



Datum van inontvangstneming : 29/01/2016

Zaak C-698/15

Verzoek om een prejudiciële beslissing

Datum van indiening:

28 december 2015

Verwijzende rechter:

Court of Appeal of England and Wales, Civil Division (Verenigd Koninkrijk)

Datum van de verwijzingsbeslissing:

9 december 2015

Verwerende partij in eerste aanleg / appellant:

Secretary of State for the Home Department

Verzoekende partijen in eerste aanleg / geïntimeerden:

David Davis MP

Tom Watson MP

Peter Brice

Geoffrey Lewis

Interveniënten:

Open Rights Group

Privacy International

Law Society of England and Wales

[*omissis*]

BESLIST WORDT ALS VOLGT

1. Het Hof van Justitie van de Europese Unie (hierna: „Hof van Justitie”) wordt om een prejudiciële beslissing overeenkomstig artikel 267 van het Verdrag

betreffende de werking van de Europese Unie verzocht over de in de bijlage bij deze beslissing uiteengezette vragen. De bijlage bij deze beslissing en de begeleidende stukken [*omissis*] zullen terstond, zonder te wachten tot de beroepstermijn is verstreken, naar het Hof van Justitie worden gezonden.

2. [*omissis*]

3. De behandeling van de zaak wordt geschorst totdat het Hof van Justitie van de Europese Unie heeft geantwoord op de in de bijlage vermelde prejudiciële vragen, of tot nader order.

[*omissis*]

[Or. 1-2]

[*omissis*]

**PREJUDICIËLE VERWIJZING NAAR HET HOF VAN JUSTITIE VAN
DE EUROPESE UNIE**

[*omissis*]

[*omissis*] **[Or. 3-5]**

BIJLAGE

[*omissis*]

**IN HET HOGER BEROEP BIJ DE COURT OF APPEAL (CIVIL
DIVISION) TEGEN DE UITSPRAAK VAN DE HIGH COURT OF
JUSTICE, QUEEN'S BENCH DIVISION, DIVISIONAL COURT** [*omissis*]

VERZOEKEN

SECRETARY OF STATE FOR THE HOME DEPARTMENT

appellant

– en –

**1) DAVID DAVIS MP 2) TOM WATSON MP 3) PETER BRICE 4)
GEOFFREY LEWIS**

geïntimeerden

**1) OPEN RIGHTS GROUP 2) PRIVACY INTERNATIONAL 3) THE LAW
SOCIETY OF ENGLAND AND WALES**

intervenienten

OM EEN PREJUDICIËLE BESLISSING OVEREENKOMSTIG ARTIKEL 267 VAN HET VERDRAG BETREFFENDE DE WERKING VAN DE EUROPESE UNIE

PREJUDICIËLE VRAGEN

1. Legt het arrest van het Hof van Justitie in de gevoegde zaken C-293/12 en C-594/12, Digital Rights Ireland en Seitlinger, ECLI:EU:C:2014:238 (hierna: „Digital Rights Ireland”) (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 met betrekking tot de toegang tot gegevens die overeenkomstig nationale wetgeving worden bewaard, teneinde te voldoen aan de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie (hierna: „Handvest”)?

2. Verruimt het arrest van het Hof van Justitie in de zaak Digital Rights Ireland de werkingsfeer van de artikelen 7 en 8 van het Handvest ten opzichte van deze van artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (hierna: „EVRM”), zoals vastgelegd in de rechtspraak van het Europees Hof voor de Rechten van de Mens (hierna: „EHRM”)? **[Or. 6]**

ACHTERGROND

Inleiding

- 1 Deze verwijzing is het gevolg van drie verzoeken om rechterlijke toetsing die zijn ingediend bij de bestuursrechtelijke afdeling van de High Court of Justice [dat wil zeggen, de Queen’s Bench Division, Divisional Court], namelijk de zaak Peter Brice [omissis], de zaak Geoffrey Lewis [omissis] en de zaak David Davis MP and Tom Watson MP [omissis]. De vier verzoekende partijen [de geïntimeerden in het hoger beroep bij de verwijzende rechter] bij die verzoeken worden hier aangeduid als „verzoekende partijen”.
- 2 Alle verzoekende partijen stellen dat de regeling inzake het bewaren van gegevens in section 1 [van de] Data Retention and Investigatory Powers Act 2014 [wet van 2014 inzake gegevensbewaring en onderzoeksbevoegdheden] (hierna: „DRIPA” of „wet”) in strijd is met de artikelen 7 en 8 van het Handvest en met artikel 8 EVRM.
- 3 De verwerende partij [de appellant bij de verwijzende rechter] in elk van de zaken is de Secretary of State for the Home Department (hierna: „Secretary of State”), die krachtens section 1 DRIPA gemachtigd is om een aanzegging te doen op grond waarvan een bedrijf dat openbare telecommunicatie aanbiedt (hierna: „openbare telecommunicatiebedrijf”) relevante communicatiegegevens dient te

bewaren. De Secretary of State voert aan dat section 1 van de DRIPA verenigbaar is met zowel de artikelen 7 en 8 van het Handvest als met artikel 8 EVRM.

- 4 De [intervenienten] [*omissis*] werden in elk van de zaken toegelaten tot interventie.

[*omissis*].

