



## Jurisprudentie

ARREST VAN HET HOF (Grote kamer)

6 oktober 2020\*

„Prejudiciële verwijzing – Verwerking van persoonsgegevens in de sector elektronische communicatie – Aanbieders van elektronischecommunicatiediensten – Algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens – Bescherming van de nationale veiligheid – Richtlijn 2002/58/EG – Werkingsfeer – Artikel 1, lid 3, en artikel 3 – Vertrouwelijk karakter van elektronische communicatie – Bescherming – Artikel 5 en artikel 15, lid 1 – Handvest van de grondrechten van de Europese Unie – Artikelen 7, 8 en 11 en artikel 52, lid 1 – Artikel 4, lid 2, VEU”

In zaak C-623/17,

betreffende een verzoek om een prejudiciële beslissing krachtens artikel 267 VWEU, ingediend door de Investigatory Powers Tribunal (rechter die toezicht uitoefent op de onderzoeksbevoegdheden van de overheid, Verenigd Koninkrijk) bij beslissing van 18 oktober 2017, ingekomen bij het Hof op 31 oktober 2017, in de procedure

**Privacy International**

tegen

**Secretary of State for Foreign and Commonwealth Affairs,**

**Secretary of State for the Home Department,**

**Government Communications Headquarters,**

**Security Service,**

**Secret Intelligence Service,**

wijst

HET HOF (Grote kamer),

samengesteld als volgt: K. Lenaerts, president, R. Silva de Lapuerta, vicepresident, J.-C. Bonichot, A. Arabadjiev, A. Prechal, M. Safjan, P. G. Xuereb en L. S. Rossi, kamerpresidenten, J. Malenovský, L. Bay Larsen, T. von Danwitz (rapporteur), C. Toader, K. Jürimäe, C. Lycourgos en N. Piçarra, rechters,

advocaat-generaal: M. Campos Sánchez-Bordona,

griffier: C. Strömholm, administrateur,

\* Procestaal: Engels.

gezien de stukken en na de terechtzitting op 9 en 10 september 2019,

gelet op de opmerkingen van:

- Privacy International, vertegenwoordigd door B. Jaffey en T. de la Mare, QC, D. Cashman, solicitor, en H. Roy, advocaat,
- de regering van het Verenigd Koninkrijk, vertegenwoordigd door Z. Lavery, D. Guðmundsdóttir en S. Brandon als gemachtigden, bijgestaan door G. Facenna en D. Beard, QC, en door C. Knight en R. Palmer, barristers,
- de Belgische regering, vertegenwoordigd door P. Cottin en J.-C. Halleux als gemachtigden, bijgestaan door J. Vanpraet, advocaat, en E de Lophem, avocat,
- de Tsjechische regering, vertegenwoordigd door M. Smolek, J. Vláčil en O. Serdula als gemachtigden,
- de Duitse regering, aanvankelijk vertegenwoordigd door M. Hellmann, R. Kanitz, D. Klebs en T. Henze, vervolgens door J. Möller, M. Hellmann, R. Kanitz en D. Klebs als gemachtigden,
- de Estse regering, vertegenwoordigd door A. Kalbus als gemachtigde,
- de Ierse regering, vertegenwoordigd door M. Browne, G. Hodge en A. Joyce als gemachtigden, bijgestaan door D. Fennelly, barrister,
- de Spaanse regering, aanvankelijk vertegenwoordigd door L. Aguilera Ruiz en M. J. García-Valdecasas Dorrego, vervolgens door L. Aguilera Ruiz als gemachtigden,
- de Franse regering, aanvankelijk vertegenwoordigd door E. de Moustier, E. Armoët, A.-L. Desjonquères, F. Alabrune, D. Colas en D. Dubois, vervolgens door E. de Moustier, E. Armoët, A.-L. Desjonquères, F. Alabrune en D. Dubois als gemachtigden,
- de Cypriotische regering, vertegenwoordigd door E. Symeonidou en E. Neofytou als gemachtigden,
- de Letse regering, aanvankelijk vertegenwoordigd door V. Soņeca en I. Kucina, vervolgens door V. Soņeca als gemachtigden,
- de Hongaarse regering, aanvankelijk vertegenwoordigd door G. Koós, M. Z. Fehér, G. Tornyai en Z. Wagner, vervolgens door G. Koós en M. Z. Fehér als gemachtigden,
- de Nederlandse regering, vertegenwoordigd door C.S. Schillemans en M.K. Bulterman als gemachtigden,
- de Poolse regering, vertegenwoordigd door B. Majczyna, J. Sawicka en M. Pawlicka als gemachtigden,
- de Portugese regering, vertegenwoordigd door L. Inez Fernandes, M. Figueiredo en F. Aragão Homem als gemachtigden,
- de Zweedse regering, aanvankelijk vertegenwoordigd door A. Falk, H. Shev, C. Meyer-Seitz, L. Zettergren en A. Alriksson, vervolgens door H. Shev, C. Meyer-Seitz, L. Zettergren en A. Alriksson als gemachtigden,

