geheim moet opereren. Het ontbreken van procesvertegenwoordiging in de eerste twee stadia zal ook de uitoefening van een recht van hoger beroep bemoeilijken. Dit kan alleen in stadium 2 gecompenseerd worden als het slachtoffer op basis van een vermoeden dat hij wordt gevolgd een procedure bij de toezichthouder start. Daarom is het heel belangrijk dat de rechter/toezichthouder toegang heeft tot alle geheime informatie en voldoende technische bijstand in deze steeds complexere materie van datatechnologie. Dit blijkt duidelijk uit de geciteerde overweging in de *Kennedy*-zaak, die de constante jurisprudentie van het Hof in dit opzicht bevestigt. De toezichthouder zal ook over precieze wettelijke normen moeten beschikken en hoge eisen aan de motivering van collectieve aftapbeslissingen moeten stellen. Anders dreigt een praktijk van 'stempelbeschikkingen'.

9. Uit de jurisprudentie van het Hof blijkt dat er maar een beperkte margin of appreciation is, hoewel deze varieert naar het stadium van het toezicht. De onderhavige zaak is daarvan een bevestiging. In maar liefst zestig overwegingen onderzoekt het Hof alle hiervoor genoemde aspecten van het toezicht en beoordeelt het ze bijna allemaal als te licht, niet alleen de wettelijke regels die de procedure regelen, maar ook de onderbouwing van de specifieke maatregelen zelf. Ik verwijs naar de interessante r.o. 263-267.

10. Een apart aspect van het toezicht is het politieke toezicht. Dat is weliswaar iets anders dan het (pseudo)rechterlijke toezicht, maar toch betrekt het Hof de vraag of er afdoende politiek toezicht (waaraan het ook eisen van onafhankelijkheid stelt) is bij zijn beoordeling. Dat zien we in deze zaak in r.o. 283: "The Court must also examine whether the supervisory body's activities are open to public scrutiny". In r.o. 278 had het al geconstateerd dat politiek toezicht (bijvoorbeeld door een minister) dat niet onafhankelijk is onvoldoende is. De vraag moet worden gesteld of dat niet ook geldt voor het parlementaire toezicht in Nederland in de 'Commissie Stiekem' in de Tweede Kamer waarvan de verrichtingen volkomen ondoorzichtig zijn en die niet los staat van het Parlement.

11. Ik verwijs tot slot naar Sarah Eskens, Ot van Daalen & Nico van Eijk, *Ten standards for oversight and transparency of national intelligence services,* Amsterdam: Instituut voor Informatierecht 2015 ook gepubliceerd in http://jnslp.com/2016/07/25/10-standards-oversight-transparency-national-intelligence-services/, waarin de hele jurisprudentie van het Hof wordt geanalyseerd.

EU recht

12. Het HvJ EU is door de Dataretentierichtlijn (2002/58) en het Handvest ook geconfronteerd met een soortgelijke toetsing als het EHRM waarvan het de door deze ontwikkelde jurisprudentie getrouw volgt, zonder overigens art. 8 EVRM rechtstreeks toe te passen, maar door invulling te geven aan de art. 7 en 8 van het Handvest overeenkomstig art. 52 dat het EVRM als minimum beschermingsnorm aangeeft. Tot dusver toetste het voornamelijk de kwaliteit van de EU regelingen, zie HvJ EU 8 april 2014, (*Digital Rights/Ireland*, zaken C-293/12 en C-594/12) en HvJ EU 6 oktober 2015 (zaak *Schrems/Ireland*, zaak C-362/14), *NJ* 2016/446 en NJ 2016/447, m.nt. E.J. Dommering. Dat is begrijpelijk omdat het HvJ EU op basis van prejudiciële vragen de verenigbaarheid van nationaal recht met het EU recht of van een richtlijn met het Handvest beoordeelt. De *Digital Rights* uitspraak is gevolgd door de zaak *Tele2*, HvJ EU 21 december 2016, *NJ* 2017/186. Het Hof achtte het systeem van de Dataretentierichtlijn dat de verplichting oplegt alle communicatiegegevens van telefoon en internetverkeer van alle gebruikers gedurende zekere tijd op te slaan in strijd met de art. 7 (privacy), 8 (dataprotectie) en 11 (vrijheid van meningsuiting) van het Handvest. Dat is de eerste door het EHRM geformuleerde kwaliteitseis waaraan dit soort wetgeving moet voldoen: Bestaat er een definitie van de categorieën van personen die mogen worden afgeluisterd? Het is de uitdrukking van het beginsel uit het dataprotectierecht: 'select before you collect'. Ook dit aspect zou bij een toetsing van de WIV relevant kunnen worden, omdat deze wet in de eerste fase van een onderzoek een zeer ruime verzamelbevoegdheid aan de Veiligheidsdienst toekent.

E.J. Dommering

NJ 2017/186

HOF VAN JUSTITIE VAN DE EUROPESE UNIE
21 december 2016, nr. C-203/15 en C-698/15
(K. Lenaerts, A. Tizzano, R. Silva de Lapuerta, T. von Danwitz, J.L. da Cruz Vilaça, E. Juhász, M. Vilaras, A. Borg Barthet, J. Malenovský, E. Levits, J.-C. Bonichot, A. Arabadjiev, S. Rodin, F. Biltgen, C. Lycourgos; A-G H. Saugmandsgaard Øe)
m.nt. E.J. Dommering

Art. 5, 6, 9, 15 lid 1 e-Privacyrichtlijn; art. 7, 8, 11, 52 lid 1 Handvest Grondrechten EU

RvdW 2017/251
Computerrecht 2017/50
Module Privacy en persoonsgegevens 2017/1150
ECLI:EU:C:2016:572
ECLI:EU:C:2016:970

Verzoeken om een prejudiciële beslissing, ingediend door de Kammarrätt i Stockholm (bestuursrechter in tweede aanleg Stockholm, Zweden) en de Court of Appeal (England and Wales) (Civil Division) (rechter in tweede aanleg in burgerlijke zaken, Engeland en Wales, Verenigd Koninkrijk), bij beslissingen van, respectievelijk, 29 april 2015 en 9 december 2015.

Elektronische communicatie. Verwerking van persoonsgegevens. Vertrouwelijk karakter van de

elektronische communicatie. Bescherming. Nationale wettelijke regeling. Aanbieders van elektronischecommunicatiediensten. Verplichting betreffende het algemeen en ongedifferentieerd bewaren van de verkeersgegevens en de locatiegegevens. Nationale autoriteiten. Toegang tot gegevens. Geen voorafgaande toetsing door een rechterlijke instantie of door een onafhankelijke bestuurlijke autoriteit. Verenigbaarheid met het Unierecht.

Art. 15 lid 1 Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), zoals gewijzigd bij Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009, gelezen tegen de achtergrond van de art. 7, 8, 11, 52 lid 1 Handvest Grondwet EU, moet in die zin worden uitgelegd dat het zich verzet tegen een nationale regeling die, ter bestrijding van criminaliteit, voorziet in algemene en ongedifferentieerde bewaring van alle verkeersgegevens en locatiegegevens van alle abonnees en geregistreerde gebruikers betreffende alle elektronische communicatiemiddelen.

Art. 15 lid 1 Richtlijn 2002/58/EG, zoals gewijzigd bij Richtlijn 2009/136/EG, gelezen tegen de achtergrond van de art. 7, 8, 11, 52 lid 1 van het Handvest, moet in die zin worden uitgelegd dat het zich verzet tegen een nationale regeling die de bescherming en de beveiliging van de verkeersgegevens en de locatiegegevens en in het bijzonder de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens regelt zonder, in het kader van de bestrijding van criminaliteit, te bepalen dat die toegang alleen wordt verleend ter bestrijding van ernstige criminaliteit, dat die toegang aan een voorafgaand toezicht door een rechterlijke instantie of een onafhankelijke bestuurlijke autoriteit is onderworpen, en dat de betrokken gegevens op het grondgebied van de Unie moeten worden bewaard.

De tweede vraag van de Court of Appeal (England and Wales) (Civil Division) (rechter in tweede aanleg in burgerlijke zaken, Engeland en Wales, Verenigd Koninkrijk) is niet-ontvankelijk.

Tele2 Sverige AB (C-203/15)
tegen
Post- och telestyrelsen en Secretary of State for the Home Department (C-698/15)
tegen
T. Watson, P. Brice, G. Lewis

Hof van Justitie EU:

1 De verzoeken om een prejudiciële beslissing betreffen de uitlegging van artikel 15, lid 1, van richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (*PB* 2002, L 201, p. 37), zoals gewijzigd bij richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 (*PB* 2009, L 337, p. 11) (hierna: 'richtlijn 2002/58'), gelezen tegen de achtergrond van de artikelen 7 en 8 en artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie (hierna: 'Handvest').

2 Deze verzoeken zijn ingediend in het kader van twee gedingen, het eerste tussen Tele2 Sverige AB en de Post- och telestyrelse (Zweedse toezichthoudende autoriteit voor post en telecommunicatie; hierna: 'PTS') over een door laatstgenoemde aan Tele2 Sverige gegeven bevel om de verkeersgegevens en de locatiegegevens van haar abonnees en geregistreerde gebruikers te bewaren (zaak C-203/15), en het tweede tussen Tom Watson, Peter Brice en Geoffrey Lewis enerzijds en de Secretary of State for the Home Department (minister van Binnenlandse Zaken, Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland) anderzijds over de overeenstemming met het Unierecht van section 1 van de Data Retention and Investigatory Powers Act 2014 (wet van 2014 betreffende de bewaring van gegevens en de onderzoeksbevoegdheden; hierna: 'DRIPA') (zaak C-698/15).

Toepasselijke bepalingen

Unierecht

Richtlijn 2002/58

3 In de overwegingen 2, 6, 7, 11, 21, 22, 26 en 30 van richtlijn 2002/58 staat te lezen:

"(2) Deze richtlijn strekt tot eerbiediging van de grondrechten en beginselen die tot uitdrukking zijn gebracht in met name het [Handvest]. In het bijzonder strekt deze richtlijn tot volledige eerbiediging van de in de artikelen 7 en 8 [van het Handvest] bedoelde rechten […].

[…]

(6) Het internet vervangt traditionele marktstructuren door te voorzien in een gemeenschappelijke, wereldwijde infrastructuur voor de levering van een breed scala van elektronischecommunicatiediensten. Algemeen beschikbare elektronischecommunicatiediensten via het internet bieden de gebruikers nieuwe mogelijkheden, maar houden ook nieuwe gevaren in voor de bescherming van hun persoonsgegevens en persoonlijke levenssfeer.

(7) Voor openbare communicatienetwerken moeten specifieke wettelijke, bestuursrechtelijke en technische bepalingen worden vastgesteld teneinde de fundamentele rechten en vrijheden van natuurlijke personen en de rechtmatige belangen van rechtspersonen te beschermen tegen met name de steeds grotere mogelijkheden in verband met de geautomatiseerde opslag en verwerking van gegevens met betrekking tot de abonnees en de gebruikers.

[…]

(11) Deze richtlijn is evenmin als richtlijn 95/46/EG [van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (*PB* 1995, L 281, p. 31)] van toepassing op vraagstukken met betrekking tot de bescherming van fundamentele rechten en vrijheden in verband met niet onder het gemeenschapsrecht vallende activiteiten. Zij verandert bijgevolg niets aan het bestaande evenwicht tussen het recht van personen op persoonlijke levenssfeer en de mogelijkheid voor de lidstaten om de in artikel 15, lid 1, van deze richtlijn bedoelde maatregelen te nemen, die nodig zijn voor de bescherming van de openbare veiligheid, defensie, staatsveiligheid (met inbegrip van het economisch welzijn van de staat wanneer de activiteit verband houdt met de staatsveiligheid) en de wetshandhaving op strafrechtelijk gebied. Bijgevolg doet deze richtlijn geen afbreuk aan de mogelijkheid voor de lidstaten om wettelijk toegestane interceptie van elektronische communicatie uit te voeren of andere maatregelen vast te stellen, wanneer dat voor één van voornoemde doeleinden noodzakelijk is, mits zij daarbij het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, zoals geïnterpreteerd in de uitspraken van het Europees Hof voor de rechten van de mens, in acht nemen. Zulke maatregelen dienen passend te zijn voor, en strikt evenredig met, het beoogde doel en noodzakelijk in een democratische samenleving en moeten adequate waarborgen bevatten overeenkomstig het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden.

[…]

(21) Er moeten maatregelen worden getroffen om onbevoegde toegang tot communicatie te verhinderen, teneinde het vertrouwelijk karakter van communicatie via openbare communicatienetwerken en openbare elektronischecommunicatiediensten te beschermen, zowel ten aanzien van de inhoud zelf als van gegevens over die communicatie. De nationale wetgeving van sommige lidstaten verbiedt uitsluitend opzettelijke onbevoegde toegang tot communicatie.

(22) Het verbod op het opslaan van communicatie en de daarmee verband houdende verkeersgegevens door anderen dan de gebruikers of zonder hun toestemming is niet bedoeld om de automatische, tussentijdse en tijdelijke opslag van die informatie te verbieden, voor zover deze opslag uitsluitend dient voor het doorzenden in het elektronischecommunicatienetwerk en mits de informatie niet langer wordt opgeslagen dan nodig voor het doorzenden en het beheer van het verkeer, en het vertrouwelijk karakter tijdens de opslag gewaarborgd blijft. […]

[…]

(26) De gegevens over abonnees die in elektronischecommunicatienetwerken worden verwerkt om verbindingen tot stand te brengen en informatie over te dragen, bevatten informatie over het privéleven van natuurlijke personen en betreffen het recht op respect voor hun correspondentie of de rechtmatige belangen van rechtspersonen. Dergelijke gegevens mogen slechts worden opgeslagen voor zover dat nodig is voor het leveren van de dienst, voor facturering en voor interconnectiebetalingen, en slechts gedurende een beperkte tijd. Elke verdere verwerking van dergelijke gegevens […] is slechts toegestaan indien de abonnee daarmee heeft ingestemd op basis van precieze en volledige informatie van de aanbieder van de openbare elektronischecommunicatiedienst over de door hem geplande verdere verwerking van de gegevens en over het recht van de abonnee een dergelijke verwerking niet toe te staan of de toestemming daartoe in te trekken. […]

[…]

(30) Systemen voor elektronischecommunicatienetwerken en -diensten moeten op dusdanige wijze worden ontworpen dat het aantal persoonsgegevens tot het strikt noodzakelijke minimum wordt beperkt. […]"

4 Artikel 1, 'Werkingssfeer en doelstelling', van richtlijn 2002/58 bepaalt:

"1. Deze richtlijn voorziet in de harmonisering van de regelgeving van de lidstaten die nodig is om een gelijk niveau van bescherming van fundamentele rechten en vrijheden — met name het recht op een persoonlijke levenssfeer en vertrouwelijkheid — bij de verwerking van persoonsgegevens in de sector elektronische communicatie te waarborgen en om te zorgen voor het vrij verkeer van dergelijke gegevens en van elektronischecommunicatieapparatuur en -diensten in de Gemeenschap.

2. Voor de doelstellingen van lid 1 vormen de bepalingen van deze richtlijn een specificatie van en een aanvulling op richtlijn [95/46]. Bovendien voorzien zij in bescherming van de rechtmatige belangen van abonnees die rechtspersonen zijn.

3. Deze richtlijn is niet van toepassing op activiteiten die niet onder het EG-Verdrag vallen, zoals die bedoeld in de titels V en VI van het Verdrag betreffende de Europese Unie, en in geen geval op activiteiten die verband houden met de openbare veiligheid, defensie, staatsveiligheid (met inbegrip van het economische welzijn van de staat wanneer de activiteit verband houdt met de staatsveiligheid) en de activiteiten van de staat op strafrechtelijk gebied."