[*omissis*]. Hoewel dit uiteindelijk een zaak is voor het Hof van Justitie, is de Court of Appeal van oordeel dat de intervenienten moeten worden beschouwd als partijen en hun moet worden toegestaan deel te nemen in de verwijzingsprocedure. [Or. 7]

De Divisional Court

- 5 De Divisional Court [van de Queen's Bench Division] heeft geoordeeld (vonnis van 17 juli 2015, <http://www.bailii.org/ew/cases/EWHC/Admin/2015/2092.html>) dat section 1 van de DRIPA is strijdig met het Unierecht, voor zover

a) het geen duidelijke en precieze regels oplegt die bepalen dat de toegang tot en het gebruik van overeenkomstig een aanzegging tot bewaring bewaarde communicatiegegevens strikt gebonden zijn aan het doel, nauwkeurig afgebakende ernstige strafbare feiten te voorkomen, op te sporen of strafrechtelijk te vervolgen, en

b) de toegang tot de gegevens 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 en het gebruik ervan te beperken tot wat strikt noodzakelijk is ter verwezenlijking van het nagestreefde doel.

- 6 De Divisional Court kwam tot die conclusie, omdat hij van oordeel was dat het arrest van het Hof van Justitie in de gevoegde zaken C-293/12 en C-594/12, Digital Rights Ireland en Seitlinger, ECLI:EU:C:2014:238 (hierna: „Digital Rights Ireland”) „dwingende vereisten van Unierecht” oplegt die van toepassing zijn op de regelingen van de lidstaten inzake het bewaren van communicatiegegevens en de toegang ertoe.

De Court of Appeal

- 7 De Secretary of State is in hoger beroep gegaan bij de Court of Appeal. De Court of Appeal gaf het voorlopige oordeel [uitspraak van 20 november 2015, <http://www.bailii.org/ew/cases/EWCA/Civ/2015/1185.html>] dat het Hof van Justitie in het arrest Digital Rights Ireland geen specifieke dwingende vereisten van Unierecht heeft neergelegd waarmee nationale wetgeving dient te stroken,

maar slechts beschermingen vaststelde en beschreef die ontbraken in de geharmoniseerde Unieregeling.

- 8 Voorts betwijfelde de Court of Appeal of het Hof van Justitie in het arrest Digital Rights Ireland de bedoeling had verder te gaan dan de rechtspraak van het Europees Hof voor de Rechten van de Mens en strengere vereisten voor de bescherming van persoonsgegevens neer te leggen dan die welke zijn vastgelegd in de rechtspraak van het EHRM. **[Or. 8]**
- 9 Gezien echter het feit dat de antwoorden op deze vragen van Unierecht niet duidelijke waren, maar dat de Court of Appeal ze wel nodig had om een uitspraak te doen in de procedure, heeft de Court of Appeal een prejudiciële vraag voorgelegd aan het Hof van Justitie.
- 10 De zaken zijn gezamenlijk behandeld en er wordt één stel vragen voorgelegd aan het Hof van Justitie. Die vragen dienen te worden behandeld in het kader van nationale wetgeving, die voorziet in een regeling inzake het bewaren van gegevens, zoals uiteengezet in de punten 11 tot en met 21 hieronder, en in een regeling inzake de toegang tot bewaarde gegevens, zoals uiteengezet in de punten 22 tot en met 29 hieronder.

Nationale wetgeving: bewaring

- 11 De nationale wetgeving inzake gegevensbewaring bevindt zich in a) de DRIPA; b) de Data Retention Regulations 2014 [de voorschriften inzake gegevensbewaring van 2014] (SI 2014/2042) (hierna: „Voorschriften”), en c) de Retention of Communications [Data] Code of Practice [de praktijkrichtlijn voor het bewaren van communicatie(gegevens)] (hierna: „praktijkrichtlijn inzake bewaring”).
- 12 Section 1 van de DRIPA bepaalt het volgende:

„Aan waarborgen onderworpen bevoegdheden tot het bewaren van relevante communicatiegegevens

1) De Secretary of State kan door middel van een aanzegging (hierna: „aanzegging tot bewaring”) eisen dat een openbaar telecommunicatiebedrijf relevante communicatiegegevens bewaart, indien naar de opvatting van de Secretary of State het noodzakelijk en evenredig is dat te eisen, 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 uit 2000 inzake toezicht op onderzoeksbevoegdheden] (redenen waarom 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 dienen te worden bewaard;
 - d) andere voorwaarden of beperkingen bevatten met betrekking tot de gegevensbewaring;
 - 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 voorschriften vaststellen met nadere regelingen over de bewaring van relevante communicatiegegevens.
- 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, het doen, het van kracht worden, de herziening, de wijziging of de herroeping van een aanzegging tot bewaring;
 - d) de volledigheid, de veiligheid, de bescherming, het openbaar maken of het vernietigen van de gegevens die krachtens deze section worden bewaard, alsmede de toegang tot die gegevens; **[Or. 9]**
 - e) de handhaving, of de controle op de naleving, van relevante voorschriften of beperkingen;
 - f) een praktijkrichtlijn met betrekking tot relevante voorwaarden, beperkingen of bevoegdheden;
 - g) de (al dan niet aan voorwaarden verbonden) vergoeding door de Secretary of State van kosten die openbare telecommunicatiebedrijven maken om te voldoen aan relevante voorschriften of beperkingen, en
 - h) de buitenwerkingtreding van de 2009 Regulations [voorschriften uit 2009] en de overgang naar de gegevensbewaring op grond van deze section.