- de Noorse regering, vertegenwoordigd door T.B. Leming, M. Emberland en J. Vangsnes als gemachtigden,
- de Europese Commissie, aanvankelijk vertegenwoordigd door H. Kranenborg, M. Wasmeier, D. Nardi en P. Costa de Oliveira, vervolgens door H. Kranenborg, M. Wasmeier en D. Nardi als gemachtigden,
- de Europese Toezichthouder voor gegevensbescherming, vertegenwoordigd door T. Zerdick en A. Buchta als gemachtigden,

gehoord de conclusie van de advocaat-generaal ter terechtzitting van 15 januari 2020,

het navolgende

### Arrest

- 1 Het verzoek om een prejudiciële beslissing betreft de uitlegging van artikel 1, lid 3, en artikel 15, lid 1, van richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PB 2002, L 201, blz. 37), zoals gewijzigd bij richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 (PB 2009, L 337, blz. 11) (hierna: „richtlijn 2002/58”), gelezen in het licht van artikel 4, lid 2, VEU en de artikelen 7 en 8 en artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie (hierna: „Handvest”).
- 2 Dit verzoek is ingediend in het kader van een geding tussen Privacy International enerzijds en de Secretary of State for Foreign and Commonwealth Affairs (minister van Buitenlandse Zaken en Gemenebestzaken, Verenigd Koninkrijk), de Secretary of State for the Home Department (minister van Binnenlandse Zaken, Verenigd Koninkrijk), de Government Communications Headquarters (hoofdkwartier voor regeringscommunicatie, Verenigd Koninkrijk; hierna: „GCHQ”), de Security Service (veiligheidsdienst, Verenigd Koninkrijk; hierna: „MI5”) en de Secret Intelligence Service (geheime inlichtingendienst, Verenigd Koninkrijk; hierna: „MI6”) anderzijds, over de rechtmatigheid van een wettelijke regeling die de verwerving en het gebruik van bulkcommunicatiegegevens door de veiligheids- en inlichtingendiensten toestaat.

### Toepasselijke bepalingen

#### *Unierecht*

##### *Richtlijn 95/46*

- 3 Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PB 1995, L 281, blz. 31) is met ingang van 25 mei 2018 ingetrokken bij verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016

betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG (PB 2016, L 119, blz. 1). Artikel 3 („Werkingsfeer”) van die richtlijn luidde als volgt:

„1. De bepalingen van deze richtlijn zijn van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede op de niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

2. De bepalingen van deze richtlijn zijn niet van toepassing op de verwerking van persoonsgegevens:

- die met het oog op de uitoefening van niet binnen de werkingssfeer van het gemeenschapsrecht vallende activiteiten geschiedt zoals die bedoeld in de titels V en VI [VEU] en in ieder geval verwerkingen die betrekking hebben op de openbare veiligheid, defensie, de veiligheid van de staat (waaronder de economie van de staat, wanneer deze verwerkingen in verband staan met vraagstukken van staatsveiligheid), en de activiteiten van de staat op strafrechtelijk gebied;
- die door een natuurlijk persoon in activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden wordt verricht.”

#### *Richtlijn 2002/58*

4 In de overwegingen 2, 6, 7, 11, 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] van toepassing op vraagstukken met betrekking tot de bescherming van fundamentele rechten en vrijheden in verband met niet onder het [Unierecht] 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 [op 4 november 1950 te Rome ondertekende] Europese 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.

[...]

- (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. Indien zulks nodig is voor het doeltreffender maken van het op hun verzoek doorgeven van voor het publiek toegankelijke informatie aan andere afnemers van de dienst, laat deze richtlijn onverlet dat deze informatie langer blijft opgeslagen mits ze in ieder geval onbeperkt voor het publiek toegankelijk is en gegevens inzake de individuele abonnees of gebruikers die om deze informatie verzoeken, gewist worden.

[...]

- (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. Verkeersgegevens die worden gebruikt voor de marketing van communicatiediensten [...] moeten ook worden gewist of anoniem gemaakt [...].

[...]

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

5 Artikel 1 („Werkingsfeer 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 [Europese Unie].

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 [VWEU] 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.”

6 Artikel 2 („Definities”) van die richtlijn luidt:

„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, blz. 33)] van toepassing.

Daarnaast wordt in deze richtlijn verstaan onder:

- a) ‚gebruiker’: natuurlijke persoon die gebruikmaakt van een openbare elektronischecommunicatiedienst voor particuliere of zakelijke doeleinden zonder noodzakelijkerwijze op die dienst te zijn geabonneerd;
- 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;

[...]”