5 In artikel 2, 'Definities', van richtlijn 2002/58, staat:

"Tenzij anders is bepaald, zijn de definities van richtlijn [95/46] en richtlijn 2002/21/EG van het Europees Parlement en de Raad van 7 maart

2002 inzake een gemeenschappelijk regelgevingskader voor elektronischecommunicatienetwerken en -diensten ('kaderrichtlijn') [(*PB* 2002, L 108, p. 33)] van toepassing.
Daarnaast wordt in deze richtlijn verstaan onder:
[…]
b) 'verkeersgegevens': gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronischecommunicatienetwerk of voor de facturering ervan;
c) 'locatiegegevens': gegevens die in een elektronischecommunicatienetwerk of door een elektronischecommunicatiedienst worden verwerkt, waarmee de geografische positie van de eindapparatuur van een gebruiker van een openbare elektronischecommunicatiedienst wordt aangegeven;
d) 'communicatie': informatie die wordt uitgewisseld of overgebracht tussen een eindig aantal partijen door middel van een openbare elektronischecommunicatiedienst. Dit omvat niet de informatie die via een omroepdienst over een elektronischecommunicatienetwerk wordt overgebracht, behalve wanneer de informatie kan worden gerelateerd aan de identificeerbare abonnee of gebruiker die de informatie ontvangt;
[…]"

6 Artikel 3, 'Betrokken diensten', van richtlijn 2002/58 bepaalt:

"Deze richtlijn is van toepassing op de verwerking van persoonsgegevens in verband met de levering van openbare elektronischecommunicatiediensten over openbare communicatienetwerken in de Gemeenschap, met inbegrip van openbare communicatienetwerken die systemen voor gegevensverzameling en identificatie ondersteunen."

7 Artikel 4, 'Beveiliging van de verwerking', van deze richtlijn luidt als volgt:

"1. De aanbieder van een openbare elektronischecommunicatiedienst treft passende technische en organisatorische maatregelen om de veiligheid van zijn diensten te garanderen, indien nodig in overleg met de aanbieder van het openbare communicatienetwerk wat de veiligheid van het netwerk betreft. Die maatregelen waarborgen een beveiligingsniveau dat in verhouding staat tot het betrokken risico, rekening houdend met de stand van de techniek en de kosten van uitvoering ervan.
1 bis. Onverminderd richtlijn [95/46] zorgen de in lid 1 bedoelde maatregelen ervoor dat in ieder geval:
— wordt gewaarborgd dat alleen gemachtigd personeel voor wettelijk toegestane doeleinden toegang heeft tot de persoonsgegevens;
— opgeslagen of verzonden persoonsgegevens worden beschermd tegen onbedoelde of onwettige vernietiging, onbedoeld verlies of wijziging, en niet-toegestane of onwettige opslag, verwerking, toegang of vrijgave, en
— een beveiligingsbeleid wordt ingevoerd met betrekking tot de verwerking van persoonsgegevens.
[…]"

8 In artikel 5, 'Vertrouwelijk karakter van de communicatie', van richtlijn 2002/58 staat:

"1. De lidstaten garanderen via nationale wetgeving het vertrouwelijke karakter van de communicatie en de daarmee verband houdende verkeersgegevens via openbare communicatienetwerken en via openbare elektronischecommunicatiediensten. Zij verbieden met name het afluisteren, aftappen, opslaan of anderszins onderscheppen of controleren van de communicatie en de daarmee verband houdende verkeersgegevens door anderen dan de gebruikers, indien de betrokken gebruikers daarin niet hebben toegestemd, tenzij dat bij wet is toegestaan overeenkomstig artikel 15, lid 1. Dit lid laat de technische opslag die nodig is voor het overbrengen van informatie onverlet, onverminderd het vertrouwelijkheidsbeginsel.
[…]
3. De lidstaten dragen ervoor zorg dat de opslag van informatie of het verkrijgen van toegang tot informatie die reeds is opgeslagen in de eindapparatuur van een abonnee of gebruiker, alleen is toegestaan op voorwaarde dat de betrokken abonnee of gebruiker toestemming heeft verleend, na te zijn voorzien van duidelijke en volledige informatie overeenkomstig richtlijn [95/46], onder meer over de doeleinden van de verwerking. Zulks vormt geen beletsel voor enige vorm van technische opslag of toegang met als uitsluitend doel de uitvoering van de verzending van een communicatie over een elektronischecommunicatienetwerk, of, indien strikt noodzakelijk, om ervoor te zorgen dat de aanbieder van een uitdrukkelijk door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij deze dienst levert."

9 Artikel 6, 'Verkeersgegevens', van richtlijn 2002/58 bepaalt:

"1. Verkeersgegevens met betrekking tot abonnees en gebruikers die worden verwerkt en opgeslagen door de aanbieder van een openbaar elektronischecommunicatienetwerk of -dienst, moeten, wanneer ze niet langer nodig zijn voor het doel van de transmissie van communicatie, worden gewist of anoniem gemaakt, onverminderd de leden 2, 3 en 5, alsmede artikel 15, lid 1.
2. Verkeersgegevens die noodzakelijk zijn ten behoeve van de facturering van abonnees en interconnectiebetalingen mogen worden verwerkt. Die verwerking is slechts toegestaan tot aan het einde van de termijn waarbinnen de rekening in rechte kan worden aangevochten of de betaling kan worden afgedwongen.
3. De aanbieder van een openbare elektronischecommunicatiedienst mag ten behoeve

van de marketing van elektronischecommunicatiediensten of voor de levering van diensten met toegevoegde waarde de in lid 1 bedoelde gegevens verwerken voor zover en voor zolang dat nodig is voor dergelijke diensten of marketing, indien de abonnee of de gebruiker waarop de gegevens betrekking hebben daartoe zijn voorafgaande toestemming heeft gegeven. Gebruikers of abonnees kunnen hun toestemming voor de verwerking van verkeersgegevens te allen tijde intrekken.

[…]

5. De verwerking van verkeersgegevens overeenkomstig de leden 1 tot en met 4 mag alleen worden uitgevoerd door personen die werkzaam zijn onder het gezag van de aanbieders van de openbare communicatienetwerken of -diensten voor facturering of verkeersbeheer, behandeling van verzoeken om inlichtingen van klanten, opsporing van fraude en marketing van elektronischecommunicatiediensten van de aanbieder of de levering van diensten met toegevoegde waarde, en moet beperkt blijven tot hetgeen noodzakelijk is om die activiteiten te kunnen uitvoeren."

10 In artikel 9, 'Andere locatiegegevens dan verkeersgegevens', lid 1, van deze richtlijn staat:

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

11 Artikel 15, 'Toepassing van een aantal bepalingen van richtlijn [95/46]', van deze richtlijn luidt als volgt:

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

[…]

1 ter. Aanbieders zetten interne procedures op voor de afhandeling van verzoeken om toegang tot persoonsgegevens van gebruikers op de grondslag van nationale bepalingen die overeenkomstig lid 1 zijn aangenomen. Zij verstrekken aan de bevoegde nationale instantie op verzoek gegevens over deze procedures, het aantal ontvangen verzoeken, de aangevoerde wettelijke motivering en hun antwoord.

2. Het bepaalde in hoofdstuk III van richtlijn [95/46] inzake beroep op de rechter, aansprakelijkheid en sancties geldt voor de nationale bepalingen die uit hoofde van deze richtlijn worden aangenomen en ten aanzien van de individuele rechten die uit deze richtlijn voortvloeien.

[…]"

Richtlijn 95/46

12 Artikel 22 van richtlijn 95/46, dat deel uitmaakt van hoofdstuk III van deze richtlijn, luidt als volgt:

"Onverminderd de administratieve voorziening die met name bij de in artikel 28 bedoelde toezichthoudende autoriteit kan worden getroffen voordat de zaak aanhangig wordt gemaakt voor de rechter, bepalen de lidstaten dat een ieder zich tot de rechter kan wenden wanneer de rechten die hem worden gegarandeerd door het op de betrokken verwerking toepasselijke nationale recht geschonden worden."

Richtlijn 2006/24

13 Artikel 1, 'Onderwerp en werkingssfeer', lid 2, van richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronischecommunicatiediensten of van openbare communicatienetwerken en tot wijziging van richtlijn 2002/58/EG (*PB* 2006, L 105, p. 54) bepaalde:

"Deze richtlijn heeft betrekking op verkeers- en locatiegegevens van natuurlijke en rechtspersonen, evenals op de daarmee verband houdende gegevens die nodig zijn om de abonnee of geregistreerde gebruiker te identificeren. Zij is niet van toepassing op de inhoud van elektronische communicatie, de informatie die wordt geraadpleegd met behulp van een elektronischecommunicatienetwerk daaronder begrepen."

14 Artikel 3, 'Verplichting om gegevens te bewaren', van deze richtlijn luidt als volgt:

"1. In afwijking van de artikelen 5, 6 en 9 van richtlijn [2002/58] nemen de lidstaten bepalingen aan om te waarborgen dat de in artikel 5 bedoelde gegevens, voor zover deze in het kader van de aanbieding van de bedoelde communicatiediensten worden gegenereerd of verwerkt door onder hun rechtsmacht vallende aanbieders van openbare elektronischecommunicatiediensten of een openbaar communicatienetwerk bij het leveren van de betreffende communicatiediensten, worden bewaard overeenkomstig de bepalingen van deze richtlijn.

2. De verplichting tot gegevensbewaring voorzien in lid 1 omvat de bewaring van de in artikel 5 bedoelde gegevens betreffende oproeppogingen zonder resultaat waarbij die gegevens, voor zover die in verband met de aanbieding van de bedoelde communicatiediensten worden gegenereerd, verwerkt en opgeslagen (wat telefoniegegevens betreft) of gelogd (wat internetgegevens betreft) door onder de rechtsmacht van de betrokken lidstaat vallende aanbieders van openbaar beschikbare elektronischecommunicatiediensten of van een openbaar communicatienetwerk. Deze richtlijn bevat geen vereisten betreffende de bewaring van gegevens in verband met niet tot stand gekomen verbindingen."

Zweeds recht

15 Uit de verwijzingsbeslissing in zaak C-203/15 blijkt dat de Zweedse wetgever, om richtlijn 2006/24 in nationaal recht om te zetten, de lag (2003:389) om elektronisk kommunikation [wet (2003:389) betreffende elektronische communicatie; hierna: 'LEK'] en de förordning (2003:396) om elektronisk kommunikation [verordening (2003:396) betreffende elektronische communicatie; hierna: 'FEK'] heeft gewijzigd. Beide teksten, in de op het hoofdgeding toepasselijke versie ervan, bevatten regels over het bewaren van de gegevens betreffende elektronische communicatie en over de toegang van de nationale autoriteiten tot die gegevens.

16 De toegang tot die gegevens wordt bovendien geregeld in de lag (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet [wet (2012:278) betreffende de verzameling van gegevens over elektronische communicatie bij de opsporingsactiviteiten van handhavingsautoriteiten; hierna: 'wet 2012:278'] en in de rättegångsbalk (wetboek van burgerlijke rechtsvordering; hierna: 'RB').

Verplichting tot bewaring van de gegevens betreffende de elektronische communicatie

17 Volgens de door de verwijzende rechterlijke instantie in zaak C-203/15 verstrekte gegevens legt § 16 a van hoofdstuk 6 van de LEK, gelezen in samenhang met § 1 van hoofdstuk 2 van deze wet, de aanbieders van elektronischecommunicatiediensten de verplichting op tot bewaring van de gegevens die volgens richtlijn 2006/24 dienden te worden bewaard. Het gaat om de gegevens betreffende de abonnementen en de elektronische communicatie die nodig zijn voor het opsporen en identificeren van de bron en de bestemming van een communicatie, voor het bepalen van de datum, het tijdstip, de duur en de aard van de communicatie, voor het identificeren van de gebruikte communicatieapparatuur en voor het bepalen van de locatie van de mobiele communicatieapparatuur bij de aanvang en de beëindiging van de communicatie. De bewaringsverplichting betreft gegevens die zijn gegenereerd of verwerkt in het kader van telefoondiensten, telefoondiensten via mobiele aansluitingspunten, systemen voor elektronischeberichtenverkeer, en diensten die toegang tot het internet verschaffen of capaciteit voor internettoegang ter beschikking stellen (connector). Deze verplichting geldt ook voor de gegevens betreffende niet tot stand gekomen communicaties. Zij ziet echter niet op de inhoud van de communicaties.

18 In de §§ 38 tot en met 43 van de verordening (2003:396) betreffende elektronische communicatie wordt nader uiteengezet welke categorieën van gegevens moeten worden bewaard. Wat de telefoondiensten betreft, moeten met name het bellende en het opgebelde nummer worden bewaard, alsook de datum en het traceerbare tijdstip waarop de communicatie begon en eindigde. Met betrekking tot de telefoondiensten via mobiele aansluitingspunten worden aanvullende verplichtingen opgelegd, zoals bijvoorbeeld het bewaren van de locatiegegevens van het begin en het einde van de communicatie. Met betrekking tot de telefoondiensten waarbij internetprotocollen worden gebruikt, moeten, behalve bovengenoemde gegevens, met name ook de IP-adressen van de beller en van de opgebelde persoon worden bewaard. Met betrekking tot de systemen van elektronischeberichtenverkeer moeten met name de nummers en de IP-adressen of andere berichtadressen van de verzenders en de ontvangers worden bewaard. Ter zake van de diensten die toegang tot het internet verschaffen, moeten bijvoorbeeld het IP-adres van de gebruiker alsook de datum en het traceerbare tijdstip van de log-in en log-off van de internetsessie worden bewaard.

Bewaringstermijn van de gegevens

19 Volgens § 16 d van hoofdstuk 6 van de LEK moeten de in § 16 a van dat hoofdstuk bedoelde gegevens door de aanbieders van elektronischecommunicatiediensten worden bewaard gedurende zes maanden te rekenen vanaf de dag waarop de communicatie is beëindigd. Zij moeten vervolgens onverwijld worden gewist, tenzij in § 16 d, tweede alinea, van dat hoofdstuk anders is bepaald.

Toegang tot de bewaarde gegevens

20 De toegang tot de door de nationale autoriteiten bewaarde gegevens wordt geregeld door de bepalingen van wet 2012:278, van de LEK en van de RB.

— *Wet 2012:278*

21 In het kader van de inlichtingsactiviteiten mogen de nationale politie, de Säkerhetspolis (inlichtingendienst, Zweden) en de Tullverk (douane, Zweden) op grond van § 1 van wet 2012:278 onder de in die wet gestelde voorwaarden buiten medeweten van degene die overeenkomstig de LEK een elektronischecommunicatienetwerk of een elektronischecommunicatiedienst aanbiedt, gegevens verzamelen over de berichten die in een elektronischecommunicatienetwerk zijn overgebracht, de elektronischecommunicatieapparatuur die in een bepaald geografisch gebied aanwezig was, en het geografische gebied of de geografische gebieden waarin bepaalde elektronischecommunicatieapparatuur aanwezig is of was.

22 Volgens de §§ 2 en 3 van wet 2012:278 kunnen de gegevens in beginsel worden verzameld indien de omstandigheden van dien aard zijn dat de maatregel bijzonder noodzakelijk is voor het voorkomen, verhinderen of vaststellen van een criminele activiteit die ofwel een of meer strafbare feiten omvat waarop ten minste twee jaar gevangenisstraf staat, ofwel een van de in § 3 van die wet genoemde handelingen, waaronder strafbare feiten waarop een gevangenisstraf van minder dan twee jaar staat. De redenen voor deze maatregel moeten opwegen tegen de aantasting of de schade die deze maatregel meebrengt voor degene die er het voorwerp van is, of voor een tegengesteld belang. Volgens § 5 van die wet mag de maatregel niet meer dan een maand duren.

23 De beslissing om een dergelijke maatregel te treffen wordt genomen door de directeur van de betrokken autoriteit of door een daartoe gemachtigde persoon. Zij is niet onderworpen aan voorafgaande toetsing door een rechterlijke instantie of door een onafhankelijke bestuurlijke autoriteit.

24 Volgens § 6 van wet 2012:278 moet de Säkerhets- och integritetsskyddsnämnd (veiligheids- en integriteitscommissie, Zweden) in kennis worden gesteld van elke beslissing waarbij toestemming wordt verleend voor het verzamelen van gegevens. Op grond van § 1 van de lag (2007:980) om tillsyn över viss brottsbekämpande verksamhet [wet (2007:980) betreffende het toezicht op bepaalde wetshandhavingsactiviteiten] moet die autoriteit toezien op de toepassing van de wet door de handhavingsautoriteiten.

— *LEK*

25 Volgens § 22, eerste alinea, punt 2, van hoofdstuk 6 van de LEK moet iedere aanbieder van elektronischecommunicatiediensten op verzoek van het parket, van de nationale politie, van de inlichtingendienst of van enige andere strafrechtelijke autoriteit de abonnementsgegevens meedelen indien die gegevens verband houden met een vermoeden van een strafbaar feit. Volgens de door de verwijzende rechterlijke instantie in zaak C-203/15 verstrekte gegevens is het niet noodzakelijk dat het daarbij gaat om een ernstig strafbaar feit.