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

6) Een openbare telecommunicatiebedrijf dat op grond van deze section relevante communicatiegegevens bewaart, maakt deze niet openbaar, tenzij dit gebeurt

a) in overeenstemming met

i) hoofdstuk 2 van deel 1 van de Regulation of Investigatory Powers Act 2000 (het verkrijgen en openbaar maken van communicatiegegevens), of

ii) een rechterlijke beslissing of een andere machtiging of bevel van de rechter, of

b) volgens de in subsection 3) bedoelde voorschriften.

7) De Secretary of State kan voorschriften vaststellen die voorzien in regelingen die overeenstemmen met enige regeling die getroffen is (of kan worden getroffen) krachtens subsection 4, onder d) tot en met g), of 6 met betrekking tot communicatiegegevens die door aanbieders van telecommunicatiediensten worden bewaard op grond van een praktijkrichtlijn op grond van section 102 van de Anti-terrorism, Crime and Security Act 2001 [wet uit 2001 inzake terrorismebestrijding, misdaad en veiligheid].”

13 Krachtens section 1, lid 1, DRIPA, kan de Secretary of State een aanzegging tot bewaring doen uitgaan op grond waarvan een openbare telecommunicatiebedrijf is verplicht relevante communicatiegegevens te bewaren. Voorschrift 4 van de Voorschriften treft een nadere regeling met betrekking tot aanzeggingen tot bewaring. Op grond van section 1, lid 1, DRIPA kan de Secretary of State bepalen dat alle communicatiegegevens die binnen de werkingssfeer van de DRIPA vallen, worden bewaard, mits de Secretary of State een dergelijk vereiste noodzakelijk en evenredig acht. Aanzeggingen tot bewaring zijn geheim. Dienovereenkomstig zijn de nationale rechters ervan uitgegaan dat

„[...] wij de geldigheid van de DRIPA dienen te toetsen, ervan uitgaande dat de op grond daarvan gedane aanzeggingen tot bewaring een werkingssfeer hebben die zo ruim is als wettelijk toegestaan, namelijk een aanwijzing aan iedere [aanbieder van communicatiediensten] om gedurende een periode van twaalf maanden alle communicatiegegevens te bewaren. Beide partijen zijn in hun betoog daarvan uitgegaan. In deze uitspraak noemen wij een systeem waarin de staat kan eisen dat aanbieders van telecommunicatie gedurende een periode alle communicatiegegevens bewaren een „algemene bewaarregeling” (uitspraak van de Divisional Court, punt 65). [Or. 10]

14 Section 2 van de DRIPA bepaalt dat onder „communicatiegegevens” wordt verstaan hetgeen is gesteld in section 21, lid 4, van de Regulation of Investigatory Powers Act 2000 [wet uit 2000 inzake het toezicht op onderzoeksbevoegdheden] (hierna: „RIPA”), voor zover dat van toepassing is met betrekking tot telecommunicatiediensten en telecommunicatiesystemen. Section 21, lid 4, RIPA, bepaalt het volgende;

„4) In dit hoofdstuk wordt onder ‚communicatiegegevens’ een van de hieronder gegeven definities verstaan

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

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

i) van de posterijen of 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.”

15 Section 2 van de DRIPA definieert „relevante communicatiegegevens” als „het type communicatiegegevens dat wordt genoemd in de [Data Retention (EC Directive) Regulations 2009 (S.L 2009/859)] [voorschriften uit 2009 inzake gegevensbewaring (EG richtlijn)] voor zover dergelijke gegevens ontstaan of worden verwerkt in het Verenigd Koninkrijk door openbare telecommunicatiebedrijven tijdens het aanbieden van de betrokken telecommunicatiediensten”. Een nuttige beschrijving van relevante communicatiegegevens wordt gegeven in de punten 2.11 tot en met 2.15 van de praktijkrichtlijn inzake bewaring. Hieronder valt de locatie van de gebruiker [van de dienst]. Bij section 21 van Counter-Terrorism and Security Act 2015 [wet uit 2015 inzake contraterorisme en veiligheid] werd de definitie van „relevante” communicatiegegevens uitgebreid tot gegevens waarmee kan worden vastgesteld welk IP-adres, of andere identicator, toebehoort aan de afzender of de ontvanger van een communicatie. Die section is op 13 april 2015 in werking getreden.

16 Onder „relevante communicatiegegevens” wordt niet de inhoud van een communicatie verstaan. „Niettegenstaande het feit dat onder communicatiegegevens niet de inhoud van communicatie wordt verstaan, kunnen zij [toch] zeer onthullend en informatief zijn en derhalve in hoge mate

binnendringen in de persoonlijke levenssfeer van de gebruikers van communicatiediensten” (§ 7 van het vonnis van de Court of Appeal). [Or. 11]