7 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 [Unie], met inbegrip van openbare communicatienetwerken die systemen voor gegevensverzameling en identificatie ondersteunen.”

8 In artikel 5 („Vertrouwelijk karakter van de communicatie”) van die richtlijn 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 elektronisch communicatienetwerk, 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 elektronischcommunicatienetwerk 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 elektronischcommunicatiedienst mag ten behoeve van de marketing van elektronischcommunicatiediensten 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 elektronischcommunicatiediensten 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 Artikel 9 („Andere locatiegegevens dan verkeersgegevens”) van die richtlijn bepaalt in lid 1:

„Wanneer andere locatiegegevens dan verkeersgegevens die betrekking hebben op gebruikers of abonnees van elektronischcommunicatienetwerken 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 anders 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 richtlijn 2002/58 bepaalt in lid 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, d.w.z. de staatsveiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van ongevoegd gebruik van het elektronische communicatiesysteem 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 [Unierecht], met inbegrip van de beginselen als bedoeld in artikel 6, leden 1 en 2, van het Verdrag betreffende de Europese Unie.”

#### *Verordening 2016/679*

- 12 Artikel 2 van verordening 2016/679 bepaalt:

„1. Deze verordening is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

2. Deze verordening is niet van toepassing op de verwerking van persoonsgegevens:

- a) in het kader van activiteiten die buiten de werkingssfeer van het Unierecht vallen;
- b) door de lidstaten bij de uitvoering van activiteiten die binnen de werkingssfeer van titel V, hoofdstuk 2, VEU vallen;

[...]

d) door de bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.

[...]”

- 13 Artikel 4 van die verordening luidt:

„Voor de toepassing van deze verordening wordt verstaan onder:

[...]

2) ‚verwerking’: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;



[...]”

14 In artikel 23, lid 1, van dezelfde verordening staat:

„De reikwijdte van de verplichtingen en rechten als bedoeld in de artikelen 12 tot en met 22 en artikel 34, alsmede in artikel 5 kan, voor zover de bepalingen van die artikelen overeenstemmen met de rechten en verplichtingen als bedoeld in de artikelen 12 tot en met [22], worden beperkt door middel van Unierechtelijke of lidstaatrechtelijke bepalingen die op de verwerkingsverantwoordelijke of de verwerker van toepassing zijn, op voorwaarde dat die beperking de wezenlijke inhoud van de grondrechten en fundamentele vrijheden onverlet laat en in een democratische samenleving een noodzakelijke en evenredige maatregel is ter waarborging van:

- a) de nationale veiligheid;
- b) landsverdediging;
- c) de openbare veiligheid;
- d) de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid;
- e) andere belangrijke doelstellingen van algemeen belang van de Unie of van een lidstaat, met name een belangrijk economisch of financieel belang van de Unie of van een lidstaat, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid;
- f) de bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures;
- g) de voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes voor gereguleerde beroepen;
- h) een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van het openbaar gezag in de in de punten a), tot en met e) en punt g) bedoelde gevallen;
- i) de bescherming van de betrokkene of van de rechten en vrijheden van anderen;
- j) de inning van civielrechtelijke vorderingen.”

15 Artikel 94, lid 2, van verordening 2016/679 bepaalt:

„Verwijzingen naar de ingetrokken richtlijn gelden als verwijzingen naar deze verordening. Verwijzingen naar de groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens, die bij artikel 29 van [richtlijn 95/46] is opgericht, gelden als verwijzingen naar het bij deze verordening opgerichte Europees Comité voor gegevensbescherming.”

### *Recht van het Verenigd Koninkrijk*

- 16 Section 94 („Aanwijzingen in het belang van de nationale veiligheid etc.”) van de Telecommunications Act 1984 (Telecommunicatiewet van 1984; hierna: „wet van 1984”), in de op de feiten van het hoofdingeving toepasselijke versie, bepaalt:

„(1) Na overleg met een persoon op wie deze section van toepassing is, kan de Secretary of State [minister] aan die persoon de algemene aanwijzingen geven die hij noodzakelijk acht in het belang van de nationale veiligheid of de betrekkingen met de regering van een land of gebied buiten het Verenigd Koninkrijk.

(2) Indien de Secretary of State zulks noodzakelijk acht in het belang van de nationale veiligheid of de betrekkingen met de regering van een land of gebied buiten het Verenigd Koninkrijk, kan hij, na overleg met een persoon op wie deze section van toepassing is, die persoon een aanwijzing geven om (naargelang van de omstandigheden van het geval) de in die aanwijzing gespecificeerde handeling te verrichten dan wel daarvan af te zien.

(2A) De Secretary of State kan alleen dan een aanwijzing krachtens lid 1 of lid 2 geven, indien hij van oordeel is dat het door die aanwijzing voorgeschreven gedrag in verhouding staat tot het ermee beoogde doel.