— *RB*

26 De RB regelt de mededeling van de bewaarde gegevens aan de nationale autoriteiten in het kader van opsporingsonderzoeken. Volgens § 19 van hoofdstuk 27 van de RB is het 'onder toezicht plaatsen van elektronische communicaties' buiten medeweten van derden in beginsel toegestaan in het kader van opsporingsonderzoeken naar, met name, strafbare feiten waarop een gevangenisstraf van ten minste zes maanden staat. Onder het 'onder toezicht plaatsen van elektronische communicaties' dient volgens § 19 van hoofdstuk 27 van de RB te worden verstaan, het buiten medeweten van derden verkrijgen van gegevens over berichten die in een elektronischecommunicatienetwerk worden overgebracht, de elektronischecommunicatieapparatuur die in een bepaald geografisch gebied aanwezig is of was, en het geografische gebied of de geografische gebieden waarin bepaalde elektronischecommunicatieapparatuur aanwezig is of was.

27 Volgens de door de verwijzende rechterlijke instantie in zaak C-203/15 verstrekte gegevens kunnen op grond van § 19 van hoofdstuk 27 van de RB geen inlichtingen worden verkregen over de inhoud van een bericht. In beginsel kan op grond van § 20 van hoofdstuk 27 van de RB het onder toezicht plaatsen van elektronische communicaties slechts worden gelast wanneer een persoon op grond van plausibele aanwijzingen van een strafbaar feit wordt verdacht en de maatregel van bijzonder belang is voor het onderzoek, waarbij dit onderzoek betrekking moet hebben op een strafbaar feit waarop een gevangenisstraf van ten minste twee jaar staat of op de poging tot, de voorbereiding van of de strafbare samenspanning tot een dergelijk strafbaar feit. Volgens § 21 van hoofdstuk 27 van de RB moet het parket, behoudens in gevallen van spoedeisendheid, de bevoegde rechter toestemming vragen voor het onder toezicht plaatsen van elektronische communicaties.

Beveiliging en bescherming van de bewaarde gegevens

28 Volgens § 3 a van hoofdstuk 6 van de LEK moeten de aanbieders van elektronischecommunicatiediensten op wie een verplichting tot bewaring van de gegevens rust, passende technische en organisatorische maatregelen nemen om de bescherming van de gegevens bij de verwerking ervan te garanderen. Volgens de door de verwijzende rechterlijke instantie in zaak C-203/15 verstrekte gegevens bevat het Zweedse recht echter geen bepalingen over de plaats waar de gegevens moeten worden bewaard.

Recht van het Verenigd Koninkrijk

DRIPA

29 Section 1, 'Aan waarborgen onderworpen bevoegdheden tot bewaring van relevante communicatiegegevens', van de DRIPA bepaalt:

"(1) De Secretary of State kan door middel van een handeling (de 'aanzegging tot bewaring') eisen dat een openbaar telecommunicatiebedrijf relevante communicatiegegevens bewaart, indien hij van mening is dat dit noodzakelijk en evenredig is met het oog op een of meer van de doelstellingen van de punten (a) tot en met (h) van section 22, lid 2, van de Regulation of Investigatory Powers Act 2000 [wet van 2000 houdende regeling van de onderzoeksbevoegdheden] (doelstellingen waarvoor communicatiegegevens mogen worden verzameld).

(2) Een aanzegging tot bewaring kan

(a) betrekking hebben op één bepaald bedrijf of een bepaalde categorie bedrijven;

(b) de bewaring van alle gegevens of een bepaald type gegevens vereisen;

(c) de periode of de perioden aangeven gedurende welke de gegevens moeten worden bewaard;

(d) andere voorwaarden of beperkingen bevatten met betrekking tot de bewaring van de gegevens;

(e) voor verschillende doeleinden verschillende regelingen treffen, en

(f) betrekking hebben op gegevens die al dan niet bestaan op het moment waarop de aanzegging wordt gedaan of van kracht wordt.

(3) De Secretary of State kan, bij wege van verordening, nadere regelingen over de bewaring van relevante communicatiegegevens vaststellen.

(4) Dergelijke regelingen kunnen met name betrekking hebben op:

(a) de voorwaarden voor het doen van een aanzegging;

(b) de maximumduur van de gegevensbewaring op grond van een aanzegging tot bewaring;

(c) de inhoud, de vaststelling, het van kracht worden, de herziening, de wijziging of de herroeping van een aanzegging tot bewaring;

(d) de volledigheid, de beveiliging of de bescherming van de op grond van deze section bewaarde gegevens, de toegang tot die gegevens en het openbaar maken of het vernietigen ervan;

(e) de handhaving, of de controle op de naleving, van de relevante voorschriften of beperkingen;

(f) een gedragscode met betrekking tot de relevante voorwaarden, beperkingen of bevoegdheden;

(g) de (al dan niet aan voorwaarden verbonden) vergoeding door de Secretary of State van de kosten die openbare telecommunicatiebedrijven maken om te voldoen aan relevante voorschriften of beperkingen, en

(h) de buitenwerkingtreding van de [Data Retention (EC Directive) Regulations 2009 (voorschriften van 2009 inzake gegevensbewaring in de zin van de EG-richtlijn)] en de overgang naar de gegevensbewaring op grond van deze section.

(5) De maximumduur bedoeld in lid 4, onder b), bedraagt niet meer dan 12 maanden vanaf de dag genoemd met betrekking tot de gegevens die worden beheerst door de in lid 3 bedoelde voorschriften.

[…]"

30 Section 2 van de DRIPA definieert 'relevante communicatiegegevens' als 'het type communicatiegegevens dat wordt genoemd in de bijlage bij de voorschriften van 2009 inzake gegevensbewaring in de zin van de EG-richtlijn, voor zover dergelijke gegevens in het Verenigd Koninkrijk ontstaan of worden verwerkt door openbare telecommunicatiebedrijven tijdens het aanbieden van de betrokken telecommunicatiediensten'.

RIPA

31 In lid 4 van section 21 van de wet van 2000 houdende regeling van de onderzoeksbevoegdheden (hierna: 'RIPA'), dat deel uitmaakt van hoofdstuk II, 'Verkrijging en onthulling van communicatiegegevens', van deze wet wordt gepreciseerd:

"In dit hoofdstuk wordt onder 'communicatiegegevens' een van de hieronder staande begrippen verstaan:

(a) verkeersgegevens die deel uitmaken van een communicatie of daaraan zijn toegevoegd (door de afzender of anderszins) ten behoeve van de posterijen of van een telecommunicatiesysteem waardoor deze communicatie wordt of kan worden doorgeleid;

(b) informatie die geen inhoud van een communicatie omvat [behalve informatie die onder a) valt] en betrekking heeft op het gebruik door een persoon

(i) van de posterijen of van een telecommunicatiedienst, of

(ii) in verband met het aanbieden aan of gebruik door een persoon van een telecommunicatiedienst of een onderdeel van een telecommunicatiesysteem;

(c) informatie die niet onder de punten a) of b) valt, die wordt bewaard of verkregen door een persoon die een post- of telecommunicatiedienst aanbiedt met betrekking tot personen aan wie hij de dienst aanbiedt."

32 Volgens de verwijzingsbeslissing in zaak C-698/15 omvatten deze gegevens de 'locatiegegevens van een gebruiker', maar niet de gegevens over de inhoud van een communicatie.

33 Met betrekking tot de toegang tot de bewaarde gegevens bepaalt section 22 van de RIPA:

"(1) Deze section is van toepassing wanneer een voor de toepassing van dit hoofdstuk aangewezen persoon van mening is dat het om in lid

2) genoemde redenen noodzakelijk is communicatiegegevens te verkrijgen.
(2) Het is om in dit lid genoemde redenen noodzakelijk de communicatiegegevens te verkrijgen wanneer dit nodig is:
(a) in het belang van de nationale veiligheid;
(b) om criminaliteit te voorkomen of aan het licht te brengen of om verstoring van de openbare orde te voorkomen;
(c) in het belang van het economisch welzijn van het Verenigd Koninkrijk;
(d) in het belang van de openbare veiligheid;
(e) ter bescherming van de volksgezondheid;
(f) voor het vaststellen van de grondslag of voor het innen van aan de overheid verschuldigde belastingen, accijnzen, heffingen of andere imposten, bijdragen of lasten;
(g) ter voorkoming, in een noodsituatie, van de dood, van verwondingen of van andere schade aan de lichamelijke of geestelijke gezondheid van een persoon, of ter leniging van verwondingen of schade aan de lichamelijke of geestelijke gezondheid van een persoon;
(h) voor alle andere [niet onder de punten a) tot en met g) vallende] doelen die die nader worden bepaald in een door de Secretary of State uitgevaardigd bevel.
(4) Onverminderd het bepaalde in lid 5), kan de verantwoordelijke, indien hij van mening is dat een post- of telecommunicatiebedrijf in het bezit is van gegevens, in het bezit van gegevens zou kunnen zijn of gegevens zou kunnen verkrijgen, van dit post- of telecommunicatiebedrijf eisen
(a) dat het deze gegevens verkrijgt voor zover het deze niet al bezit, en
(b) in elk geval alle in zijn bezit zijnde of later verkregen gegevens onthult.
(5) De verantwoordelijke mag geen toestemming in de zin van lid 3) geven en geen aanzegging in de zin van lid 4) doen, tenzij hij van oordeel is dat het verkrijgen van de betrokken gegevens op grond van een toegestane gedraging of van een aanzegging evenredig is met het doel dat met het verkrijgen van de gegevens wordt nagestreefd."

34 Volgens section 65 van de RIPA kan bij het Investigatory Powers Tribunal (rechter die toezicht uitoefent op de onderzoeksbevoegdheden, Verenigd Koninkrijk) een klacht worden ingediend indien er een reden is om te veronderstellen dat gegevens op onjuiste wijze zijn verkregen.

Data Retention Regulations 2014

35 De Data Retention Regulations 2014 (voorschriften inzake gegevensbewaring van 2014) zijn vastgesteld op basis van de DRIPA en bestaan uit drie delen, waarvan het tweede deel de sections 2 tot en met 14 van deze voorschriften bevat. Section 4, 'Aanzegging tot bewaring van gegevens', bepaalt:

"(1) In de aanzegging tot bewaring moet worden gepreciseerd:
(a) het openbaar telecommunicatiebedrijf waartoe zij is gericht (of de beschrijving van het bedrijf),
(b) de relevante communicatiegegevens die moeten worden bewaard,
(c) de periode of de perioden gedurende dewelke de gegevens moeten worden bewaard,
(d) alle andere eisen of beperkingen ter zake van de bewaring van de gegevens.
(2) In een aanzegging tot bewaring kan niet worden geëist dat gegevens meer dan 12 maanden worden bewaard, vanaf:
(a) in geval van verkeersgegeven of gegevens betreffende het gebruik van de dienst, de dag van de betrokken communicatie, en
(b) in geval van gegevens betreffende de abonnees, de dag waarop de betrokken persoon de betrokken communicatiedienst verlaat, of de dag waarop het gegeven is gewijzigd (indien dat op een eerdere datum is gebeurd).
[…]"

36 Section 7, 'Volledigheid en beveiliging van de gegevens', van deze voorschriften bepaalt:

"(1) Een openbaar telecommunicatiebedrijf dat op grond van section 1 van de [DRIPA] communicatiegegevens bewaart, moet:
(a) ervoor zorgen dat de gegevens even volledig en ten minste even beveiligd en beschermd zijn als de gegevens van de systemen waaruit zij afkomstig zijn,
(b) door middel van technische en organisatorische maatregelen ervoor zorgen dat alleen daartoe speciaal gemachtigde personeelsleden toegang kunnen krijgen tot de gegevens, en
(c) de gegevens, door middel van passende technische en organisatorische maatregelen, beschermen tegen onrechtmatige vernietiging, onvoorzien verlies of onvoorziene beschadiging, of niet-toegestane of ongeoorloofde bewaring, verwerking, toegang of onthulling.
(2) Een openbaar telecommunicatiebedrijf dat op grond van section 1 van de [DRIPA] communicatiegegevens bewaart, moet de gegevens vernietigen wanneer de bewaring ervan niet langer is toegestaan op grond van deze section of op grond van een andere wetsbepaling.
(3) De in lid 2) bedoelde eis van vernietiging van de gegevens betekent dat de gegevens moeten worden gewist op een wijze die de toegang tot die gegevens onmogelijk maakt.
(4) Het volstaat dat het bedrijf de nodige maatregelen neemt om de gegevens maandelijks, of met kortere tussenpozen indien dat voor het bedrijf in de praktijk mogelijk is, te wissen."

37 Section 8, 'Onthulling van de bewaarde gegevens', bepaalt:

"(1) Een openbaar telecommunicatiebedrijf moet voorzien in een passende beveiliging

(technische en organisatorische maatregelen daaronder begrepen) van de toegang tot de communicatiegegevens die op grond van section 1 van de [DRIPA] worden bewaard, teneinde elke niet onder section 1, lid 6), onder a), van de [DRIPA] vallende onthulling te voorkomen.

(2) Een openbaar telecommunicatiebedrijf dat op grond van section 1 van de [DRIPA] communicatiegegevens bewaart, moet de gegevens aldus bewaren dat zij zonder onnodige vertraging in antwoord op een aanzegging kunnen worden overgelegd."

38 Section 9, 'Toezicht door de Information Commissioner [(toezichthouder op de informatie)]', bepaalt:

"De Information Commissioner ziet toe op de inachtneming van de in dit deel geformuleerde eisen of beperkingen in verband met de volledigheid, de beveiliging en de vernietiging van de op grond van section 1 van de DRIPA bewaarde gegevens."

Gedragscode

39 De punten 2.5 tot en met 2.9 en 2.36 tot en met 2.45 van de Acquisition and Disclosure of Communications Data Code of Practice (gedragscode voor de verkrijging en de onthulling van communicatiegegevens; hierna: 'gedragscode') bevatten richtsnoeren over de noodzaak en de evenredigheid van het verkrijgen van communicatiegegevens. Volgens de door de verwijzende rechterlijke instantie in zaak C-698/15 verstrekte uitleg moet overeenkomstig de punten 3.72 tot en met 3.77 van deze gedragscode bijzondere aandacht worden besteed aan de noodzaak en de evenredigheid wanneer de gevraagde communicatiegegevens betrekking hebben op een persoon die lid is van een beroepsgroep die beschikt over informatie waarvoor het beroepsgeheim geldt of over anderszins vertrouwelijke informatie.

40 Op grond van de punten 3.78 tot en met 3.84 van die gedragscode is een rechterlijk bevel vereist in het bijzondere geval van een verzoek om communicatiegegevens dat wordt gedaan om de bron van journalisten te achterhalen. Volgens de punten 3.85 tot en met 3.87 van die gedragscode is rechterlijke goedkeuring vereist in het geval van een door lokale autoriteiten geformuleerd verzoek om toegang. Daarentegen is geen rechterlijke machtiging of machtiging door een onafhankelijke entiteit vereist voor toegang tot communicatiegegevens waarvoor een in de wet verankerd beroepsgeheim geldt, of tot communicatiegegevens met betrekking tot artsen, parlementsleden of geestelijken.

41 In punt 7.1 van de gedragscode wordt bepaald dat de communicatiegegevens die worden verworven of verkregen op grond van de bepalingen van de RIPA en alle uittreksels, samenvattingen en afschriften van deze gegevens veilig moeten worden bewaard en opgeslagen. Bovendien moeten de in de Data Protection Act (wet betreffende de bescherming van gegevens) gestelde eisen in acht worden genomen.

42 In punt 7.18 van de gedragscode staat dat wanneer een overheidsinstantie van het Verenigd Koninkrijk van plan is om communicatiegegevens aan buitenlandse instanties te onthullen, zij met name moet onderzoeken of die gegevens passend zullen worden beschermd. Uit punt 7.22 van deze gedragscode blijkt echter dat gegevens aan derde landen kunnen worden overgedragen wanneer die overdracht noodzakelijk is om redenen die verband houden met een aanzienlijk openbaar belang, zelfs ingeval het derde land geen passend niveau van bescherming garandeert. Volgens de uitleg die de verwijzende rechterlijke instantie in zaak C-698/15 dienaangaande heeft verstrekt, kan de Secretary of State een nationaal veiligheidscertificaat afgeven, op grond waarvan voor bepaalde gegevens de bepalingen van de wet niet hoeven te worden geëerbiedigd.