- 17 Het doen van een aanzegging tot bewaring is op grond van de nationale wetgeving niet afhankelijk van een voorafgaande rechterlijke of onafhankelijke goedkeuring. De Secretary of State dient ervan overtuigd te zijn dat het vereiste tot bewaring van relevante communicatiegegevens „noodzakelijk en evenredig” is om een of meer van de redenen waarom relevante communicatiegegevens mogen worden bewaard. Voorschrift 5 zet uiteen waarmee de Secretary of State rekening moet houden alvorens aanzeggingen tot bewaring te doen en vereist dat overleg wordt gepleegd met het betrokken openbare telecommunicatiebedrijf. Nadere details ter zake zijn te vinden in de praktijkrichtlijn inzake bewaring in de punten 3.14 tot en met 3.18 (factoren waarmee de Secretary of State rekening dient te houden) en 3.9 tot en met 3.13 (Overleg met dienstenaanbieders). De Secretary of State dient op grond van section 6 van de Human Rights Act 1998 [Wet uit 1998 inzake de mensenrechten] zijn bevoegdheid krachtens section 1, lid 1, van de DRIPA uit te oefenen in overeenstemming met het EVRM. Het aantal gedane aanzeggingen tot bewaring, de betrokken partijen, de werkingssfeer en de inhoud ervan, alsmede de redenen waarom zij zijn gedaan, worden niet openbaar gemaakt.
- 18 De redenen waarom relevante communicatiegegevens ingevolge section 1, lid 1, van de DRIPA mogen worden bewaard, zijn uiteengezet in section 22, lid 2, onder a) tot en met h), van de RIPA en de Regulation of Investigatory Powers (Communications Data) Order 2010 (SI 2010/480) [verordening uit 2010 inzake het toezicht op onderzoeksbevoegdheden (communicatiegegevens)], zoals gewijzigd bij de Regulation of Investigatory Powers (Communications Data) (Amendment) Order 2015 (SI 2015/228) (hierna: „Verordening”). Het betreft de volgende redenen:
- a) de belangen van de nationale veiligheid;
 - b) het voorkomen of aan het licht brengen van misdrijven of het voorkomen van wanorde;
 - c) de belangen van de economische welvaart van het Verenigd Koninkrijk voor zover deze belangen van belang zijn voor de nationale veiligheid;
 - d) de belangen van de openbare veiligheid;
 - e) het beschermen van de volksgezondheid;
 - f) het opleggen of innen van aan de overheid verschuldigde belastingen, accijnzen, heffingen of andere imposten, bijdragen of kosten;
 - g) het voorkomen, in een noodsituatie, van de dood of verwondingen of ander letsel met betrekking tot de lichamelijke of geestelijke gezondheid van

- een persoon, of het lenigen van verwondingen of letsel met betrekking tot de lichamelijke of geestelijke gezondheid van een persoon;
- h) het ondersteunen van onderzoek naar vermeende gerechtelijke dwalingen; **[Or. 12]**
- i) het ondersteunen van de identificatie van een persoon die niet door een misdrijf om het leven is gebracht of die niet in staat is zichzelf te identificeren door een lichamelijke of geestelijke gesteldheid die niet voortkomt uit een misdrijf (zoals een natuurramp of een ongeval), en met betrekking tot een persoon die is overleden of niet in staat is zichzelf te identificeren, het verkrijgen van informatie verkrijgen over de naaste verwanten of andere aan een dergelijke persoon gelieerde personen, of over de reden van zijn dood of zijn gesteldheid;
- j) het uitoefenen van functies met betrekking tot het reguleren van financiële diensten en markten of met betrekking tot financiële stabiliteit, en
- k) iedere reden die is uiteengezet in een krachtens section 22, lid 2, onder h), van de RIPA gegeven verordening van de Secretary of State.
- 19 Section 1, lid 5, van de DRIPA en voorschrift 4, lid 2, van de Voorschriften bepalen dat de gegevens gedurende een periode van maximaal twaalf maanden mogen worden bewaard. De periode mag niet langer duren dan noodzakelijk en evenredig is (punt 3.27 van de praktijkrichtlijn inzake bewaring). Op grond van voorschrift 6 dient de Secretary of State een aanzegging tot bewaring steeds opnieuw te bekijken.
- 20 Ingevolge section 1, lid 6, van de DRIPA maakt een openbare telecommunicatiebedrijf dat op grond van deze section relevante communicatiegegevens bewaart, de gegevens niet openbaar, behalve in overeenstemming met de (hierna uiteengezette) regels betreffende toegang zoals uiteengezet in hoofdstuk 2, deel 1, van de RIPA of een rechterlijke beslissing of andere rechterlijke goedkeuring of bevelschrift, of zoals bepaald in voorschriften. Voorschriften 7 en 8 voorzien in verplichtingen voor openbare telecommunicatiebedrijven die relevante communicatiegegevens bewaren, waaronder het veiligstellen van de integriteit en veiligheid ervan, het beschermen tegen onvoorziene of onwettige vernietiging, onvoorziene verlies of verandering, of het niet-goedgekeurd of onwettig bewaren, verwerken, raadplegen of openbaar maken ervan; het vernietigen van de gegevens om het onmogelijk te maken ze te raadplegen als de bewaring van de gegevens niet langer is toegestaan; en het opzetten van passende veiligheidssystemen (zie ook de punten 6.1 tot en met 6.47 van de praktijkrichtlijn inzake bewaring).
- 21 Voorschrift 9 belast de Information Commissioner [<https://ico.org.uk>] met de controle op de naleving van deze Regulations uit 2014 (zie de punten 7.1 tot en met 7.11 van de praktijkrichtlijn inzake bewaring).