(3) Een persoon op wie deze section van toepassing is, dient alle aanwijzingen op te volgen die hem door de Secretary of State krachtens deze section worden gegeven, niettegenstaande eventuele andere verplichtingen die op hem rusten ingevolge deel 1 of hoofdstuk 1 van deel 2 van de Communications Act 2003 [Communicatiewet 2003], en, in het geval van een aanwijzing gegeven aan een exploitant van een openbaar elektronischcommunicatienetwerk, ongeacht of deze exploitant die aanwijzing ontvangt in een andere hoedanigheid dan die van exploitant van een dergelijk netwerk.

(4) De Secretary of State deponeert bij elk van de kamers van het parlement een afschrift van elke krachtens deze section gegeven aanwijzing, tenzij hij van oordeel is dat openbaarmaking van de aanwijzing de nationale veiligheid of de betrekkingen met de regering van een land of gebied buiten het Verenigd Koninkrijk, dan wel de zakelijke belangen van een persoon zou schaden.

(5) Het is een persoon verboden om enige informatie betreffende overeenkomstig deze section genomen maatregelen openbaar te maken indien de Secretary of State aan hem heeft meegedeeld dat openbaarmaking van die informatie naar zijn oordeel de nationale veiligheid of de betrekkingen met de regering van een land of gebied buiten het Verenigd Koninkrijk, dan wel de zakelijke belangen van een ander persoon zou schaden. In dat geval kan die persoon ook niet krachtens de wet of anderszins worden verplicht om die informatie openbaar te maken.

[...]

(8) Deze section is van toepassing op de [Office of communications (OFCOM)] en op exploitanten van openbare elektronischcommunicatienetwerken.”

- 17 In section 21, leden 4 en 6, van de Regulation of Investigatory Powers Act 2000 (wet van 2000 houdende regeling van de onderzoeksbevoegdheden; hierna: „RIPA”) is bepaald:

„(4) [...] onder ‚communicatiegegevens’ [wordt] verstaan:

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

- (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 postdiensten of van een telecommunicatiedienst, of
  - (ii) van een onderdeel van een telecommunicatiesysteem in het kader van de aanbieder van of het gebruik door een persoon van een telecommunicatiedienst;
- (c) informatie die niet onder (a) of (b) valt en die door een persoon die een post- of telecommunicatiedienst aanbiedt, wordt bewaard of verkregen met betrekking tot personen aan wie hij de dienst aanbiedt.

[...]

- (6) [...] onder ‚verkeersgegevens‘ met betrekking tot een communicatie [wordt] verstaan:
  - (a) alle gegevens die een persoon, apparaat of locatie identificeren waarnaar of waarvandaan een communicatie wordt of kan worden verzonden, of die tot doel hebben deze persoon, dit apparaat of deze locatie te identificeren;
  - (b) alle gegevens aan de hand waarvan de apparatuur door middel waarvan de communicatie wordt of kan worden verzonden, wordt geïdentificeerd of geselecteerd, of die ertoe strekken deze apparatuur te identificeren of te selecteren;
  - (c) alle gegevens die signalen bevatten voor de bediening van de apparatuur die wordt gebruikt in een telecommunicatiesysteem voor het verzenden van een communicatie, en
  - (d) alle gegevens die de informatie identificeren die deel uitmaakt van een bepaalde communicatie of daaraan is toegevoegd, of die andere gegevens identificeren als informatie die deel uitmaakt van een bepaalde communicatie of daaraan is toegevoegd.

[...]”

- 18 De sections 65 tot en met 69 RIPA bevatten regels inzake de werking en de bevoegdheden van de Investigatory Powers Tribunal (rechter die toezicht uitoefent op de onderzoeksbevoegdheden van de overheid, Verenigd Koninkrijk). Volgens section 65 van die wet kan bij deze rechter een klacht worden ingediend indien er redenen zijn om aan te nemen dat gegevens op onjuiste wijze zijn verkregen.

### Hoofdgeding en prejudiciële vragen

- 19 Begin 2015 werd onder meer in een rapport van de Intelligence and Security Committee of Parliament (parlementaire inlichtingen- en veiligheidscommissie, Verenigd Koninkrijk) bekendgemaakt dat door de verschillende veiligheids- en inlichtingendiensten van het Verenigd Koninkrijk, te weten de GCHQ, de MI5 en de MI6, bulkcommunicatiegegevens werden verwerkt en gebruikt. Op 5 juni 2015 heeft Privacy International, een non-gouvernementele organisatie, bij de Investigatory Powers Tribunal een zaak aangespannen tegen de minister van Buitenlandse Zaken en Gemenebestzaken, de minister van Binnenlandse Zaken en die veiligheids- en inlichtingendiensten, waarbij zij de rechtmatigheid van die praktijken heeft betwist.
- 20 De verwijzende rechter heeft die praktijken om te beginnen getoetst aan het nationale recht en aan de bepalingen van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, ondertekend te Rome op 4 november 1950 (hierna: „EVRM”), en vervolgens aan het Unierecht. In een vonnis van 17 oktober 2016 heeft deze rechter vastgesteld dat verweerders in het hoofdgeding hebben erkend dat genoemde veiligheids- en inlichtingendiensten in het kader van hun