43 In punt 8.1 van die gedragscode wordt eraan herinnerd dat de RIPA voorziet in een Interception of Communications Commissioner (toezichthouder op de onderschepping van communicaties, Verenigd Koninkrijk), wiens rol er met name in bestaat, op onafhankelijke wijze toezicht uit te oefenen op de uitoefening en de nakoming van de in hoofdstuk II van deel I van de RIPA genoemde rechten en plichten. Uit punt 8.3 van die gedragscode blijkt dat deze toezichthouder, wanneer hij kan 'aantonen dat een persoon schade heeft geleden door een uit opzet of onvoorzichtigheid voortvloeiend verzuim', deze persoon op de hoogte mag brengen van een vermoeden van onrechtmatig gebruik van bevoegdheden.

Hoofdgedingen en prejudiciële vragen

Zaak C-203/15

44 Op 9 april 2014 heeft Tele2 Sverige, een in Zweden gevestigde aanbieder van electronischecommunicatiediensten, de PTS officieel ervan in kennis gesteld dat zij, ten vervolge op de ongeldigverklaring van richtlijn 2006/24 bij het arrest van 8 april 2014, *Digital Rights Ireland e.a.* (C-293/12 en C-594/12; hierna: 'arrest *Digital Rights*', EU:C:2014:238 (*NJ* 2016/446, m.nt. E.J. Dommering; *red.*)), per 14 april 2014 de in de LEK bedoelde elektronischecommunicatiegegevens niet meer zou bewaren en de tot dan toe bewaarde gegevens zou vernietigen.

45 Op 15 april 2014 heeft de Rikspolisstyrelse (algemeen bestuur van de nationale politie, Zweden) bij de PTS een klacht ingediend wegens het feit dat Tele2 Sverige hem de betrokken gegevens niet langer meedeelde.

46 Op 29 april 2014 heeft de justitieminister (minister van Justitie, Zweden) een bijzondere rapporteur belast met de toetsing van de Zweedse regeling aan het arrest *Digital Rights*. In een rapport van 13 juni 2014 met als opschrift 'Datalagring, EU-rätten och svensk rätt, nº Ds 2014:23' (Bewaring van

gegeven, Unierecht en Zweeds recht; hierna: 'rapport van 2014') is de bijzondere rapporteur tot de slotsom gekomen dat de nationale regeling betreffende de bewaring van gegevens, zoals die is neergelegd in de §§ 16 a tot en met 16 f van de LEK, niet in strijd met het Unierecht was en evenmin met het op 4 november 1950 te Rome ondertekende Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (hierna: 'EVRM'). De bijzondere rapporteur heeft beklemtoond dat het arrest *Digital Rights* niet in die zin kon worden uitgelegd dat het beginsel zelf van het algemeen en ongedifferentieerd bewaren van de gegevens daarin is gelaakt. Volgens hem mag het arrest *Digital Rights* ook niet in die zin worden begrepen dat het Hof daarin een aantal criteria heeft geformuleerd waaraan een regeling volledig moet voldoen om als evenredig te kunnen worden beschouwd. Om uit te maken of de Zweedse regeling in overeenstemming is met het Unierecht, zouden alle omstandigheden, zoals de omvang van de bewaring van de gegevens uit het oogpunt van de bepalingen betreffende de toegang tot de gegevens, de duur van de bewaring van de gegevens, de bescherming en de beveiliging daarvan, dienen te worden beoordeeld.

47 Op basis daarvan heeft de PTS Tele2 Sverige op 19 juni 2014 laten weten dat deze laatste de krachtens de nationale regeling op haar rustende verplichtingen niet nakwam door de in de LEK bedoelde gegevens niet gedurende zes maanden te bewaren ten behoeve van de bestrijding van de criminaliteit. Op 27 juni 2014 heeft de PTS Tele2 Sverige gelast, deze gegevens uiterlijk per 25 juli 2014 te bewaren.

48 Van oordeel dat het rapport van 2014 op een onjuiste uitlegging van het arrest *Digital Rights* berustte, en dat de verplichting tot bewaring van de gegevens in strijd was met de door het Handvest gewaarborgde grondrechten, heeft Tele2 Sverige tegen het bevel van 27 juni 2014 beroep ingesteld bij de Förvaltningsrätt i Stockholm (bestuursrechter in eerste aanleg Stockholm, Zweden). Nadat deze rechterlijke instantie het beroep bij vonnis van 13 oktober 2014 had verworpen, heeft Tele2 Sverige tegen dit vonnis hoger beroep ingesteld bij de verwijzende rechterlijke instantie.

49 Volgens de verwijzende rechterlijke instantie moet de verenigbaarheid van de Zweedse regeling met het Unierecht worden beoordeeld tegen de achtergrond van artikel 15, lid 1, van richtlijn 2002/58. Waar deze richtlijn het beginsel formuleert dat de verkeersgegevens en de locatiegegevens moeten worden gewist of anoniem moeten worden gemaakt wanneer zij niet langer nodig zijn voor de transmissie van een communicatie, voorziet artikel 15, lid 1, van deze richtlijn echter in een uitzondering op dit beginsel, aangezien het de lidstaten toestaat om, wanneer dit wordt gerechtvaardigd door een van de aldaar genoemde redenen, de verplichting tot het wissen of anoniem maken van de gegevens te beperken of te bepalen dat de gegevens moeten worden bewaard. In bepaalde situaties zou het Unierecht aldus het bewaren van de elektronischecommunicatiegegevens toestaan.

50 De verwijzende rechterlijke instantie vraagt zich niettemin af of een verplichting tot het algemeen en ongedifferentieerd bewaren van de elektronischecommunicatiegegevens, zoals die welke aan de orde is in het hoofdgeding, gelet op het arrest *Digital Rights*, verenigbaar is met artikel 15, lid 1, van richtlijn 2002/58, gelezen tegen de achtergrond van de artikelen 7 en 8 en artikel 52, lid 1, van het Handvest. Gelet op de uiteenlopende meningen van de partijen dienaangaande, zou het Hof ondubbelzinnig dienen te antwoorden op de vraag of, zoals Tele2 Sverige meent, het algemeen en ongedifferentieerd bewaren van de elektronischecommunicatiegegevens op zichzelf onverenigbaar is met de artikelen 7 en 8 en artikel 52, lid 1, van het Handvest, dan wel of, zoals uit het rapport van 2014 zou blijken, de verenigbaarheid van een dergelijke bewaring van gegevens moet worden getoetst aan de bepalingen betreffende de toegang tot de gegevens, de bescherming en beveiliging van de gegevens en de duur van de bewaring ervan.

51 In die omstandigheden heeft verwijzende rechterlijke instantie de behandeling van de zaak geschorst en het Hof de volgende prejudiciële vragen gesteld:

"1) Is een algemene verplichting tot bewaring van gegevens die van toepassing is op alle personen, alle elektronischecommunicatiemiddelen en alle verkeersgegevens, zonder dat enig onderscheid wordt gemaakt, enige beperking wordt gesteld of enige uitzondering wordt gemaakt op basis van het nagestreefde doel, de bestrijding van ernstige criminaliteit, […], verenigbaar met artikel 15, lid 1, van richtlijn 2002/58, gelet op de artikelen 7 en 8 en artikel 52, lid 1, van het Handvest?

2) Indien de eerste vraag ontkennend wordt beantwoord, kan een dergelijke bewaringsverplichting dan niettemin zijn toegestaan:

a) indien de toegang van de nationale autoriteiten tot de bewaarde gegevens is geregeld op de wijze als beschreven in de punten 19-36 [van de verwijzingsbeslissing], en

b) indien de vereisten van bescherming en beveiliging van de gegevens zijn geregeld op de wijze als beschreven in de punten 38-43 [van de verwijzingsbeslissing], en

c) indien alle betrokken gegevens moeten worden bewaard gedurende zes maanden te rekenen vanaf de dag waarop de communicatie werd beëindigd alvorens te worden gewist, zoals is uiteengezet in punt 37 [van de verwijzingsbeslissing]?"

Zaak C-698/15

52 Watson, Brice en Lewis hebben, ieder afzonderlijk, bij de High Court of Justice of England and Wales, Queens' Bench Division (Divisional Court) (rechter in eerste aanleg in bestuurszaken, Engeland en Wales, Verenigd Koninkrijk), beroep

in rechte ingesteld dat ertoe strekte de wettigheid van section 1 van de DRIPA te toetsen, en hebben in dat verband met name aangevoerd dat deze section onverenigbaar was met de artikelen 7 en 8 van het Handvest en met artikel 8 van het EVRM.

53 Bij arrest van 17 juli 2015 heeft de High Court of Justice of England and Wales, Queens' Bench Division (Divisional Court), vastgesteld dat in het arrest *Digital Rights* melding werd gemaakt van 'dwingende vereisten van Unierecht' die gelden voor de regelingen van de lidstaten op het gebied van bewaring van communicatiegegevens en van toegang tot dergelijke gegevens. Aangezien het Hof in dat arrest heeft geoordeeld dat richtlijn 2006/24 onverenigbaar was met het evenredigheidsbeginsel, zou volgens deze rechtspraak een nationale regeling met dezelfde inhoud als deze richtlijn evenmin met dit beginsel verenigbaar kunnen zijn. Volgens de aan het arrest *Digital Rights* ten grondslag liggende logica zou een wettelijke regeling waarbij een stelsel van algemene bewaring van communicatiegegevens wordt ingevoerd, de door de artikelen 7 en 8 van het Handvest gewaarborgde rechten schenden, tenzij deze wettelijke regeling wordt aangevuld door een in het nationale recht opgezet stelsel van toegang tot de gegevens dat voldoende waarborgen biedt voor de bescherming van die rechten. Zo zou section 1 van de DRIPA niet verenigbaar zijn met de artikelen 7 en 8 van het Handvest voor zover het geen duidelijke en nauwkeurige regels bevat voor de toegang tot en het gebruik van de bewaarde gegevens of de toegang tot deze gegevens niet afhankelijk stelt van een voorafgaand toezicht door een rechterlijke instantie of door een onafhankelijke bestuurlijke entiteit.

54 De Secretary of State heeft tegen dit arrest hoger beroep ingesteld bij de Court of Appeal (England and Wales) (Civil Division) (rechter in tweede aanleg in burgerlijke zaken, Engeland en Wales, Verenigd Koninkrijk).

55 Deze rechterlijke instantie wijst erop dat section 1, lid 1, van de DRIPA de Secretary of State machtigt om, zonder voorafgaande toestemming van een rechterlijke instantie of van een onafhankelijke bestuurlijke entiteit, een algemene regeling vast te stellen die de openbare telecommunicatiebedrijven de verplichting oplegt om alle gegevens betreffende elke post- of telecommunicatiedienst maximaal twaalf maanden te bewaren, wanneer hij van mening is dat een dergelijke eis noodzakelijk en evenredig is voor het bereiken van de in de regeling van het Verenigd Koninkrijk genoemde doelstellingen. Ook al omvatten deze gegevens niet de inhoud van een communicatie, daarmee zou bijzonder ernstig worden binnengedrongen in de persoonlijke levenssfeer van de gebruikers van communicatiediensten.

56 In de verwijzingsbeslissing en in haar op het hoger beroep gewezen arrest van 20 november 2015 waarin zij heeft beslist het onderhavige verzoek om een prejudiciële beslissing aan het Hof voor te leggen, heeft de verwijzende rechterlijke instantie geoordeeld dat de nationale regels betreffende het bewaren van de gegevens zeker onder artikel 15, lid 1, van richtlijn 2002/58 vallen en dus moeten voldoen aan de eisen van het Handvest. Volgens artikel 1, lid 3, van deze richtlijn zou de Uniewetgever de regels betreffende de toegang tot de bewaarde gegevens echter niet hebben geharmoniseerd.

57 Wat de invloed van het arrest *Digital Rights* op de in het hoofdgeding gerezen vragen betreft, wijst de verwijzende rechterlijke instantie erop dat het Hof in de zaak die tot dit arrest heeft geleid, uitspraak diende te doen over de geldigheid van richtlijn 2006/24 en niet over de geldigheid van een nationale regeling. Met name gelet op het nauwe verband tussen de bewaring van de gegevens en de toegang tot deze gegevens, zou het absoluut noodzakelijk zijn geweest dat deze richtlijn gepaard ging met een aantal garanties, en dat in het arrest *Digital Rights*, bij het onderzoek van de wettigheid van het bij deze richtlijn ingevoerde stelsel van bewaring van gegevens, de regels betreffende de toegang tot die gegevens werden geanalyseerd. Het Hof zou dus niet van plan zijn geweest om in dat arrest dwingende eisen te formuleren voor de nationale regelingen betreffende de toegang tot de gegevens die geen Unierecht ten uitvoer brengen. Bovendien zou de redenering van het Hof nauw verband houden met het door deze richtlijn nagestreefde doel. Een nationale regeling zou echter moeten worden beoordeeld tegen de achtergrond van de doelstellingen en de context ervan.

58 Met betrekking tot de noodzaak om het Hof een verzoek om een prejudiciële beslissing voor te leggen, wijst de verwijzende rechterlijke instantie met name op het feit dat op de datum van de verwijzingsbeslissing zes rechterlijke instanties van andere lidstaten, waaronder vijf rechterlijke instanties in laatste aanleg, nationale wettelijke regelingen nietig hadden verklaard op basis van het arrest *Digital Rights*. Het antwoord op de gestelde vragen zou dus niet zonder meer duidelijk zijn en zou noodzakelijk zijn voor de afdoening van de bij deze rechterlijke instantie aanhangige zaken.

59 In die omstandigheden heeft de Court of Appeal (England and Wales) (Civil Division) de behandeling van de zaak geschorst en het Hof de volgende prejudiciële vragen gesteld:

> "1) Legt het arrest *Digital Rights* (waaronder met name de punten 60 tot en met 62 ervan) dwingende vereisten van Unierecht op die van toepassing zijn op de nationale regeling van een lidstaat inzake de toegang tot gegevens die overeenkomstig de nationale wettelijke regeling worden bewaard, teneinde te voldoen aan de artikelen 7 en 8 van het Handvest?
>
> 2) Verruimt het arrest *Digital Rights* de werkingssfeer van de artikelen 7 en/of 8 van het Handvest ten opzichte van die van artikel 8 van het EVRM, zoals vastgelegd in de rechtspraak van het Europees Hof voor de Rechten van de Mens?"

Procedure bij het Hof

60 Bij beschikking van 1 februari 2016, *Davis e.a.* (C-698/15, niet gepubliceerd, EU:C:2016:70), heeft de president van het Hof het verzoek van de Court of Appeal (England and Wales) (Civil Division) om zaak C-698/15 te behandelen volgens de versnelde procedure van artikel 105, lid 1, van het Reglement voor de procesvoering van het Hof toegewezen.

61 Bij beslissing van de president van het Hof van 10 maart 2016 zijn de zaken C-203/15 en C-698/15 gevoegd voor de mondelinge behandeling en het arrest.

Beantwoording van de prejudiciële vragen

Eerste vraag in zaak C-203/15

62 Met de eerste vraag in zaak C-203/15 wenst de Kammarrätt i Stockholm in wezen te vernemen of artikel 15, lid 1, van richtlijn 2002/58, gelezen tegen de achtergrond van de artikelen 7 en 8 en artikel 52, lid 1, van het Handvest, in die zin moet worden uitgelegd dat het zich verzet tegen een nationale regeling als aan de orde in het hoofdgeding die, ter bestrijding van criminaliteit, voorziet in algemene en ongedifferentieerde bewaring van alle verkeersgegevens en locatiegegevens van alle abonnees en geregistreerde gebruikers betreffende alle elektronischecommunicatiemiddelen.

63 Deze vraag vindt haar oorsprong met name in het feit dat richtlijn 2006/24, welke de in het hoofdgeding aan de orde zijnde nationale regeling in nationaal recht beoogde om te zetten, bij het arrest *Digital Rights* ongeldig is verklaard, maar dat de partijen van mening verschillen over de draagwijdte van dit arrest en over de invloed ervan op die regeling, die de bewaring van de verkeersgegevens en van de locatiegegevens en de toegang van de nationale autoriteiten tot die gegevens regelt.

64 Vooraf dient te worden onderzocht of een nationale regeling als aan de orde in het hoofdgeding binnen de werkingssfeer van het Unierecht valt.