Nationale wetgeving: toegang

- 22 Toegang tot bewaarde gegevens wordt geregeld in a) hoofdstuk 2 van deel II van de RIPA; b) de Verordening; en c) de Acquisition and Disclosure of Communications Data Code of Practice [praktijkrichtlijn inzake de verwerving en de openbaarmaking van communicatiegegevens] (hierna: „praktijkrichtlijn inzake verwerving”). **[Or. 13]**
- 23 De overheid kan krachtens section 22, lid 4, van de RIPA aanbieders van communicatiediensten door middel van een aanzegging verplichten om haar communicatiegegevens mede te delen. De vorm en de inhoud van dergelijke aanzeggingen wordt geregeld door section 23, lid 2, van de RIPA. Een dergelijke aanzegging geldt voor een beperkte tijd met bepalingen aangaande annulering en hernieuwing (section 23, leden 4 tot en met 8, RIPA; praktijkrichtlijn inzake verwerving, punten 3.51 tot en met 3.64).
- 24 De verwerving van communicatiegegevens moet noodzakelijk en evenredig zijn ten aanzien van een of meer van de in section 22 van de RIPA opgesomde redenen, die overeenkomen met de hierboven uiteengezette redenen voor het bewaren van relevante communicatiegegevens (section 22, leden 1, 2 en 5, van de RIPA; praktijkrichtlijn inzake verwerving, punt 2.2. Aanwijzingen met betrekking tot noodzakelijkheid en evenredigheid zijn te vinden in de punten 2.5 tot en met 2.9 en 2.36 tot en met 2.45 van de praktijkrichtlijn inzake verwerving).
- 25 Er dient speciale aandacht te worden besteed aan de noodzakelijkheid en de evenredigheid wanneer de communicatiegegevens betrekking hebben op een persoon die beroepshalve omgaat met informatie waarvoor het beroepsgeheim geldt of met anderszins vertrouwelijke informatie (zoals artsen, advocaten, journalisten, parlementsleden, en bedienaars van de godsdienst) (praktijkrichtlijn inzake verwerving, punten 3.72 tot en met 3.77). Een rechterlijke beslissing is vereist in het specifieke geval dat om communicatiegegevens wordt verzocht om een journalistieke bron te achterhalen (praktijkrichtlijn inzake verwerving, punten 3.78 tot en met 3.84). Toegang door de lokale overheid vereist rechterlijke goedkeuring (praktijkrichtlijn inzake verwerving, punten 3.85 tot en met 3.87). Geen rechterlijke of onafhankelijke goedkeuring is vereist om toegang te verkrijgen tot communicatiegegevens waarvoor het beroepsgeheim geldt of communicatiegegevens met betrekking tot artsen, parlementsleden en bedienaars van de godsdienst. **[Or. 14]**
- 26 Voordat de overheid om communicatiegegevens kan verzoeken, moet de aangewezen persoon in de relevante overheidsdienst toestemming hebben gegeven. Een aangewezen persoon is iemand die een voorgeschreven ambt, rang of positie bekleedt in een relevante overheidsdienst die is aangewezen om op grond van de Verordening communicatiegegevens te verwerven. In section 3 van de praktijkrichtlijn inzake verwerving zijn de procedures uiteengezet met

betrekking tot het doen van het verzoek, hetgeen de aangewezen persoon in aanmerking dient te nemen en het besluit om een aanzegging te doen.

- 27 Artikel 6 van de Verordening beperkt de redenen waarom bepaalde overheidsdiensten communicatiegegevens kunnen eisen. De aangewezen persoon kan slechts rekening houden met de noodzakelijkheid op gronden die vallen onder hun bevoegdheid als overheidsinstantie en slechts met betrekking tot zaken die vallen onder de wettelijke of bestuurlijke taak van de desbetreffende overheidsinstantie.
- 28 Communicatiegegevens die worden verkregen op grond van de bepalingen van de RIPA, en alle afschriften, uittreksels en samenvattingen ervan, dienen veilig te worden bewaard en opgeslagen. De eisen van de Data Protection Act [wet op de gegevensbescherming] (hierna: „DPA”), waarbij de gegevensbeschermingsrichtlijn werd omgezet, dienen te worden nageleefd (praktijkrichtlijn inzake verwerving, section 7). Het vrijgeven aan buitenlandse overheden wordt geregeld door section 6 en bijlage 5 van de DPA, welke voorzien in onafhankelijk toezicht door de Information Commissioner, en door het Achtste beginsel inzake gegevensbescherming in bijlage 1 bij de DPA dat samen met de uitzonderingen in bijlage 4 bij de DPA, de artikelen 25 en 26 van de gegevensbeschermingsrichtlijn betreffende de overdracht van persoonsgegevens aan derde landen omzet (praktijkrichtlijn inzake verwerving, punten 7.18 tot en met 7.22). Op grond van section 28 van de Data Protection Act 1998 kan de Secretary of State echter een nationaal veiligheidscertificaat afgeven, waarmee gegevens van de bepalingen van de wet worden uitgezonderd. Een dergelijk certificaat is afgegeven voor de veiligheids- en inlichtingendiensten van het Verenigd Koninkrijk.
- 29 De RIPA voorziet in een Interception of Communications Commissioner [<http://www.iocco-uk.info>] wiens opdracht luidt onafhankelijk toezicht te houden op de uitoefening en de vervulling van de bevoegdheden en de verplichtingen van hoofdstuk II van deel 1 van de RIPA (praktijkrichtlijn inzake verwerving, sections 8 en 9). De Commissioner houdt geen toezicht op het gebruik van section 1 van de DRIPA. Er is bepaald dat aan zowel het publiek als het parlement regelmatig wordt gerapporteerd (sections 57, lid 2, en 58 RIPA) en de documentatie en rapportering door de overheid is geregeld (praktijkrichtlijn inzake verwerving, punten 6.1 tot en met 6.8). Indien men meent dat gegevens op onjuiste wijze zijn verworven, kan klacht worden neergelegd bij het Investigatory Powers Tribunal [<http://www.ipt-uk.com/>] (section 65 RIPA). De Commissioner is niet bevoegd om een zaak naar het Tribunal te verwijzen. De Commissioner kan een persoon slechts informeren over een vermoedelijk onwettig gebruik van bevoegdheden als hij kan „vaststellen dat een individu is geraakt door een opzettelijk of roekeloos verzuim”. Zelfs als de Commissioner ervan overtuigd is dat sprake is van een opzettelijk of roekeloos verzuim, is het hem niet toegestaan dit openbaar te maken als door openbaarmaking de nationale veiligheid in het gedrang zou komen (praktijkrichtlijn inzake verwerving, § 8.3).