activiteiten bulkdatasets met persoonsgegevens (*bulk personal data*) verzamelen en gebruiken, zoals biografische gegevens of reisgegevens, financiële of zakelijke informatie, communicatiegegevens die gevoelige informatie kunnen bevatten die onder het beroepsgeheim valt, of journalistiek materiaal. Die gegevens, die langs verschillende, mogelijk geheime wegen worden verkregen, worden volgens de verwijzende rechter door middel van kruiscontrole of automatische verwerking geanalyseerd en kunnen aan andere personen of autoriteiten worden bekendgemaakt en met buitenlandse partners worden gedeeld. In dit kader maken de veiligheids- en inlichtingendiensten ook gebruik van bulkcommunicatiegegevens die zij hebben verkregen van exploitanten van openbare elektronischecommunicatienetwerken op grond van met name de krachtens artikel 94 van de wet van 1984 gegeven ministeriële aanwijzingen. Volgens de verwijzende rechter doen de GCHQ en de MI5 dit sinds 2001 respectievelijk 2005.

- 21 De verwijzende rechter heeft geoordeeld dat het aldus verzamelen en gebruiken van gegevens in overeenstemming was met het nationale recht alsook – sinds 2015 – met artikel 8 EVRM, onder voorbehoud van de nog niet onderzochte kwesties inzake de evenredigheid van de betrokken maatregelen en inzake de doorgifte van gegevens aan derden. Met betrekking tot dit laatste punt heeft hij gepreciseerd dat aan hem bewijs was overgelegd inzake de geldende waarborgen, met name met betrekking tot de procedures voor de toegang tot de gegevens en de bekendmaking van de gegevens buiten de veiligheids- en inlichtingendiensten, de regels voor de bewaring van de gegevens en het bestaan van een onafhankelijk toezichtmechanisme.
- 22 Wat de rechtmatigheid van de in het hoofdgeding aan de orde zijnde maatregelen inzake de verwerving en het gebruik van gegevens vanuit het oogpunt van het Unierecht betreft, heeft de verwijzende rechter in een vonnis van 8 september 2017 onderzocht of die maatregelen binnen de werkingssfeer van dit recht vallen en, zo ja, of zij daarmee verenigbaar zijn. Hij heeft met betrekking tot de bulkcommunicatiegegevens vastgesteld dat de exploitanten van elektronischecommunicatienetwerken krachtens section 94 van de wet van 1984 verplicht waren om in het geval van een door een Secretary of State gegeven aanwijzing in die zin, aan de veiligheids- en inlichtingendiensten de gegevens te verstrekken die zij hadden verzameld in het kader van hun economische activiteit waarop het Unierecht van toepassing was. Dit was daarentegen niet het geval voor de verwerving van andere gegevens, die de betrokken diensten verwierven zonder gebruikmaking van die dwingende bevoegdheden. Op basis van die vaststelling heeft de verwijzende rechter het noodzakelijk geacht om zich tot het Hof te wenden met de vraag of een regeling als die van section 94 binnen de werkingssfeer van het Unierecht valt en, zo ja, of en in hoeverre de vereisten die voortvloeien uit het arrest van 21 december 2016, *Tele2 Sverige en Watson e.a.* (C-203/15 en C-698/15; EU:C:2016:970; hierna: „arrest Tele2”), op die regeling van toepassing zijn.
- 23 Dienaangaande merkt de verwijzende rechter in zijn verzoek om een prejudiciële beslissing op dat een Secretary of State volgens section 94 van de wet van 1984 aan aanbieders van openbare elektronischecommunicatiediensten de algemene of specifieke aanwijzingen kan geven die hij noodzakelijk acht in het belang van de nationale veiligheid of de betrekkingen met een buitenlandse regering. Onder verwijzing naar de definities in artikel 21, leden 4 en 6, RIPA verduidelijkt deze rechter dat de betrokken gegevens verkeersgegevens en informatie over gebruikte diensten in de zin van deze bepaling omvatten, waarbij uitsluitend de inhoud van de communicatie is uitgesloten. Die gegevens en die informatie geven onder meer uitsluitel omtrent het „wie, waar, wanneer en hoe” van een communicatie. De gegevens worden doorgezonden aan de veiligheids- en inlichtingendiensten en door deze diensten bewaard ten behoeve van hun activiteiten.
- 24 Volgens de verwijzende rechter verschilt de in het hoofdgeding aan de orde zijnde regeling van die van de Data Retention and Investigatory Powers Act 2014 (wet van 2014 betreffende de bewaring van gegevens en de onderzoeksbevoegdheden), die aan de orde was in de zaak die heeft geleid tot het arrest van 21 december 2016, *Tele2* (C-203/15 en C-698/15, EU:C:2016:970), aangezien die laatste regeling voorzag in een verplichting voor aanbieders van elektronischecommunicatiediensten om bepaalde gegevens te bewaren en deze niet alleen ter beschikking te stellen van de veiligheids- en

inlichtingendiensten, in het belang van de nationale veiligheid, maar ook van andere overheidsinstanties, afhankelijk van hun behoeften. Bovendien had dat arrest betrekking op een strafrechtelijk onderzoek en niet op de nationale veiligheid.