Werkingssfeer van richtlijn 2002/58

65 De lidstaten die schriftelijke opmerkingen bij het Hof hebben ingediend, hebben uiteenlopende opvattingen geformuleerd over het antwoord op de vraag of, en in hoeverre ter bestrijding van criminaliteit vastgestelde nationale regelingen betreffende de bewaring van de verkeersgegevens en van de locatiegegevens en betreffende de toegang van de nationale autoriteiten tot die gegevens binnen de werkingssfeer van richtlijn 2002/58 vallen. Terwijl met name de Belgische, de Deense, de Duitse en de Estse regering, Ierland en de Nederlandse regering zich op het standpunt hebben gesteld dat die vraag bevestigend dient te worden beantwoord, heeft de Tsjechische regering voorgesteld, die vraag ontkennend te beantwoorden, en erop gewezen dat deze regelingen uitsluitend tot doel hebben criminaliteit te bestrijden. De regering van het Verenigd Koninkrijk heeft aangevoerd dat alleen de regelingen betreffende de bewaring van de gegevens en niet de regelingen betreffende de toegang van de nationale rechtshandhavingsautoriteiten tot die gegevens binnen de werkingssfeer van deze richtlijn vallen.

66 Ten slotte heeft de Commissie in haar bij het Hof ingediende schriftelijke opmerkingen in zaak C-203/15 weliswaar betoogd dat de in het hoofdgeding aan de orde zijnde nationale regeling binnen de werkingssfeer van richtlijn 2002/58 valt, maar heeft zij in haar ingediende schriftelijke opmerkingen in zaak C-698/15 gesteld dat alleen de nationale regels betreffende de bewaring van de gegevens en niet die betreffende de toegang van de nationale autoriteiten tot die gegevens binnen de werkingssfeer van deze richtlijn vallen. Laatstgenoemde regels zouden volgens haar echter in aanmerking moeten worden genomen om te beoordelen of een nationale regeling betreffende de bewaring van gegevens door de aanbieders van elektronischecommunicatiediensten een evenredige ingreep in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten vormt.

67 In dit verband dient erop te worden gewezen dat bij de beoordeling van de omvang van de werkingssfeer van richtlijn 2002/58 met name rekening moet worden gehouden met de algemene opzet van deze richtlijn.

68 Volgens artikel 1, lid 1, van richtlijn 2002/58 voorziet deze richtlijn met name in de harmonisatie van de nationale regelgeving die nodig is om een gelijk niveau van bescherming van fundamentele rechten en vrijheden — met name het recht op een persoonlijke levenssfeer en vertrouwelijkheid — bij de verwerking van persoonsgegevens in de sector elektronische communicatie te waarborgen.

69 Volgens artikel 1, lid 3, van deze richtlijn zijn van de werkingssfeer van deze richtlijn uitgesloten de 'activiteiten van de staat' op de aldaar bedoelde gebieden, te weten met name de activiteiten van de staat op strafrechtelijk gebied en die welke verband houden met openbare veiligheid, defensie en staatsveiligheid, met inbegrip van het economische welzijn van de staat wanneer de activiteit verband houdt met de staatsveiligheid (zie naar analogie, met betrekking tot artikel 3, lid 2, eerste streepje, van richtlijn 95/46, arresten van 6 november 2003, *Lindqvist*, C-101/01, EU:C:2003:596, punt 43 (*NJ* 2004/248; *red.*), en 16 december 2008, *Satakunnan Markkinapörssi en Satamedia*, C-73/07, EU:C:2008:727, punt 41 (*NJ* 2009/193, m.nt. M.R. Mok; *red.*)).

70 In artikel 3 van richtlijn 2002/58 staat dat deze richtlijn van toepassing is op de verwerking van persoonsgegevens in verband met de levering van openbare elektronischecommunicatiediensten over openbare communicatienetwerken in de Unie, met inbegrip van de openbare communicatienetwerken die systemen voor gegevensverzameling en identificatie ondersteunen (hierna: 'elektronischecommunicatiediensten'). Bijgevolg moet worden

geoordeeld dat deze richtlijn de activiteiten van de aanbieders van dergelijke diensten regelt.

71 Artikel 15, lid 1, van richtlijn 2002/58 staat de lidstaten toe om, met inachtneming van de aldaar geformuleerde voorwaarden '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'. In artikel 15, lid 1, tweede zin, van die richtlijn worden als voorbeeld van maatregelen die de lidstaten aldus kunnen treffen, genoemd de maatregelen 'om gegevens […] te bewaren'.

72 De in artikel 15, lid 1, van richtlijn 2002/58 bedoelde wettelijke maatregelen betreffen specifieke activiteiten van de staten of van de overheidsdiensten en hebben niets van doen met de gebieden waarop particulieren activiteiten ontplooien (zie in die zin arrest van 29 januari 2008, *Promusicae*, C-275/06, EU:C:2008:54, punt 51 (*NJ* 2009/551, m.nt. P.B. Hugenholtz; *red.*)). Bovendien blijken de doelstellingen die dergelijke maatregelen volgens die bepaling moeten nastreven, in het onderhavige geval het waarborgen van de nationale veiligheid, de landsverdediging en de openbare veiligheid en het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronischecommunicatiesysteem, grotendeels overeen te stemmen met de doelstellingen van de in artikel 1, lid 3, van die richtlijn bedoelde activiteiten.

73 Gelet op de algemene opzet van richtlijn 2002/58, kan uit de in het voorgaande punt van het onderhavige arrest genoemde elementen echter niet worden afgeleid dat de in artikel 15, lid 1, van richtlijn 2002/58 bedoelde wettelijke maatregelen van de werkingssfeer van deze richtlijn zijn uitgesloten, omdat daardoor aan deze bepaling elk nuttig effect zou worden ontnomen. Deze bepaling vooronderstelt immers noodzakelijkerwijze dat de aldaar bedoelde nationale maatregelen, zoals die betreffende de bewaring van gegevens ter bestrijding van criminaliteit, binnen de werkingssfeer van die richtlijn vallen, omdat in deze laatste uitdrukkelijk wordt bepaald dat de lidstaten die maatregelen slechts mogen treffen met inachtneming van de aldaar geformuleerde voorwaarden.

74 Bovendien regelen de in artikel 15, lid 1, van richtlijn 2002/58 bedoelde wettelijke maatregelen de activiteit van de aanbieders van elektronischecommunicatiediensten voor de in die bepaling vermelde doeleinden. Artikel 15, lid 1, gelezen in samenhang met artikel 3 van die richtlijn, moet dus in die zin worden uitgelegd dat dergelijke wettelijke maatregelen binnen de werkingssfeer van die richtlijn vallen.

75 In het bijzonder een wettelijke maatregel als aan de orde in het hoofdgeding, die aan deze aanbieders de verplichting oplegt om de verkeersgegevens en de locatiegegevens te bewaren, valt dus binnen de werkingssfeer van deze richtlijn, omdat een dergelijke activiteit noodzakelijkerwijze inhoudt dat de aanbieders persoonsgegevens verwerken.

76 Binnen de werkingssfeer van de richtlijn valt ook een wettelijke maatregel als aan de orde in het hoofdgeding die betrekking heeft op de toegang van de nationale autoriteiten tot de door de aanbieders van elektronischecommunicatiediensten bewaarde gegevens.

77 De in artikel 5, lid 1, van richtlijn 2002/58 gewaarborgde bescherming van het vertrouwelijke karakter van de communicatie en van de daarmee verband houdende verkeersgegevens, geldt immers voor de door alle andere personen dan de gebruikers getroffen maatregelen, ongeacht of het daarbij gaat om particuliere personen of entiteiten dan wel om overheidsentiteiten. Zoals in overweging 21 van die richtlijn wordt gezegd, beoogt deze richtlijn 'elke' onbevoegde 'toegang' tot de communicatie, daaronder begrepen de toegang tot de 'gegevens over die communicatie', te verhinderen teneinde het vertrouwelijke karakter van de elektronische communicaties te beschermen.

78 In die omstandigheden heeft een wettelijke maatregel waarbij een lidstaat op grond van artikel 15, lid 1, van richtlijn 2002/58, ter verwezenlijking van de in die bepaling vermelde doelstellingen, aan de aanbieders van elektronischecommunicatiediensten de verplichting oplegt om de nationale autoriteiten onder de in een dergelijke maatregel genoemde voorwaarden toegang te verlenen tot de door die aanbieders bewaarde gegevens, betrekking op de verwerking van persoonsgegevens door die aanbieders, en deze verwerking valt binnen de werkingssfeer van die richtlijn.

79 Aangezien de bewaring van gegevens uitsluitend gebeurt om de bevoegde nationale autoriteiten in voorkomend geval toegang te kunnen geven tot die gegevens, impliceert een nationale regeling die voorziet in de bewaring van gegevens bovendien in beginsel noodzakelijkerwijs bepalingen betreffende de toegang van de bevoegde nationale autoriteiten tot de door de aanbieders van elektronischecommunicatiediensten bewaarde gegevens.

80 Deze uitlegging vindt steun in artikel 15, lid 1 ter, van richtlijn 2002/58, volgens hetwelk de aanbieders op de grondslag van nationale bepalingen die overeenkomstig artikel 15, lid 1, van deze richtlijn zijn aangenomen, interne procedures opzetten voor de afhandeling van verzoeken om toegang tot de persoonsgegevens van de gebruikers.

81 Uit een en ander volgt dat een nationale regeling als aan de orde in het hoofdgeding in de zaken C-203/15 en C-698/15 binnen de werkingssfeer van richtlijn 2002/58 valt.

Uitlegging van artikel 15, lid 1, van richtlijn 2002/58 tegen de achtergrond van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest

82 Opgemerkt dient te worden dat, volgens artikel 1, lid 2, van richtlijn 2002/58 de bepalingen van deze richtlijn 'een specificatie van en een

aanvulling op' richtlijn 95/46 vormen. Zoals in overweging 2 van richtlijn 2002/58 wordt gezegd, beoogt deze richtlijn in het bijzonder de volledige eerbiediging van de in de artikelen 7 en 8 van het Handvest bedoelde rechten te waarborgen. Dienaangaande blijkt uit de memorie van toelichting bij het voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie [COM(2000) 385 definitief], waaruit richtlijn 2002/58 is voortgekomen, dat de Uniewetgever heeft willen 'zorgen voor een hoge mate van bescherming van de persoonsgegevens en van de persoonlijke levenssfeer voor alle elektronischecommunicatiediensten, ongeacht de gebruikte technologie'.

83 Daartoe bevat richtlijn 2002/58 specifieke bepalingen die, zoals met name uit de overwegingen 6 en 7 van deze richtlijn blijkt, de gebruikers van elektronischecommunicatiediensten beogen te beschermen tegen de gevaren die de nieuwe technologieën en de steeds grotere mogelijkheden van geautomatiseerde opslag en verwerking van gegevens voor de persoonsgegevens en de persoonlijke levenssfeer van die gebruikers meebrengen.

84 Artikel 5, lid 1, van deze richtlijn bepaalt met name dat de lidstaten via nationale wetgeving het vertrouwelijke karakter van de communicatie via openbare communicatienetwerken en via openbare elektronischecommunicatiediensten en van de daarmee verband houdende verkeersgegevens moeten garanderen.

85 Het bij richtlijn 2002/58 ingevoerde beginsel van vertrouwelijkheid van de communicatie impliceert onder meer, zoals uit artikel 5, lid 1, tweede zin, van deze richtlijn blijkt, een in beginsel voor alle andere personen dan de gebruikers geldend verbod op het zonder toestemming van de gebruikers opslaan van de verkeersgegevens betreffende de elektronische communicatie. Deze bepaling maakt slechts een uitzondering voor de personen die overeenkomstig artikel 15, lid 1, van deze richtlijn de wettelijke toelating hebben gekregen, en voor de technische opslag die nodig is voor het overbrengen van informatie (zie in die zin arrest van 29 januari 2008, *Promusicae*, C-275/06, EU:C:2008:54, punt 47).

86 Zoals ook uit de overwegingen 22 en 26 van richtlijn 2002/58 blijkt, is de verwerking en de opslag van de verkeersgegevens volgens artikel 6 van deze richtlijn slechts toegestaan voor zover en zolang dat nodig is voor de facturering van de diensten, voor de marketing van die diensten en voor de levering van diensten met toegevoegde waarde (zie in die zin arrest van 29 januari 2008, *Promusicae*, C-275/06, EU:C:2008:54, punten 47 en 48). Wat in het bijzonder de facturering van de diensten betreft, is een dergelijke verwerking slechts toegestaan tot aan het einde van de periode waarbinnen de rekening volgens de wet kan worden aangevochten of de betaling kan worden afgedwongen. Zodra die periode is verstreken, moeten de verwerkte en opgeslagen gegevens worden gewist of anoniem worden gemaakt. Wat de andere locatiegegevens dan de verkeersgegevens betreft, bepaalt artikel 9, lid 1, van deze richtlijn dat die gegevens slechts onder bepaalde voorwaarden mogen worden verwerkt nadat zij anoniem zijn gemaakt of wanneer de gebruikers of abonnees daarvoor hun toestemming hebben gegeven.

87 De draagwijdte van de bepalingen van de artikelen 5 en 6 en artikel 9, lid 1, van richtlijn 2002/58, die de vertrouwelijkheid van de communicaties en van de daarmee verband houdende gegevens beogen te waarborgen en het gevaar van misbruik zo laag mogelijk beogen te houden, moet bovendien worden beoordeeld tegen de achtergrond van overweging 30 van deze richtlijn, volgens welke '[s]ystemen voor elektronischecommunicatienetwerken en -diensten […] op dusdanige wijze [moeten] worden ontworpen dat het aantal persoonsgegevens tot het strikt noodzakelijke minimum wordt beperkt'.

88 Artikel 15, lid 1, van richtlijn 2002/58 staat de lidstaten weliswaar toe, te voorzien in uitzonderingen op de in artikel 5, lid 1, van deze richtlijn geformuleerde principeverplichting om de vertrouwelijkheid van de persoonsgegevens te waarborgen, en op de in de artikelen 6 en 9 van die richtlijn vermelde overeenkomstige verplichtingen (zie in die zin arrest van 29 januari 2008, *Promusicae*, C-275/06, EU:C:2008:54, punt 50).

89 Omdat artikel 15, lid 1, van richtlijn 2002/58 de lidstaten toestaat, de draagwijdte van de principeverplichting tot waarborging van de vertrouwelijkheid van de communicatie en van de daarmee verband houdende gegevens te beperken, moet het volgens vaste rechtspraak van het Hof echter strikt worden uitgelegd (zie naar analogie arrest van 22 november 2012, *Probst*, C-119/12, EU:C:2012:748, punt 23). Een dergelijke bepaling kan dus niet rechtvaardigen dat de in artikel 5 van deze richtlijn bepaalde uitzondering op deze principeverplichting en, in het bijzonder, op het verbod om deze gegevens op te slaan de regel wordt, omdat laatstgenoemde bepaling in dat geval grotendeels haar inhoud zou verliezen.

90 In dit verband dient erop te worden gewezen dat artikel 15, lid 1, eerste zin, van richtlijn 2002/58 bepaalt dat de aldaar bedoelde wettelijke maatregelen die afwijken van het beginsel van vertrouwelijkheid van de communicaties en van de daarmee verband houdende verkeersgegevens, tot doel moeten hebben de 'waarborging van de nationale [veiligheid], d.w.z. de staatsveiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronischecommunicatiesysteem', of een van de andere doelen genoemd in artikel 13, lid 1, van richtlijn 95/46, waarnaar artikel 15, lid 1, eerste zin, van richtlijn 2002/58 verwijst (zie in die zin arrest van 29 januari 2008, *Promusicae*, C-275/06,

EU:C:2008:54, punt 53). Een dergelijke opsomming van doelstellingen is exhaustief, zoals blijkt uit artikel 15, lid 1, tweede zin, van deze richtlijn, volgens welke de wettelijke maatregelen moeten worden gerechtvaardigd door 'de redenen' die in artikel 15, lid 1, eerste zin, van die richtlijn 'worden genoemd'. Bijgevolg mogen de lidstaten dergelijke maatregelen niet treffen voor andere doeleinden dan die welke in laatstgenoemde bepaling worden genoemd.