Relevante bepalingen van Unierecht

- 30 Handvest, artikelen 7, 8, 51 en 52 en de officiële toelichtingen bij het Handvest. **[Or. 15]**
- 31 Richtlijn betreffende privacy en elektronische communicatie (2002/58/EG), artikelen 1, lid 3, 5, 6, 9 en 15.
- 32 Gegevensbeschermingsrichtlijn (95/46/EG), artikelen 3, lid 2, en 13.
- 33 Richtlijn betreffende de bewaring van gegevens (2006/24/EG), artikelen 3 tot en met 9.

Hoofdpunten uit het betoog van partijen

Verzoekende partijen

Eerste vraag

- 34 De verzoekende partijen voeren aan dat het Hof van Justitie in het arrest in de zaak Digital Rights Ireland (waaronder in het bijzonder de punten 60 tot en met 62 ervan) dwingende vereisten van Unierecht heeft vastgesteld, waaraan de nationale wetgeving van lidstaten dient te voldoen als in die nationale wetgeving wordt voorzien in de bewaring van communicatiegegevens.
- 35 Het Hof van Justitie heeft geoordeeld dat wetgeving op grond waarvan commerciële communicatiebedrijven massaal alle communicatiegegevens dienen te bewaren om te zorgen dat die gegevens toegankelijk zijn voor overheidsdiensten, een bijzonder ernstige inmenging in de in de artikelen 7 en 8 van het Handvest neergelegde grondrechten vormt (punten 25 tot en met 27 en 32 tot en met 37). De inmenging voldoet aan een doel van algemeen belang, en de vraag is of zij evenredig is (punten 41 tot en met 45). Vanwege het belang van gegevensbescherming voor de persoonlijke levenssfeer, en de omvang en ernst van de inmenging, dient de evenredigheidstoetsing strikt te zijn. De uitzonderingen op de bescherming van persoonsgegevens en de beperkingen ervan dienen binnen de grenzen van het strikt noodzakelijke te blijven (punten 47, 48 en 52). Om aan de noodzakelijkheidstoets te voldoen, dient de wetgeving te voorzien in duidelijke en precieze regels die de werkingssfeer en de toepassing van de betrokken maatregel regelen en minimale vereisten opleggen, zodat de personen wier gegevens zijn bewaard over voldoende garanties beschikken dat hun persoonsgegevens doeltreffend worden beschermd tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en elk onrechtmatig gebruik van deze gegevens (punt 54). **[Or. 16]**

- 36 Het Hof van Justitie heeft de noodzakelijkheidstoets vervolgens toegepast in het kader van een Unierechtelijke algemene bewaarregeling voor communicatiegegevens (de richtlijn betreffende de bewaring van gegevens). Het Hof stelde op een aantal onderdelen vast dat de wetgeving tekortschoot met betrekking tot minimale waarborgen. In het bijzonder was er geen sprake van a) een objectief criterium om de toegang tot de gegevens en het gebruik ervan te beperken tot zaken die voldoende ernstig zijn om de inmenging te rechtvaardigen (punt 60); b) materiële en procedurele voorwaarden om het doel van toegang en gebruik strikt te beperken tot het opsporen van nauwkeurig omschreven ernstige strafbare feiten (punt 61); c) toegang die was onderworpen aan enige voorafgaande controle door een rechter of een onafhankelijke administratieve instantie (punt 62), en d) een vereiste dat de gegevens op het grondgebied van de Unie moeten worden bewaard (punt 68).
- 37 Een algemene bewaarregeling voor communicatiegegevens in het *nationale recht* die afwijkt van de rechten en verplichtingen in de artikelen 5, 6 en 9 van de richtlijn betreffende privacy en elektronische communicatie dient te voldoen aan de in artikel 15, lid 1, van die richtlijn genoemde gronden voor afwijking. Voorts vormt een algemene bewaarregeling een bijzonder ernstige inmenging in de in de artikelen 7 en 8 van het Handvest neergelegde grondrechten. Om niet met die rechten in strijd te zijn, dient een dergelijke regeling eveneens de door het Hof van Justitie vastgestelde minimale waarborgen met betrekking tot de toegang tot gegevens te bevatten. Een rechtmatige regeling inzake toegang is een voorafgaande voorwaarde voor een wet op basis waarvan ieders gegevens mogen worden bewaard. Tenzij sprake is van een rechtmatig kader voor toegang en gebruik, zouden de gegevens in het geheel niet mogen worden bewaard. De regering van het Verenigd Koninkrijk kan derhalve niet aanvoeren dat toegang tot gegevens buiten de werkingssfeer van het Unierecht valt. Het is voldoende (hetgeen de regering van het Verenigd Koninkrijk aanvaardt) dat nationale regelingen inzake de bewaring van gegevens onder de werkingssfeer van het Unierecht vallen.