- 25 De verwijzende rechter voegt daaraan toe dat op de door de veiligheids- en inlichtingendiensten opgebouwde databases geautomatiseerde en niet-gerichte bulkverwerking wordt toegepast, bedoeld om eventuele onbekende bedreigingen aan het licht te brengen. Dit betekent volgens de verwijzende rechter dat de aldus gevormde metadatasets zo volledig mogelijk moeten zijn, opdat men kan beschikken over een „hooiberg” waarin kan worden gezocht naar de „speld” die daarin is verborgen. Met betrekking tot het nut van de verwerking van bulkgegevens door de betrokken diensten en van de technieken om die gegevens te raadplegen, verwijst de verwijzende rechter met name naar de conclusies van het rapport dat op 19 augustus 2016 is opgesteld door David Anderson, QC, die destijds de Independent Reviewer of Terrorism Legislation (onafhankelijke beoordelaar van terrorismewetgeving) van het Verenigd Koninkrijk was en zich bij het opstellen van dat rapport heeft gebaseerd op een door een team van inlichtingspecialisten uitgevoerd onderzoek en op de getuigenis van veiligheids- en inlichtingfunctionarissen.
- 26 De verwijzende rechter merkt voorts op dat de in het hoofdgeding aan de orde zijnde regeling volgens Privacy International in strijd is met het Unierecht, terwijl verweerders in het hoofdgeding van mening zijn dat de in die regeling neergelegde verplichting om gegevens door te zenden, de toegang tot die gegevens en het gebruik ervan niet onder de bevoegdheden van de Unie vallen. Dit volgt volgens hen met name uit artikel 4, lid 2, VEU, waarin is bepaald dat de nationale veiligheid tot de uitsluitende verantwoordelijkheid van elke lidstaat behoort.
- 27 Dienaangaande is de verwijzende rechter op grond van het arrest van 30 mei 2006, Parlement/Raad en Commissie (C-317/04 en C-318/04, EU:C:2006:346, punten 56-59), betreffende de overdracht van PNR-gegevens (*Passenger Name Record*) ten behoeve van de bescherming van de openbare veiligheid, van oordeel dat de activiteiten van commerciële ondernemingen in het kader van de verwerking en de doorgifte van gegevens ten behoeve van de bescherming van de nationale veiligheid niet binnen de werkingssfeer van het Unierecht lijken te vallen. Volgens de verwijzende rechter moet niet worden onderzocht of de betrokken activiteit gegevensverwerking vormt, maar enkel of die activiteit in wezen tot doel heeft een essentiële staatsfunctie in de zin van artikel 4, lid 2, VEU te ondersteunen binnen een door de overheid ingesteld kader dat betrekking heeft op de openbare veiligheid.
- 28 Voor het geval dat de in het hoofdgeding aan de orde zijnde maatregelen niettemin binnen de werkingssfeer van het Unierecht zouden vallen, is de verwijzende rechter van oordeel dat de vereisten die zijn geformuleerd in de punten 119 tot en met 125 van het arrest van 21 december 2016, Tele2 (C-203/15 en C-698/15, EU:C:2016:970), niet passend lijken in de context van de nationale veiligheid en afbreuk zouden kunnen doen aan het vermogen van de veiligheids- en inlichtingendiensten om bepaalde bedreigingen van de nationale veiligheid te beheersen.
- 29 In deze omstandigheden heeft de Investigatory Powers Tribunal besloten de behandeling van de zaak te schorsen en het Hof te verzoeken om een prejudiciële beslissing over de volgende vragen:

„Overwegende hetgeen volgt:

- a) het vermogen (van de veiligheids- en inlichtingendiensten) om de aan hen geleverde bulkcommunicatiegegevens te gebruiken is essentieel om de nationale veiligheid van het Verenigd Koninkrijk te verzekeren, met name op het gebied van terrorismebestrijding, contraspionage en de bestrijding van nucleaire proliferatie;
- b) een fundamenteel doel van het gebruik van [deze gegevens] door de veiligheids- en inlichtingendiensten is om voorheen onbekende bedreigingen voor de nationale veiligheid op te sporen door middel van niet-gerichte bulktechnieken die zijn gebaseerd op de aggregatie van

bulkcommunicatiegegevens op één plaats. Het grootste nut ervan ligt in de snelle identificatie en bepaling van het profiel van het doelwit, alsook in de verschaffing van een grond voor actie in geval van een onmiddellijke bedreiging;