91 Bovendien wordt in artikel 15, lid 1, derde zin, van richtlijn 2002/58 bepaald dat '[a]lle in dit [artikel 15, lid 1,] bedoelde maatregelen in overeenstemming [dienen] te zijn met de algemene beginselen van het [Unierecht], met inbegrip van de beginselen als bedoeld in artikel 6, leden 1 en 2, [EU]', waaronder de algemene beginselen en de grondrechten die thans worden gewaarborgd door het Handvest. Artikel 15, lid 1, van richtlijn 2002/58 moet aldus tegen de achtergrond van de door het Handvest gewaarborgde grondrechten worden uitgelegd (zie naar analogie, met betrekking tot richtlijn 95/46, arresten van 20 mei 2003, *Österreichischer Rundfunk e.a.*, C-465/00, C-138/01 en C-139/01, EU:C:2003:294, punt 68 (*NJ* 2005/15; *red.*) ; 13 mei 2014, *Google Spain en Google*, C-131/12, EU:C:2014:317, punt 68 (*NJ* 2014/385, m.nt. M.R. Mok; *red.*), en 6 oktober 2015, *Schrems*, C-362/14, EU:C:2015:650, punt 38 (*NJ* 2016/447, m.nt. E.J. Dommering; *red.*)).

92 In dit verband dient te worden beklemtoond dat de bij een nationale regeling als aan de orde in het hoofdgeding aan de aanbieders van elektronischecommunicatiediensten opgelegde verplichting om de verkeersgegevens te bewaren teneinde de bevoegde nationale autoriteiten in voorkomend geval toegang tot die gegevens te kunnen geven, niet alleen vragen doet rijzen betreffende de eerbiediging van de artikelen 7 en 8 van het Handvest, die in de prejudiciële vragen uitdrukkelijk worden genoemd, maar ook betreffende de eerbiediging van de door artikel 11 van het Handvest gewaarborgde vrijheid van meningsuiting (zie naar analogie, met betrekking tot richtlijn 2006/24, arrest *Digital Rights*, punten 25 en 70).

93 Aldus moet zowel het belang van het door artikel 7 van het Handvest gewaarborgde recht op bescherming van het privéleven als dat van het door artikel 8 van het Handvest gewaarborgde recht op bescherming van de persoonsgegevens, zoals dat blijkt uit de rechtspraak van het Hof (zie in die zin arrest van 6 oktober 2015, *Schrems*, C-362/14, EU:C:2015:650, punt 39 en aldaar aangehaalde rechtspraak), in aanmerking worden genomen bij de uitlegging van artikel 15, lid 1, van richtlijn 2002/58. Hetzelfde geldt voor het recht op vrijheid van meningsuiting, gelet op het belang van deze vrijheid in een democratische samenleving. Dit in artikel 11 van het Handvest gewaarborgde grondrecht is een van de wezenlijke grondslagen van een democratische en pluralistische samenleving, die behoort tot de waarden waarop de Unie overeenkomstig artikel 2 VEU is gebaseerd (zie in die zin arresten van 12 juni 2003, *Schmidberger*, C-112/00, EU:C:2003:333, punt 79 (*NJ* 2004/56; *red.*), en 6 september 2011, *Patriciello*, C-163/10, EU:C:2011:543, punt 31).

94 In dit verband dient eraan te worden herinnerd dat volgens artikel 52, lid 1, van het Handvest beperkingen op de uitoefening van daarin erkende rechten en vrijheden bij wet moeten worden gesteld en de wezenlijke inhoud daarvan moeten eerbiedigen. Met inachtneming van het evenredigheidsbeginsel kunnen slechts beperkingen op de uitoefening van die rechten en vrijheden worden gesteld indien deze noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen (arrest van 15 februari 2016, *N.*, C-601/15 PPU, EU:C:2016:84, punt 50).

95 Wat dit laatste betreft, wordt in artikel 15, lid 1, eerste zin, van richtlijn 2002/58 bepaald dat de lidstaten een maatregel waarbij wordt afgeweken van het beginsel van vertrouwelijkheid van de communicatie en van de daarmee verband houdende verkeersgegevens, kunnen treffen wanneer een dergelijke maatregel 'in een democratische samenleving noodzakelijk, redelijk en proportioneel is' in het licht van de in die bepalingen genoemde doelstellingen. In overweging 11 van deze richtlijn wordt gepreciseerd dat een dergelijke maatregel 'strikt' evenredig moet zijn met het nagestreefde doel. Wat in het bijzonder de bewaring van gegevens betreft, eist artikel 15, lid 1, tweede zin, van deze richtlijn dat deze gegevens slechts 'gedurende een beperkte periode' worden bewaard 'om de redenen' die in artikel 15, lid 1, eerste zin, van die richtlijn worden genoemd.

96 De eerbiediging van het evenredigheidsbeginsel vloeit ook voort uit de vaste rechtspraak van het Hof volgens welke 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 (arresten van 16 december 2008, *Satakunnan Markkinapörssi en Satamedia*, C-73/07, EU:C:2008:727, punt 56 en 9 november 2010, *Volker und Markus Schecke en Eifert*, C-92/09 en C-93/09, EU:C:2010:662, punt 77 (*NJ* 2011/68; *red.*); arrest *Digital Rights*, punt 52, en arrest van 6 oktober 2015, *Schrems*, C-362/14, EU:C:2015:650, punt 92).

97 Met betrekking tot de vraag of een regeling als aan de orde in zaak C-203/15 aan deze voorwaarden voldoet, dient erop te worden gewezen dat deze regeling voorziet in algemene en ongedifferentieerde bewaring van alle verkeersgegevens en locatiegegevens van alle abonnees en geregistreerde gebruikers betreffende alle elektronischecommunicatiemiddelen, en de aanbieders van elektronischecommunicatiediensten verplicht deze gegevens stelselmatig en voortdurend te bewaren zonder enige uitzondering. Zoals uit de verwijzingsbeslissing blijkt, komen de categorieën van gegevens waarop

deze regeling ziet, grotendeels overeen met die waarvan richtlijn 2006/24 de bewaring voorschrijft.

98 Aan de hand van de gegevens die de aanbieders van elektronischecommunicatiediensten aldus moeten bewaren, kunnen de bron en de bestemming van een communicatie worden opgespoord en geïdentificeerd en kunnen de datum, het tijdstip, de duur en de aard van de communicatie, de communicatieapparatuur van de gebruikers en de locatie van de mobiele communicatieapparatuur worden bepaald. Die gegevens omvatten onder meer 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. Aan de hand van deze gegevens 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 (zie naar analogie, met betrekking tot richtlijn 2006/24, arrest *Digital Rights*, punt 26).

99 Uit deze gegevens, in hun geheel beschouwd, kunnen zeer precieze conclusies worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren (zie naar analogie, met betrekking tot richtlijn 2006/24, arrest *Digital Rights*, punt 27). Zoals de advocaat-generaal in de punten 253, 254 en 257 tot en met 259 heeft opgemerkt, kan aan de hand van deze gegevens 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.

100 De ingreep die een dergelijke regeling in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten verricht, is groot en moet als bijzonder ernstig worden beschouwd. De omstandigheid dat de gegevens worden bewaard zonder dat de gebruikers van de elektronischecommunicatiediensten hierover worden ingelicht, kan bij de betrokken personen het gevoel opwekken dat hun privéleven constant in de gaten wordt gehouden (zie naar analogie, met betrekking tot richtlijn 2006/24, arrest *Digital Rights*, punt 37).

101 Ook al staat een dergelijke regeling niet toe om de inhoud van een communicatie te bewaren, en maakt zij dus geen inbreuk op de wezenlijke inhoud van die rechten (zie naar analogie, met betrekking tot richtlijn 2006/24, arrest *Digital Rights*, punt 39), toch kan de bewaring van de verkeersgegevens en van de locatiegegevens invloed hebben op het gebruik van de elektronischecommunicatiemiddelen en dus op de wijze waarop de gebruikers van deze communicatiemiddelen van hun in artikel 11 van het Handvest gewaarborgde vrijheid van meningsuiting gebruikmaken (zie naar analogie, met betrekking tot richtlijn 2006/24, arrest *Digital Rights*, punt 28).

102 Gelet op de ernst van de ingreep in de betrokken grondrechten door een nationale regeling die ter bestrijding van criminaliteit voorziet in de bewaring van verkeersgegevens en van locatiegegevens, kan alleen de bestrijding van ernstige criminaliteit een dergelijke maatregel rechtvaardigen (zie naar analogie, met betrekking tot richtlijn 2006/24, arrest *Digital Rights*, punt 60).

103 Daarbij komt dat de doeltreffendheid van de bestrijding van zware criminaliteit, met name van georganiseerde misdaad en terrorisme, weliswaar in aanzienlijke mate kan afhangen van het gebruik van moderne onderzoekstechnieken, maar dat een dergelijke doelstelling van algemeen belang, hoe wezenlijk zij ook is, op zich niet kan rechtvaardigen dat een nationale regeling die voorziet in algemene en ongedifferentieerde bewaring van alle verkeersgegevens en alle locatiegegevens, noodzakelijk wordt geacht voor het voeren van deze strijd (zie naar analogie, met betrekking tot richtlijn 2006/24, arrest *Digital Rights*, punt 51).

104 In dit verband dient enerzijds erop te worden gewezen dat een dergelijke regeling, gelet op de in punt 97 van het onderhavige arrest beschreven kenmerken ervan, tot gevolg heeft dat de bewaring van de verkeersgegevens en van de locatiegegevens de regel is, terwijl het bij richtlijn 2002/58 ingevoerde stelsel eist dat deze bewaring van gegevens de uitzondering vormt.

105 Anderzijds voorziet een nationale regeling als aan de orde in het hoofdgeding, die algemeen geldt voor alle abonnees en geregistreerde gebruikers en ziet op alle elektronischecommunicatiemiddelen en op alle verkeersgegevens, in geen enkele differentiatie, beperking of uitzondering naargelang van het nagestreefde doel. Zij heeft 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. Zij is dus zelfs van toepassing op personen voor wie er geen enkele aanwijzing bestaat dat hun gedrag — zelfs maar indirect of van ver — verband houdt met ernstige strafbare feiten. Bovendien bevat zij geen uitzonderingen, zodat zij zelfs van toepassing is op personen van wie de communicaties naar nationaal recht onder het beroepsgeheim vallen (zie naar analogie, met betrekking tot richtlijn 2006/24, arrest *Digital Rights*, punten 57 en 58).

106 Een dergelijke regeling eist geen enkel verband tussen de gegevens die moeten worden bewaard en een bedreiging van de openbare veiligheid. Zij beperkt de bewaring met name 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 (zie naar analogie, met betrekking tot richtlijn 2006/24, arrest *Digital Rights*, punt 59).

107 Een nationale regeling als aan de orde in het hoofdgeding gaat dus verder dan strikt noodzakelijk is, en kan niet worden beschouwd als een regeling die in een democratische samenleving gerechtvaardigd is, zoals artikel 15, lid 1, van richtlijn 2002/58, gelezen tegen de achtergrond van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, eist.

108 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, staat daarentegen niet eraan in de weg dat een lidstaat een regeling vaststelt op grond waarvan de verkeersgegevens en de locatiegegevens ter bestrijding van zware criminaliteit preventief gericht kunnen worden bewaard, op voorwaarde dat de bewaring van die gegevens, hetzij wat de categorieën van te bewaren gegevens betreft, hetzij wat de betrokken communicatiemiddelen, personen en duur van de bewaring betreft, tot het strikt noodzakelijke wordt beperkt.

109 Om aan de in het vorige punt van het onderhavige arrest genoemde eisen te voldoen, moet deze nationale regeling in de eerste plaats duidelijke en nauwkeurige regels voor de draagwijdte en de toepassing van een dergelijke maatregel van bewaring van gegevens bevatten en een minimum aan eisen stellen, zodat de personen wier gegevens zijn bewaard, voldoende garanties hebben dat hun persoonsgegevens doeltreffend worden beschermd tegen het risico van misbruik. 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 (zie naar analogie, met betrekking tot richtlijn 2006/24, arrest *Digital Rights*, punt 54 en aldaar aangehaalde rechtspraak).

110 In de tweede plaats dient — wat de materiële voorwaarden betreft waaraan een nationale regeling op grond waarvan de verkeersgegevens en de locatiegegevens preventief kunnen worden bewaard ter bestrijding van criminaliteit, moet voldoen om te waarborgen dat zij tot het strikt noodzakelijke is beperkt — erop te worden gewezen dat dergelijke voorwaarden weliswaar kunnen verschillen naargelang van de maatregelen die voor het voorkomen, onderzoeken, opsporen en vervolgen van zware criminaliteit worden getroffen, maar dat de bewaring van de gegevens niettemin steeds moet voldoen aan objectieve criteria die een verband leggen tussen de te bewaren gegevens en het nagestreefde doel. In het bijzonder moeten dergelijke voorwaarden in de praktijk van dien aard blijken te zijn dat zij de omvang van de maatregel, en dus de kring van betrokken personen, daadwerkelijk afbakenen.

111 Wat de afbakening van een dergelijke maatregel ter zake van de personen en situaties betreft die onder die maatregel kunnen vallen, moet de nationale regeling worden gebaseerd 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. Een dergelijke afbakening kan aan de hand van een geografisch criterium worden verricht wanneer de bevoegde nationale autoriteiten op basis van objectieve elementen van mening zijn dat er in een of meer geografische gebieden een hoog risico bestaat dat dergelijke handelingen worden voorbereid of gepleegd.

112 Gelet op een en ander dient op de eerste vraag in zaak C-203/15 te worden geantwoord dat artikel 15, lid 1, van richtlijn 2002/58, gelezen tegen de achtergrond van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, in die zin moet worden uitgelegd dat het zich verzet tegen een nationale regeling die, ter bestrijding van criminaliteit, voorziet in algemene en ongedifferentieerde bewaring van alle verkeersgegevens en locatiegegevens van alle abonnees en geregistreerde gebruikers betreffende alle elektronischecommunicatiemiddelen.

Tweede vraag in zaak C-203/15 en eerste vraag in zaak C-698/15

113 Om te beginnen dient erop te worden gewezen dat de Kammarrätt i Stockholm de tweede vraag in zaak C-203/15 slechts heeft gesteld voor het geval dat de eerste vraag in die zaak ontkennend wordt beantwoord. Deze tweede vraag staat echter los van de algemene of gerichte aard van bewaring van de gegevens, in de betekenis die daaraan in de punten 108 tot en met 111 van het onderhavige arrest is gegeven. Bijgevolg dienen de tweede vraag in zaak C-203/15 en de eerste vraag in zaak C-698/15, die los van de omvang van de aan de aanbieders van elektronischecommunicatiediensten opgelegde verplichting tot bewaring van gegevens is gesteld, samen te worden beantwoord.

114 Met de tweede vraag in zaak C-203/15 en de eerste vraag in zaak C-698/15 wensen de verwijzende rechterlijke instanties in wezen te vernemen of artikel 15, lid 1, van richtlijn 2002/58, gelezen tegen de achtergrond van de artikelen 7 en 8 en artikel 52, lid 1, van het Handvest, in die zin moet worden uitgelegd dat het zich verzet tegen een nationale regeling die de bescherming en de beveiliging van de verkeersgegevens en de locatiegegevens en, in het bijzonder, de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens regelt zonder te bepalen dat die toegang alleen wordt verleend ter bestrijding van ernstige criminaliteit, dat die toegang aan een voorafgaand toezicht door een rechterlijke instantie of een onafhankelijke bestuurlijke autoriteit is onderworpen, en dat de betrokken

gegevens op het grondgebied van de Unie moeten worden bewaard.

115 Met betrekking tot de doelstellingen die een rechtvaardiging kunnen vormen voor een nationale regeling die een uitzondering maakt op het beginsel van de vertrouwelijkheid van de elektronische communicatie, dient eraan te worden herinnerd dat, aangezien de in artikel 15, lid 1, eerste zin, van richtlijn 2002/58 gegeven opsomming van de doelstellingen exhaustief is, zoals in de punten 90 en 102 van het onderhavige arrest is vastgesteld, de toegang tot de bewaarde gegevens daadwerkelijk en strikt op een van die doelstellingen moet berusten. Daarbij komt dat, aangezien het met deze regeling nagestreefde doel in verhouding moet staan tot de ernst van de ingreep in de grondrechten die deze toegang meebrengt, ter zake van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten alleen de bestrijding van zware criminaliteit een dergelijke toegang tot de bewaarde gegevens kan rechtvaardigen.