Tweede vraag

- 38 De verzoekende partijen voeren aan dat de uitspraak van het Hof van Justitie in de zaak Digital Rights Ireland de werking van artikel 7 en/of artikel 8 van het Handvest niet ruimer maakt dan de werking van artikel 8 EVRM zoals vastgesteld in de rechtspraak van het EHRM.
- 39 Het EHRM zou bij toepassing van artikel 8 EVRM dezelfde aanpak hebben gehanteerd en tot dezelfde conclusies zijn gekomen als het Hof van Justitie. Het EHRM heeft bijvoorbeeld het volgende benadrukt: a) de beperkte beoordelingsruimte van de nationale overheid wanneer sprake is van een inmenging in het recht op gegevensbescherming, zelfs wanneer het gaat om strafbare feiten en openbare veiligheid; b) de noodzaak voor minimale waarborgen ter bescherming tegen het risico van misbruik of onrechtmatige toegang tot

gegevens om te zorgen dat de inmenging „overeenkomstig de wet” gebeurt en evenredig is; c) de precieze minimale waarborgen hangen van de omstandigheden af, en d) in sommige omstandigheden valt onder de noodzakelijke minimale waarborgen de voorafgaande onafhankelijke goedkeuring van toegang tot gegevens en de beperking van de toegang tot bepaalde ernstige strafbare feiten. **[Or. 17]**

- 40 Zelfs als het Hof van Justitie in het arrest Digital Rights Ireland (in tegenstelling tot het hiervoor aangevoerde) de werking van de artikelen 7 en 8 van het Handvest niet heeft verruimd ten opzichte van de werking van artikel 8 EVRM, had het Hof van Justitie het recht om dat te doen, in het bijzonder in omstandigheden waarin artikel 8 van het Handvest niet identiek is aan artikel 8 EVRM.

Eerste en tweede interveniënt

- 41 Open Rights Group en Privacy International bekrachtigen en aanvaarden de standpunten van de verzoekende partijen en brengen ook de volgende punten naar voren. Ten eerste voeren zij aan dat het onderscheppen en bewaren van gegevens op zichzelf al aanleiding geeft tot een zeer ernstige inmenging in de door de artikelen 7 en 8 van het Handvest beschermde grondrechten, ongeacht of vervolgens wordt verzocht om er toegang toe te krijgen of daarom inderdaad zou kunnen worden verzocht. Een nationale regeling die in feite de bepalingen van de gegevensbeschermingsrichtlijn weergeeft, met een lange reeks van gronden voor het toestaan van bewaring, vormt een dergelijke ernstige inmenging. Een dergelijke regeling zou het bij Unierecht vereiste hoge niveau van bescherming van grondrechten met betrekking tot de verwerking van persoonsgegevens ondermijnen, alsook het evenredigheidsbeginsel.
- 42 Zij voeren voorts aan dat, indien de bewaring plaatsvindt op een allesomvattende of algemene schaal of zonder aanzien des persoons, zij intrinsiek onevenredig is en een ongerechtvaardigde inmenging in die rechten vormt. Zij verlaten zich in dit opzicht in het bijzonder op de beslissing van het Hof van Justitie in zowel de zaak Digital Rights Ireland als zaak C-362/14, Maximilian Schrems (ECLI:EU:C:2015:650) (hierna: „Schrems”).

Derde interveniënt

- 43 The Law Society of England and Wales voert aan dat a) het Hof van Justitie in het arrest Digital Rights Ireland inderdaad minimumvereisten heeft vastgesteld waaraan nationale wetgeving die de toegang tot bewaarde gegevens regelt, dient te voldoen, en b) iedere regeling tot verplichte bewaring van gegevens vergezeld dient te gaan van passende beperkingen van de toegang tot informatie die is beschermd door het wettelijke beroepsgeheim. Een nationale wettelijke regeling die geen uitzondering of beperkingen van de toegang tot gegevens die worden beschermd door het wettelijke beroepsgeheim, bevat, zou in strijd zijn met de

vereisten van Unierecht, zoals uiteengezet in het arrest Digital Rights Ireland. **[Or. 18-19]**