- c) de leverancier van een elektronischecommunicatienetwerk is daarna niet verplicht om de bulkcommunicatiegegevens te bewaren (na de periode die vereist is voor zijn normale bedrijf); deze worden enkel bewaard door de staat (de veiligheids- en inlichtingendiensten);
  - d) de nationale rechter heeft vastgesteld dat de waarborgen die betrekking hebben op het gebruik van [deze gegevens] door de veiligheids- en inlichtingendiensten (onder voorbehoud van enkele buiten beschouwing gelaten kwesties) in overeenstemming zijn met het EVRM, en
  - e) de nationale rechter heeft vastgesteld dat de oplegging van de vereisten die gespecificeerd zijn in de punten 119 tot en met 125 van het arrest [van 21 december 2016, Tele2 (C-203/15 en C-698/15, EU:C:2016:970)], indien van toepassing, de maatregelen van de veiligheids- en inlichtingendiensten om de nationale veiligheid te waarborgen zullen dwarsbomen en daardoor de nationale veiligheid van het Verenigd Koninkrijk in gevaar zullen brengen;
- 1) Valt het in een aanwijzing van een Secretary of State aan een leverancier van een elektronischecommunicatienetwerk geformuleerde vereiste om bulkcommunicatiegegevens aan de veiligheids- en inlichtingendiensten van een lidstaat te verstrekken, gezien artikel 4 VEU en artikel 1, lid 3, van [richtlijn 2002/58] binnen de werkingssfeer van het Unierecht en [richtlijn 2002/58]?
  - 2) Indien het antwoord op de eerste vraag bevestigend luidt: zijn de [vereisten die gelden voor bewaarde communicatiegegevens, zoals gespecificeerd in de punten 119 tot en met 125 van het arrest van 21 december 2016, Tele2 (C-203/15 en C-698/15, EU:C:2016:970)] of andere vereisten, naast de vereisten die worden opgelegd door het EVRM, van toepassing op een dergelijke aanwijzing van een Secretary of State? Zo ja, hoe en in welke mate zijn deze vereisten dan van toepassing, rekening houdende met de essentiële noodzaak voor de veiligheids- en inlichtingendiensten om bulkverwerving en automatische verwerkingstechnieken te gebruiken om de nationale veiligheid te waarborgen en met de mate waarin die mogelijkheden – voor zover zij in overeenstemming zijn met het EVRM – door dergelijke vereisten op kritieke wijze kunnen worden belemmerd?"

## Prejudiciële vragen

### *Eerste vraag*

- 30 Met zijn eerste vraag wenst de verwijzende rechter in wezen te vernemen of artikel 1, lid 3, van richtlijn 2002/58, gelezen in het licht van artikel 4, lid 2, VEU, aldus moet worden uitgelegd dat een nationale regeling op grond waarvan een overheidsorgaan ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronischecommunicatiediensten een verplichting tot doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten kan opleggen, binnen de werkingssfeer van die richtlijn valt.
- 31 Privacy International voert in wezen aan dat, gelet op de lessen die kunnen worden getrokken uit de rechtspraak van het Hof betreffende de werkingssfeer van richtlijn 2002/58, deze richtlijn zowel van toepassing is op de verwerving van de betrokken gegevens door de veiligheids- en inlichtingendiensten krachtens section 94 van de wet van 1984, als op het gebruik van de gegevens door die diensten, ongeacht of de gegevens wel of niet in real time worden doorgezonden. Privacy International stelt met

name dat het feit dat de doelstelling van bescherming van de nationale veiligheid expliciet vermeld staat in artikel 15, lid 1, van richtlijn 2002/58, niet betekent dat deze richtlijn niet op dergelijke situaties van toepassing is, en dat artikel 4, lid 2, VEU niet aan dit oordeel afdoet.