116 Wat de eerbiediging van het evenredigheidsbeginsel betreft, moet een nationale regeling betreffende de voorwaarden waaronder de aanbieders van elektronischecommunicatiediensten aan de bevoegde nationale autoriteiten toegang tot de bewaarde gegevens moeten verlenen, waarborgen dat, overeenkomstig hetgeen in de punten 95 en 96 van het onderhavige arrest is vastgesteld, een dergelijke toegang niet verder gaat dan strikt noodzakelijk is.

117 Daarbij komt dat, aangezien de in artikel 15, lid 1, van richtlijn 2002/58 bedoelde wettelijke maatregelen overeenkomstig overweging 11 van deze richtlijn 'adequate waarborgen [moeten] bevatten', een dergelijke maatregel volgens de in punt 109 van het onderhavige arrest aangehaalde rechtspraak duidelijke en nauwkeurige regels moet 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.

118 Om te waarborgen dat de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens niet verder gaat dan strikt noodzakelijk is, dient in het nationale recht in elk geval te worden bepaald onder welke voorwaarden de aanbieders van elektronischecommunicatiediensten een dergelijke toegang moeten verlenen. De betrokken nationale regeling mag zich echter niet ertoe beperken, te eisen dat de toegang wordt verleend voor een van de in artikel 15, lid 1, van richtlijn 2002/58 genoemde doelstellingen, zelfs indien dit de bestrijding van zware criminaliteit zou zijn. Een dergelijke nationale regeling moet immers ook de materiële en procedurele voorwaarden voor de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens bepalen (zie naar analogie, met betrekking tot richtlijn 2006/24, arrest *Digital Rights*, punt 61).

119 Aangezien 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, moet de betrokken nationale regeling dus 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. In dit verband kan in beginsel voor het doel van bestrijding van 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 (zie naar analogie EHRM, 4 december 2015, *Zakharov tegen Rusland*, CE:ECHR:2015:1204JUD004714306, § 260). In bijzondere situaties, zoals die waarin vitale belangen van nationale veiligheid, landsverdediging of openbare veiligheid door terroristische activiteiten worden bedreigd, zou echter 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.

120 Om te waarborgen dat deze voorwaarden in de praktijk ten volle in acht worden genomen, is het van wezenlijk belang dat de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens in beginsel, behalve in gevallen van naar behoren gerechtvaardigde spoedeisendheid, wordt onderworpen aan een voorafgaand toezicht door een rechterlijke instantie of door een onafhankelijke bestuurlijke entiteit, en dat deze rechterlijke instantie of deze entiteit haar beslissing geeft 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 (zie naar analogie, met betrekking tot richtlijn 2006/24, arrest *Digital Rights*, punt 62; zie ook naar analogie, met betrekking tot artikel 8 EVRM, EHRM, 12 januari 2016, *Szabó en Vissy tegen Hongarije*, CE:ECHR:2016:0112JUD003713814, §§ 77 en 80).

121 Verder is het van belang dat de bevoegde nationale autoriteiten waaraan toegang tot de bewaarde gegevens is verleend, in het kader van de toepasselijke nationale procedures de betrokken personen daarvan op de hoogte brengen wanneer zulks de door deze autoriteiten gevoerde onderzoeken niet in gevaar kan brengen. Dit is immers noodzakelijk om de betrokken personen in staat te stellen om, in geval van schending van hun rechten, met name gebruik te maken van het recht van beroep, waarin artikel 15, lid 2, van richtlijn 2002/58, gelezen in samenhang met artikel 22 van richtlijn 95/46, uitdrukkelijk voorziet (zie naar analogie arresten

van 7 mei 2009, *Rijkeboer*, C-553/07, EU:C:2009:293, punt 52, en 6 oktober 2015, *Schrems*, C-362/14, EU:C:2015:650, punt 95).

122 Wat de regels betreffende de beveiliging en de bescherming van de door de aanbieders van elektronischecommunicatiediensten bewaarde gegevens betreft, staat vast dat artikel 15, lid 1, van richtlijn 2002/58 de lidstaten niet toestaat om af te wijken van artikel 4, lid 1, en artikel 4, lid 1 bis, van deze richtlijn. Laatstgenoemde bepalingen eisen immers dat deze aanbieders passende technische en organisatorische maatregelen treffen om de bewaarde gegevens doeltreffend te beschermen tegen het risico van misbruik en tegen elke onrechtmatige toegang tot deze gegevens. Gelet op de hoeveelheid bewaarde gegevens, op het gevoelige karakter van deze gegevens en op het risico van onrechtmatige toegang tot deze gegevens, moeten de aanbieders van elektronischecommunicatiediensten, om de volle integriteit en vertrouwelijkheid van die gegevens te verzekeren, door middel van passende technische en organisatorische maatregelen een bijzonder hoog niveau van bescherming en beveiliging waarborgen. In het bijzonder moet de nationale regeling bepalen dat de gegevens op het grondgebied van de Unie worden bewaard en na afloop van de bewaarperiode onherstelbaar worden vernietigd (zie naar analogie, met betrekking tot richtlijn 2006/24, arrest *Digital Rights*, punten 66–68).

123 In elk geval moeten de lidstaten waarborgen dat een onafhankelijke autoriteit toeziet op de inachtneming van het hoge niveau van bescherming dat wordt gewaarborgd door het Unierecht betreffende de bescherming van natuurlijke personen ter zake van de verwerking van hun persoonsgegevens, daar een dergelijk toezicht uitdrukkelijk wordt geëist door artikel 8, lid 3, van het Handvest en volgens vaste rechtspraak van het Hof een wezenlijk element van de bescherming van personen ter zake van de verwerking van hun persoonsgegevens vormt. Indien dit anders zou zijn, zou aan de personen van wie de persoonsgegevens zijn bewaard, het door artikel 8, leden 1 en 3, van het Handvest gewaarborgde recht worden ontnomen om zich ter bescherming van hun grondrechten tot de nationale toezichthoudende autoriteiten te wenden (zie in die zin arrest *Digital Rights*, punt 68, en arrest van 6 oktober 2015, *Schrems*, C-362/14, EU:C:2015:650, punten 41 en 58).

124 Het staat aan de verwijzende rechterlijke instanties, na te gaan of en in welke mate de in het hoofdgeding aan de orde zijnde nationale regelingen, zowel ter zake van de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens als ter zake van de bescherming en het niveau van beveiliging van deze gegevens, voldoen aan de eisen die voortvloeien uit 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, zoals die in de punten 115 tot en met 123 van het onderhavige arrest nader zijn uiteengezet.

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

Tweede vraag in zaak C-698/15

126 Met zijn tweede vraag in zaak C-698/15 wenst de Court of Appeal (England and Wales) (Civil Division) in wezen te vernemen of het Hof in het arrest *Digital Rights* de artikelen 7 en/of 8 van het Handvest heeft uitgelegd in een zin die verder gaat dan de uitlegging die het Europees Hof voor de Rechten van de Mens van artikel 8 EVRM heeft gegeven.

127 Om te beginnen dient eraan te worden herinnerd dat hoewel, zoals in artikel 6, lid 3, VEU wordt bepaald, de grondrechten zoals zij worden gewaarborgd door het EVRM als algemene beginselen deel uitmaken van het Unierecht, het EVRM, zolang de Unie er geen partij bij is, geen formeel in de rechtsorde van de Unie opgenomen rechtsinstrument is (zie in die zin arrest van 15 februari 2016, *N.*, C-601/15 PPU, EU:C:2016:84, punt 45 en aldaar aangehaalde rechtspraak).

128 De in het onderhavige geval aan de orde zijnde richtlijn 2002/58 moet dus uitsluitend tegen de achtergrond van de door het Handvest gewaarborgde grondrechten worden uitgelegd (zie in die zin arrest van 15 februari 2016, *N.*, C-601/15 PPU, EU:C:2016:84, punt 46 en aldaar aangehaalde rechtspraak).

129 Verder dient eraan te worden herinnerd dat volgens de toelichtingen bij artikel 52 van het Handvest artikel 52, lid 3, ervan beoogt te zorgen voor de nodige samenhang tussen het Handvest en het EVRM, 'zonder dat dit […] de autonomie van het recht van de Unie of van het Hof van Justitie van de Europese Unie aantast' (arrest van 15 februari 2016, *N.*, C-601/15 PPU, EU:C:2016:84, punt 47). In het bijzonder verhindert artikel 52, lid 3, eerste zin, van het Handvest — zoals in artikel 52, lid 3, tweede zin, daarvan uitdrukkelijk wordt bepaald — niet dat het Unierecht een ruimere bescherming biedt dan het EVRM. Daarbij komt, ten slotte, dat artikel 8 van het Handvest betrekking heeft op een ander grondrecht dan het in artikel 7 van het Handvest geformuleerde grondrecht, dat geen equivalent heeft in het EVRM.

130 Volgens vaste rechtspraak van het Hof is de rechtvaardiging van een verzoek om een prejudiciele beslissing echter niet gelegen in het formuleren van rechtsgeleerde adviezen over algemene of hypothetische vraagstukken, maar in de behoefte aan de werkelijke beslechting van een geschil dat verband houdt met het Unierecht (zie in die zin arresten van 24 april 2012, *Kamberaj*, C-571/10, EU:C:2012:233, punt 41 (*NJ* 2012/386, m.n.t M.R. Mok; *red.*); 26 februari 2013, *Åkerberg Fransson*, C-617/10, punt 42 (*NJ* 2013/348, m.nt. M.R. Mok; *red.*), en 27 februari 2014, *Pohotovosť*, C-470/12, punt 29).

131 Gelet op de met name in de punten 128 en 129 van het onderhavige arrest geformuleerde overwegingen, kan het antwoord op de vraag of de door de artikelen 7 en 8 van het Handvest verleende bescherming verder gaat dan de door artikel 8 EVRM verleende bescherming, in het onderhavige geval geen invloed hebben op de uitlegging — tegen de achtergrond van het Handvest — van richtlijn 2002/58, die aan de orde is in het hoofdgeding in zaak C-698/15.

132 Aldus kan een antwoord op de tweede vraag in zaak C-698/15 geen elementen van uitlegging van het Unierecht aandragen die noodzakelijk zijn voor de beslechting van dat geding uit het oogpunt van het Unierecht.

133 Bijgevolg is de tweede vraag in zaak C-698/15 niet-ontvankelijk.

Het Hof (Grote kamer) verklaart voor recht: zie cursieve kop.

Noot

De eerste zaak C- 203/15

1. De eerste zaak betreft het verzamelen van data door de Zweedse veiligheidsdienst en de Zweedse douane. Zij kan gezien worden als een vervolg op de toetsing van Dataretentierichtlijn (2006/24). De beslissing die daarover ging was HvJ EU 8 april 2014, (*Digital Rights/Ireland*, zaken C-293/12 en C-594/12), samen met de zaak *Schrems/Ierland* (de zaak over safe harbor, HvJ EU 6 oktober 2015, zaak C-362/14) met een noot van mij gepubliceerd in *NJ* 2016/446 en *NJ* 2016/447. In *Digital Rights* oordeelde het Hof dat de Dataretentierichtlijn op verschillende punten een ernstige inbreuk op de privacy vormde. Uit mijn vorige noot: "Er is niet alleen een inmenging in het privéleven, maar ook een inbreuk op artikel 8 van het Handvest, aangezien opslag een 'verwerking' in de zin van dat artikel is (r.o. 36). Het gaat om 'een zeer ruime en zware' inbreuk op beide rechten, temeer daar de gegevens worden bewaard om later eventueel te worden gebruikt zonder dat de betrokkene daarover wordt ingelicht, zodat de bellers of servers het gevoel kunnen hebben dat zij constant in de gaten worden gehouden (r.o. 37). Daaraan voegt het Hof dan in r.o. 55 toe dat het om een automatische verwerking gaat waardoor het risico voor onrechtmatige verwerking aanzienlijk is, in r.o. 56 dat het gaat om verkeersgegevens van alle elektronische diensten in de hele EU, dus 'de gehele Europese bevolking', en in r.o. 59 dat er op zich zelf geen enkel verband bestaat tussen opgeslagen gegevens en de zware criminaliteit die beoogd wordt te bestrijden. Het Hof acht de opslag gerechtvaardigd door de algemene belangen die ermee zijn gediend (r.o.-en 38-44)". Het Hof oordeelde toen dat de rechtsbescherming van het datasubject onvoldoende was: "In de eerste plaats ontbreekt een afdoende rechtsbescherming voor het datasubject. In r.o. 62 stelde het vast dat de toegang van de bevoegde nationale autoriteit 'bovenal' niet is onderworpen 'aan enige voorafgaande controle door een rechterlijke instantie of een onafhankelijke administratieve instantie waarvan de beslissing beoogt om de toegang tot de gegevens te beperken tot wat strikt noodzakelijk is ter verwezenlijking van het nagestreefde doel en die uitspraak doet op een gemotiveerd verzoek van deze autoriteiten, ingediend in het kader van procedures ter voorkoming, opsporing of vervolging van strafbare feiten. Het tweede punt is de plaats van opslag. Het Hof oordeelt in r.o.-en 66 en 67 dat er onvoldoende maatregelen zijn genomen ter voorkoming van misbruik. Dit spitst het in r.o. 68 toe op het feit dat niet is voorgeschreven dat de gegevens worden bewaard op het grondgebied van de staat dat de bewaarplicht heeft voorgeschreven." Alles bijeengenomen werd de gehele richtlijn nietig verklaard.

2. In het geval van de Dataretentierichtlijn was de collectieve opslag, zoals ik de grootschalige en ongedifferentieerde opslag van communicatiegegevens verder noem, ook aangevoerd, maar het HvJ EU deed de zaak af op het gebrek aan rechtsbescherming en gebreken in de opslag. In deze zaak gaat het om de verplichting van de service providers alle communicatiedata van de gebruikers gedurende 6 maanden op te slaan (zie r.o. 17-19). Het gaat dus om een algemene dataretentie zoals ook in richtlijn 2002/58 was voorzien. De veiligheidsdienst en de douane kunnen op basis van een beslissing van de directeuren van de diensten die niet aan voorafgaande onafhankelijke controle is onderworpen toegang tot deze data krijgen (r.o. 21-24). Na de uitspraak in de *Digital Rights* waarbij de Dataretentierichtlijn nietig werd verklaard weigerde Tele-2 nog te voldoen aan de verzoeken tot inzage van de hiervoor vermelde autoriteiten. De Zweedse Minister van Justitie liet vervolgens een rapport uitbrengen of de Zweedse praktijk na die nietigverklaring nog te handhaven was. De rapporteur vond van wel, omdat in de *Digital Rights* de dataretentie niet ten principale, maar op het gebrek aan rechtsbescherming was veroordeeld. Daarop werd Tele-2 voor de rechter gedaagd wegens handelen in strijd met de Zweedse retentieverplichting (r.o. 46 en 47). De rechter ecarteerde nu de inmiddels nietig verklaarde dataretentierichtlijn (2006/24) en stelde zich (en vervolgens het HvJ EU) de vraag of de Zweedse wetgeving in overeenstemming was met het uitzonderingsartikel van de richtlijn over privacy, dataprotectie en elektronische communicaties (2002/58).

Deze bevat een art. 15 dat een uitzondering toelaat op de algemene verplichting van art. 5 dat data niet langer mogen worden opgeslagen en bewerkt dan verenigbaar is met het doel. Voor aanbieders van elektronische communicatiediensten betekent die algemene regel dat opslag en verwerking niet langer is toegestaan dan voor het aanbieden van de dienst nodig is (technische opslag voor de kwaliteit van de dienstverlening, marketing en facturering). De uitzondering van art. 15 van de algemene regel zegt dat langere opslag en bewerking mogelijk is, als de proportionaliteitsbeginselen van de democratische rechtsstaat in acht worden genomen en als dat gebeurt in het belang van de staatsveiligheid, defensie, sociale veiligheid en de voorkoming en berechting van strafbare feiten. Na de nietigverklaring van de datarichtlijn 2006/24 met specifieke geharmoniseerde uitzonderingsregels, lag dus bij het Hof voor de invulling en uitleg van de algemene uitzonderingsbevoegdheid in art. 15 van de algemene richtlijn 2002/58. De verwijzende rechter stelde aan het Hof de eerste vraag of, gegeven de uitspraak in de *Digital Rights* en gegeven de constitutionele bescherming die de art. 7 en 8 van het Handvest aan privacy en dataprotectie verlenen, en gegeven de democratische en rechtsstatelijke eisen die art. 52 lid 1 van het Handvest aan de beperkingen van grondrechten stelt, de algemene Zweedse retentieverplichting wel in overeenstemming is met het EU recht. Wanneer het antwoord daarop ontkennend is, onder welke voorwaarden mag opslag dan wel, was de tweede vraag? In de prejudiciële vraag neemt de verwijzende rechter niet expliciet art. 15 van richtlijn 2002/58 op, maar impliciet is dit artikel natuurlijk wel het scharnierpunt zoals uit de beslissing van het Hof blijkt.