Secretary of State

Eerste vraag

- 44 De Secretary of State voert aan dat het Hof van Justitie in zijn uitspraak in de zaak Digital Rights Ireland (waaronder in het bijzonder de punten 60 tot en met 62 ervan) geen verplichte vereisten van Unierecht heeft vastgesteld waaraan de regelingen van de lidstaten met betrekking tot de toegang tot bewaarde gegevens moeten voldoen.
- 45 Het Hof van Justitie sprak zich uit over een verzoek om een prejudiciële beslissing betreffende de geldigheid van de richtlijn betreffende de bewaring van gegevens. Het Hof werd niet verzocht om een beslissing over de geldigheid van nationale wetgeving, en het sprak zich daarover ook niet uit.
- 46 De vraag die aan het Hof werd voorgelegd betrof de toelaatbaarheid voor de Uniewetgever om de bij de richtlijn betreffende de bewaring van gegevens opgezette geharmoniseerde, verplichte Unierechtelijke gegevensbewaarregeling aan te nemen wanneer in de Uniewetgeving in kwestie geen waarborgen waren opgenomen om bewaarde gegevens te beschermen tegen het risico van misbruik en onrechtmatige toegang. Het Hof van Justitie heeft het type waarborgen vastgesteld dat in de geharmoniseerde Unieregeling ontbrak. Het had niet de bedoeling om materiële vereisten vast te stellen met betrekking tot de toegang tot gegevens die in iedere nationale regeling moeten worden opgenomen.
- 47 Het Hof van Justitie beschikte niet over inhoudelijk bewijs van de aard en de werkingssfeer van de nationale regelingen van de lidstaten met betrekking tot de bewaring van gegevens en de toegang ertoe en in het bijzonder de aard en de werkingssfeer van de waarborgen voor de bescherming van de persoonlijke levenssfeer. Het kon dergelijke zaken derhalve niet in overweging nemen.
- 48 Voorts heeft het Hof niet onderzocht, of en in welke mate nationale regels met betrekking tot de toegang tot communicatiegegevens door rechtshandavingsinstanties uitvoering geven aan Unierecht. Noch richtlijn 95/45/EG (de gegevensbeschermingsrichtlijn), noch richtlijn 2002/58/EG (de richtlijn betreffende privacy en elektronische communicatie) reguleert de activiteiten van lidstaten met betrekking tot openbare veiligheid, defensie, staatsveiligheid of strafrecht, noch gebeurt dit door enige andere bepaling van Unierecht (behalve in de specifieke context van grensoverschrijdende samenwerking in de Unie). Het Handvest, waarop de uitspraak in de zaak Digital Rights Ireland is gebaseerd, is slechts op lidstaten van toepassing, wanneer zij het Unierecht „uitvoeren”. Het Hof van Justitie is niet nagegaan of bij nationale regelingen met betrekking tot de toegang tot bewaarde gegevens Unierecht wordt

uitgevoerd. Het kon derhalve nooit de bedoeling hebben gehad om verplichte regels vast te stellen die op lidstaten van toepassing zijn. **[Or. 19-20]**

Tweede vraag

- 49 De Secretary of State voert aan dat het Hof van Justitie niet de bedoeling had om de werkingssfeer van de artikelen 7 en 8 van het Handvest te verruimen ten opzichte van de inhoud van artikel 8, lid 2, EVRM. Integendeel, het Hof van Justitie verwees expliciet naar de rechtspraak van het EHRM en heeft die ook toegepast. Voorts vereisen artikel 15, lid 1, van de richtlijn betreffende privacy en elektronische communicatie en de artikelen 7 en 8 van het Handvest dat lidstaten voldoen aan artikel 8, lid 2, zoals uitgelegd door het EHRM.
- 50 Op grond van de rechtspraak van het EHRM wordt geen voorafgaande onafhankelijke of rechterlijke goedkeuring vereist. Ook wordt niet vereist dat het bewaren van gegevens en de toegang daartoe worden beperkt tot ernstige strafbare feiten. Dit vormt derhalve een nadere aanwijzing dat het Hof van Justitie met zijn verwijzing naar dergelijke zaken niet de bedoeling had om dwingende vereisten voor de nationale regelingen van lidstaten vast te leggen.

VERZOEK OM EEN VERSNELDE BEHANDELING

- 51 De verwijzende rechter is zich bewust van de omvang en het belang van andere zaken die bij het Hof van Justitie aanhangig zijn. Hij hoopt echter dat het Hof positief zal staan tegenover het verzoek van deze rechter om een versnelde behandeling van deze verwijzing. Wij hopen ook dat het mogelijk zal zijn deze verwijzing te voegen met die van het Kammarrätt i Stockholm, die nu voorligt als zaak C-203/15, Tele2 Sverige AB, of de opdracht te geven beide zaken gezamenlijk te behandelen.
- 52 In dit verband wijst de verwijzende rechter op het feit dat de DRIPA een vervalbepaling bevat die tot gevolg heeft dat de wet op 31 december 2016 zal vervallen. Het concrete gevolg van de uitspraak van het Hof van Justitie in de zaak Digital Rights Ireland zal echter cruciaal zijn voor de geldigheid van alle toekomstige wetgeving die de lidstaten op dit gebied aannemen. Bovendien is het, gelet op het onderwerp, onwenselijk dat onzekerheid blijft bestaan over het gevolg van die uitspraak. Om deze redenen wordt om een versnelde behandeling verzocht. **[Or. 20]**

BEGELEIDENDE STUKKEN

- 53 Dit verzoek om een prejudiciële beslissing gaat vergezeld van [afschriften van de uitspraak van de Court of Appeal van 20 november 2015, de uitspraak van de High Court of Justice, Queen's Bench Division, Divisional Court, van 17 juli

2015 en van de wetgeving van het Verenigd Koninkrijk waarnaar wordt verwezen in de bijlage bij deze beslissing] **[Or. 22]** [*omissis*]

[*omissis*]