidiariteitsvereisten als voor het openbaar ministerie zijn van toepassing. Er zijn enkele uitzonderingen wanneer de maatregel gericht is tegen bepaalde categorieën van beschermde beroepen (zoals advocaten of artsen).

94 De beslissing vermeldt, naargelang van het geval, de natuurlijke personen of rechtspersonen, feitelijke verenigingen of groeperingen, voorwerpen, plaatsen, gebeurtenissen of informatie die het voorwerp uitmaken van de specifieke methode. Ook moet het verband worden vermeld tussen de gevorderde gegevens en de potentiële dreiging die de specifieke methode rechtvaardigt.

95 De bestuurlijke commissie belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten (BIM-Commissie) en het Vast Comité van Toezicht op de inlichtingendiensten (Comité I). De Belgische regering verklaart dat de BIM-Commissie belast is met het toezicht op de door de inlichtingen- en veiligheidsdiensten gebruikte zoekmethoden, waarover zij de eerstelijnscontrole uitoefent. Deze commissie, die bestaat uit rechters, handelt volledig onafhankelijk in de uitoefening van haar opdrachten. Er wordt ook een onafhankelijke tweedelijnscontrole georganiseerd, door het Comité I.

96 Deze toegang wordt toegestaan voor het onderzoeken, opsporen en vervolgen van de inbreuken bedoeld in de artikelen 114 (beveiliging van netwerken), 124 (vertrouwelijkheid van elektronische communicatie) en 126 (bewaring van en toegang tot gegevens) van de wet van 13 juni 2005 betreffende elektronische communicatie.

97 Ik verwijs naar punt 60 van deze conclusie.

98 Arrest van 28 juli 2016, Association France Nature Environnement (C-379/15, EU:C:2016:603, punt 33).

99 Punt 100 van de schriftelijke opmerkingen van de Commissie.

100 Zaak C-41/11, EU:C:2012:103.

101 Arrest van 28 februari 2012, Inter-Environnement Wallonie en Terre wallonne (C-41/11, EU:C:2012:103, punt 58). In het arrest van 28 juli 2016, Association France Nature Environnement (C-379/15, EU:C:2016:603, punt 34), wordt uit die verklaring afgeleid dat het Hof een nationale rechterlijke instantie de mogelijkheid heeft willen bieden om per geval en bij wijze van uitzondering de gevolgen van de nietigverklaring van een met het Unierecht onverenigbaar geachte nationale bepaling te regelen.

102 Zaak C-411/17 (EU:C:2019:622, punt 178).

103 Arrest van 28 februari 2012, Inter-Environnement Wallonie en Terre wallonne (C-41/11, EU:C:2012:103, punt 57).

104 Arrest van 28 februari 2012, Inter-Environnement Wallonie en Terre wallonne (C-41/11, EU:C:2012:103, punt 62).

105 Punt 45 van de schriftelijke opmerkingen van de Deense regering.