De tweede zaak C-698/15

3. In het Verenigd Koninkrijk starten drie staatsburgers na de beslissing in de *Digital Rights* een procedure tegen de Minister van Binnenlandse zaken, waarin zij de rechtsgeldigheid van soortgelijke retentieverplichtingen als in Zweden in de Engelse wet op de veiligheidsdiensten bestrijden. Zij beroepen zich op de art. 7 en 8 van het Handvest en art. 8 EVRM (r.o. 52 e.v.). In eerste instantie krijgen zij gelijk, maar de rechter in hoger beroep vindt het nodig prejudiciële vragen te stellen. Hij wil op twee punten een uitleg hebben van de uitspraak in *Digital rights*: 1. Bevat deze uitspraak de noodzakelijkheidsverplichtingen ('mandatory requirements') die lidstaten in acht moeten nemen bij een regeling van opslag en bewerking van communicatiegegevens?, en, 2. Breidt deze uitspraak de beschermingsomvang ('the scope') van de art. 7 en 8 van het Handvest uit buiten die van art. 8 EVRM zoals door het EHRM is geïnterpreteerd? De eerste vraag gaat dus impliciet over de ruimte die de uitzonderingsregel van art. 2002/58 geeft, de tweede is gebaseerd op art. 52 lid 3 van het Handvest. Dat legt immers het EVRM als minimum beschermingsniveau vast, maar acht verdergaande bescherming onder het Handvest mogelijk.

De beslissing van het HvJ EU

4. Het Hof voegt beide zaken samen. In de eerste zaak interveniëren verschillende lidstaten, waaronder Nederland, met het betoog, dat na de nietigverklaring van Dataretentierichtlijn, er nog wel degelijk ruimte is voor collectieve opslag. De Commissie doet dat ook en zet de zaak in de sleutel van de uitleg van richtlijn 2002/58 en de beschermingsomvang daarvan. Het Hof volgt de Commissie daarin (r.o. 67 e.v.). Een belangrijke kernoverweging is daarbij r.o. 53. De al genoemde uitzonderingsregel van art. 15 van richtlijn 2002/58 verwijst naar gebieden die tot het domein van de nationale staatsveiligheid behoren (over het algemeen voorbehouden aan de lidstaten), maar dat betekent niet dat de beginselen van privacy en dataprotectie die zijn neergelegd in de richtlijn niet van toepassing zouden zijn. Het geeft daartoe ook een specifieke uitleg van de richtlijn, die dat bevestigt (r.o. 74 e.v.). De maatregelen die in deze procedure ter discussie staan (collectieve opslag) zijn het soort maatregelen waarvoor deze richtlijn beginselen beoogt vast te leggen. Vastgesteld hebbende dat maatregelen met betrekking tot de staatsbelangen die art. 15 van richtlijn 2002/58 noemt onder de richtlijn vallen als zij raken aan de privacybelangen die de richtlijn beoogt te beschermen, geeft het Hof een uitleg aan de toepassing van dit artikel in het licht van de 7, 8 en 11 en art. 52 lid 1 van het Handvest.

5. Het Hof kiest als uitgangspunt het hoge beschermingsniveau voor privacy en persoonsgegevens dat richtlijn 2002/58 beoogt te geven (r.o. 82-84). De vertrouwelijkheid van communicatie staat dus voorop en dus ook de hoofdregel dat opslag van communicatiegegevens slechts is toegestaan voor de kwaliteit van de dienstverlening, marketing en facturering. De uitzondering moet strikt worden uitgelegd, want anders zou het stellen van beschermingsregels nutteloos zijn (r.o. 89 slot: 'if the provision is not to become largely meaningless'; zie ook r.o. 104-107). Verzet het systeem van de richtlijn zich dus tegen collectieve opslag, een tweede beperking volgt uit art. 15 zelf, omdat daarin de doeleinden voor de beperking nauwkeurig zijn opgesomd, zodat je daar niet buiten mag treden (wat bij collectieve opslag het geval is). Verder moet de richtlijn in het licht van het Handvest worden uitgelegd, zoals het Hof ook bij eerdere uitleg van de richtlijn heeft vastgesteld (onder meer verwijzing naar de *Google/Spanje zaak*, C-131/12). Niet alleen dat de vergaande beperking vragen oproept in het licht van de art. 7 en 8 van het Handvest, maar ook in het kader van de vrijheid van meningsuiting (art. 11). Het Hof had dat ook al in *Digital Rights* opgemerkt (constatering in r.o. 25, maar niet beslist in dat arrest). Ook dat recht is een van de fundamenten van de democratische rechtsstaat waarop de EU is gebouwd (r.o. 93-94). Met dit allemaal in gedachten beoordeelt het Hof de Zweedse wetgeving en acht het deze een te

vergaande beperking (r.o. 97 e.v.). Het Hof acht de inbreuk op de privacy in r.o. 100 zeer ernstig, omdat het de burgers het gevoel zal geven dat zij constant worden geobserveerd (het 'Big Brother is watching you' gevoel dus), iets wat het ook al in *Digital Rights* had gezegd. Een belangrijk legitiem doel als de bestrijding van zware criminaliteit en terrorisme is onvoldoende om een dergelijke inbreuk te rechtvaardigen (r.o. 103).

6. Wat wel mag zegt het Hof in r.o. 108-111: de lidstaten mogen als een preventieve maatregel wetgeving aannemen waarin dataretentie gericht is ('targeted') en tot doel heeft specifieke zware criminaliteit te bestrijden, en wanneer de retentie beperkt is tot wat strikt noodzakelijk is met betrekking tot de feiten die het wil bestrijden, de personen die er door geraakt worden en de tijdsperiode waarin zij kan worden uitgeoefend. Er moet wetgeving zijn die de criteria daarvoor precies vastlegt. Aan die maatstaven voldeed de onderhavige Zweedse wetgeving niet. Blijft de vraag wat voldoende 'targeted' is, of anders gezegd hoe specifiek en concreet de wet moet zijn. Dat zal nog wel een politiek discussiepunt blijven.

7. In de tweede zaak trekt het Hof de tweede vraag in de eerste zaak samen met de eerste vraag in de tweede zaak. Het bespreekt daarbij de eisen die naast de beperkingen in de verzameling en opslag die het in de r.o. 108-111 omschrijft verder moeten worden gesteld. Het is beperkt tot de doeleinden opgesomd in art. 15 van de richtlijn, er moet ex ante toezicht zijn door een onafhankelijke rechter of een onafhankelijke administratieve instantie, en de wettelijke regels en procedures moeten precies zijn. Wat het Hof hier zegt stemt in grote lijnen overeen met wat het EHRM in de *Zakharov* zaak (*NJ* 2017/185, m.nt. E.J. Dommering) heeft geoordeeld.

8. Bij de beantwoording van de tweede vraag geeft het Hof een kort college hoe de relatie tussen het HvJ EU en EHRM is en hoe die tussen het Handvest en het EVRM. Zolang de EU niet tot de Raad van Europa is toegetreden is de EU ten opzichte van het EVRM een aparte rechtsorde (en dat moet volgens het Hof zo blijven, zie HvJ EU 18 december 2014, Advies 2/13; het noemt in r.o. 127 HvJ EU 15 februari 2016, C-601/15). De verwijzing in art. 52 lid 3 van het Handvest naar het EVRM is slechts bedoeld om de consistentie in de interpretatie van gelijkwaardige grondrechten in de EU en de Raad van Europa te waarborgen, maar koppelt de rechtsordes niet aan elkaar. De prejudiciële procedure is niet bedoeld om het Hof algemene dogmatische vragen te beantwoorden. Het volstaat daarom dus met een uitleg van de richtlijn 2002/58 en de art. 7, 8 en 11 van het Handvest.

Slotoverwegingen

9. Deze beslissing en die van het EHRM in de hiervoor gepubliceerde zaak *Zakharov* (*NJ* 2017/185, m.nt. E.J. Dommering) legt een fundamentele controverse bloot tussen de Europese rechterlijke macht en de politieke machten (wetgeving en bestuur) in de lidstaten in de verschillende Europese rechtsgemeenschappen. De rechters trekken een scherpe scheidslijn tussen enerzijds de bestuurlijke en wetgevende macht die terrorisme en zware criminaliteit willen beschermen en daarom totale controle over de staatsburgers willen, en anderzijds de vrijheid van de burgers die hun leven in beginsel niet gehinderd door staatsmacht willen ontplooien. Dat komt goed tot uitdrukking in de conclusie van de advocaat-generaal in deze zaak die in paragraaf 1 begint met een citaat uit 1788 van één van de Amerikaanse 'framers' van de Constitutie, Madison (*Federalist Paper* nr 51): *"If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself."* Over deze 'moeilijkheid' gaat het trekken van de scheidslijn tussen de behoefte aan controle en de bescherming van de individuele vrijheid. De rechters wijzen het model van een digitale schaduwboekhouding waarin de hele geschiedenis van alle handelingen en communicaties van de staatsburgers is te vinden (de advocaat-generaal in paragraaf 3: 'to examine the past') principieel af. De politieke machten willen die schaduwboekhouding wel, aanvaarden alleen beperkingen op de toegang tot die boekhouding. Het verbaast ons misschien niet dat 'de moeilijkheid' in totalitair geregeerde landen als Rusland niet bevredigend is opgelost (de zaak *Zakharov*). Maar zij bestaat net zo goed, en met het groeien van de datatechnologie steeds vaker, in parlementaire democratieën: Deze zaak gaat over Zweden en het Verenigd Koninkrijk. *Digital Rights* ging over Ierland. Ik signaleerde in mijn noot bij *Zakharov* dat 'de moeilijkheid' in Nederland in het bij het parlement aanhangige wetsontwerp voor de wijziging van de Wet op de inlichtingen en veiligheidsdiensten (WIV) niet bevredigend is opgelost. De 'moeilijkheid' zit in de vraag of de wettelijke criteria wel voldoende 'targeted' zijn en of de rechtsbescherming afdoende is geregeld. Deze zaak werpt het zoeklicht op het aanhangige wetsontwerp 'Bewaarplicht telecommunicatiegegevens' (*Kamerstukken II* 2016/17, 34537) dat in de huidige versie een algemene bewaarplicht handhaaft. In haar interventie bij het HvJ EU in deze zaak had de Nederlandse regering betoogd dat *Digital Rights* dat niet had afgewezen. Daarin krijgt zij in deze zaak dus ongelijk.

10. Art. 4 van het VWEU verdrag verklaart dat de nationale veiligheid de uitsluitende bevoegdheid van de lidstaten blijft. In deze beslissing nuanceert het Hof dit door te beslissen dat de invulling daarvan wel degelijk onderworpen blijft aan de beperkingen die uit het Handvest voortvloeien. Het Hof doet dat via een tweetrapsraket. Eerst geeft het een uitleg aan het systeem van richtlijn 2002/58 en de plaats die art. 15 dat over nationale veiligheid gaat daarin heeft. Dan legt het art. 15 uit in het kader van

de werking van de relevante artikelen in het Handvest.

11. Het Hof acht niet alleen de privacy en de dataprotectie, maar ook de vrijheid van meningsuiting in het geding (art. 11 van het Handvest). Die stap heeft het EHRM tot dusver niet gezet. De redenering is dat een algemene dataretentieplicht een 'Big Brother is watching you' effect heeft en daarmee het onbelemmerd gebruik van communicatiemiddelen hindert. Dat lijkt mij terecht. Communicatie in de privésfeer raakt aan de vrijheid van denken en uitwisseling van gedachten en daarmee aan de vorming van een publiek te uiten mening. Deze benadering vindt geleidelijk ingang. Ik noem het 'intellectuele privacy' (zie *Het Verschil van Mening, De geschiedenis van een verkeerd begrepen idee*, Amsterdam: Bert Bakker 2016, p. 32).

E.J. Dommering

NJ 2017/187

HOF VAN JUSTITIE VAN DE EUROPESE UNIE
9 januari 2015, nr. C-498/14 PPU
(L. Bay Larsen, K. Jürimaë, J. Malenovský, M. Safjan, A. Prechal; A-G N. Jääskinen)
m.nt. Th.M. de Boer

Art. 11 lid 7 en 8 Brussel II-bis

ECLI:EU:C:2015:3

Verzoek om een prejudiciële beslissing krachtens art. 267 VWEU, ingediend door de Cour d'appel te Brussel (België) bij beslissing van 7 november 2014.

Brussel II-bis. Bevoegdheid inzake ouderlijke verantwoordelijkheid. Kinderontvoering. Procedure na afwijzing verzoek teruggeleiding; bevoegde rechter.

Art. 11 lid 7 en 8 Verordening Brussel II-bis moet aldus worden uitgelegd dat het er in beginsel niet tegen verzet dat een lidstaat een gespecialiseerd gerecht de bevoegdheid verleent om vragen betreffende de terugkeer van of het gezagsrecht over het kind te onderzoeken in het kader van de procedure die in deze bepaling is vastgesteld, zelfs wanneer bij een hof of rechtbank voor het overige reeds een bodemprocedure inzake de ouderlijke verantwoordelijkheid voor het kind aanhangig is gemaakt.

B.
tegen
A.

Hof van Justitie EU:

1 Het verzoek om een prejudiciële beslissing betreft de uitlegging van artikel 11, leden 7 en 8, van verordening (EG) nr. 2201/2003 van de Raad van 27 november 2003 betreffende de bevoegdheid en de erkenning en tenuitvoerlegging van beslissingen in huwelijkszaken en inzake de ouderlijke verantwoordelijkheid, en tot intrekking van verordening (EG) nr. 1347/2000 (*PB* L 338, blz. 1; hierna: 'verordening').

2 Dit verzoek is ingediend in het kader van een geding tussen de heer B. en mevrouw A. betreffende de ouderlijke verantwoordelijkheid voor hun zoon N., die door A. wordt vastgehouden in Polen.

Toepasselijke bepalingen

Haags Verdrag van 1980

3 Artikel 3 van het Verdrag van 's-Gravenhage van 25 oktober 1980 betreffende de burgerrechtelijke aspecten van internationale ontvoering van kinderen (hierna: 'Haags Verdrag van 1980') bepaalt:

"Het overbrengen of het niet doen terugkeren van een kind wordt als ongeoorloofd beschouwd, wanneer

a) dit geschiedt in strijd met een gezagsrecht, dat is toegekend aan een persoon, een instelling of enig ander lichaam, alleen of gezamenlijk, ingevolge het recht van de staat waarin het kind onmiddellijk voor zijn overbrenging of vasthouding zijn gewone verblijfplaats had, en

b) dit recht alleen of gezamenlijk daadwerkelijk werd uitgeoefend op het tijdstip van het overbrengen of het niet doen terugkeren, dan wel zou zijn uitgeoefend, indien een zodanige gebeurtenis niet had plaatsgevonden.

Het onder a) bedoelde gezagsrecht kan in het bijzonder voortvloeien uit een toekenning van rechtswege, een rechterlijke of administratieve beslissing of een overeenkomst die geldig is ingevolge het recht van die staat."

4 Artikel 12 van dit Verdrag is als volgt verwoord:

"Wanneer een kind ongeoorloofd is overgebracht of wordt vastgehouden in de zin van artikel 3 en er minder dan één jaar is verstreken tussen de overbrenging of het niet doen terugkeren en het tijdstip van de indiening van het verzoek bij de rechterlijke of administratieve autoriteit van de verdragsluitende staat waar het kind zich bevindt, gelast de betrokken autoriteit de onmiddellijke terugkeer van het kind.

[…]"

5 Artikel 13 van het Haags Verdrag van 1980 bepaalt:

"Niettegenstaande het bepaalde in het voorgaande artikel, is de rechterlijke of administratieve autoriteit van de aangezochte staat niet gehouden de terugkeer van het kind te gelasten, indien de persoon, de instelling of het lichaam dat zich tegen de terugkeer verzet, aantoont dat:

a) de persoon, de instelling of het lichaam dat de zorg had voor de persoon van het kind, het recht betreffende het gezag niet daadwerkelijk uitoefende ten tijde van de overbrenging of