- 32 De regering van het Verenigd Koninkrijk, de Tsjechische en de Estse regering, Ierland en de Franse, de Cypriotische, de Hongaarse, de Poolse en de Zweedse regering stellen daarentegen in wezen dat richtlijn 2002/58 niet van toepassing is op de in het hoofdgeding aan de orde zijnde nationale regeling, aangezien deze regeling tot doel heeft de nationale veiligheid te waarborgen. Die regeringen zijn van mening dat de activiteiten van de veiligheids- en inlichtingendiensten behoren tot de essentiële functies van de lidstaten in verband met de handhaving van de openbare orde en de bescherming van de binnenlandse veiligheid en de territoriale integriteit, en dus onder de exclusieve bevoegdheid van de lidstaten vallen, zoals met name uit artikel 4, lid 2, derde zin, VEU volgt.
- 33 Volgens de genoemde regeringen kan richtlijn 2002/58 dan ook niet aldus worden uitgelegd dat nationale maatregelen die erop gericht zijn de nationale veiligheid te waarborgen, binnen haar werkingssfeer vallen. Artikel 1, lid 3, van die richtlijn bakent die werkingssfeer af en sluit – in navolging van artikel 3, lid 2, eerste streepje, van richtlijn 95/46 – daarvan uit activiteiten die verband houden met openbare veiligheid, defensie en staatsveiligheid. Volgens de betrokken regeringen weerspiegelen die bepalingen de in artikel 4, lid 2, VEU vastgelegde bevoegdheidsverdeling en zouden zij van hun nuttig effect worden beroofd indien maatregelen op het vlak van de nationale veiligheid moesten voldoen aan de vereisten van richtlijn 2002/58. Die regeringen zijn bovendien van mening dat de door het Hof in het arrest van 30 mei 2006, Parlement/Raad en Commissie (C-317/04 en C-318/04, EU:C:2006:346), ontwikkelde rechtspraak betreffende artikel 3, lid 2, eerste streepje, van richtlijn 95/46 ook geldt voor artikel 1, lid 3, van richtlijn 2002/58.
- 34 In dit verband zij erop gewezen dat richtlijn 2002/58 volgens artikel 1, lid 1, onder meer de nationale regelgeving harmoniseert 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.
- 35 Volgens artikel 1, lid 3, van die richtlijn zijn van de werkingssfeer ervan uitgesloten de „activiteiten van de staat” op de aldaar bedoelde gebieden, waaronder 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. De in die bepaling als voorbeeld genoemde activiteiten zijn in alle gevallen specifieke activiteiten van staten of overheidsdiensten en hebben niets van doen met de gebieden waarop particulieren activiteiten ontplooiën (arrest van 2 oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punt 32 en aldaar aangehaalde rechtspraak).
- 36 Voorts bepaalt artikel 3 van richtlijn 2002/58 dat deze richtlijn van toepassing is op de verwerking van persoonsgegevens in verband met de levering van openbare elektronische communicatiediensten over openbare communicatienetwerken in de Unie, met inbegrip van de openbare communicatienetwerken die systemen voor gegevensverzameling en identificatie ondersteunen (hierna: „elektronische communicatiediensten”). Bijgevolg moet worden aangenomen dat deze richtlijn de activiteiten van de aanbieders van dergelijke diensten regelt (arrest van 2 oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punt 33 en aldaar aangehaalde rechtspraak).
- 37 Op grond van artikel 15, lid 1, van richtlijn 2002/58 kunnen de lidstaten in dat kader met inachtneming van de in deze bepaling geformuleerde voorwaarden „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” (arrest van 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 71).

- 38 Artikel 15, lid 1, van richtlijn 2002/58 vooronderstelt noodzakelijkerwijs dat de daarin bedoelde nationale wettelijke maatregelen binnen de werkingssfeer van deze richtlijn vallen, aangezien deze richtlijn uitdrukkelijk bepaalt dat de lidstaten die maatregelen slechts mogen treffen met inachtneming van de in de richtlijn geformuleerde voorwaarden. Bovendien regelen die maatregelen de activiteit van aanbieders van elektronischecommunicatiediensten voor de in die bepaling vermelde doeleinden (arrest van 2 oktober 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, punt 34 en aldaar aangehaalde rechtspraak).
- 39 Met name op grond van deze overwegingen heeft het Hof geoordeeld dat artikel 15, lid 1, van richtlijn 2002/58, gelezen in samenhang met artikel 3 van deze richtlijn, aldus moet worden uitgelegd dat binnen de werkingssfeer van deze richtlijn niet alleen wettelijke maatregelen vallen die aanbieders van elektronischecommunicatiediensten de verplichting opleggen om verkeers- en locatiegegevens te bewaren, maar ook wettelijke maatregelen die hun de verplichting opleggen om de bevoegde nationale autoriteiten toegang tot die gegevens te verlenen. Dergelijke wettelijke maatregelen impliceren immers noodzakelijkerwijs dat die aanbieders die gegevens verwerken, en kunnen, voor zover zij de activiteiten van die aanbieders regelen, niet worden gelijkgesteld met de in artikel 1, lid 3, van richtlijn 2002/58 bedoelde specifieke activiteiten van staten (zie in die zin arrest van 2 oktober 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, punten 35 en 37 en aldaar aangehaalde rechtspraak).
- 40 Met betrekking tot een wettelijke maatregel als section 94 van de wet van 1984, op grond waarvan de bevoegde autoriteit aanbieders van elektronischecommunicatiediensten de aanwijzing kan geven om door middel van doorzending bulkcommunicatiegegevens te verstrekken aan de veiligheids- en inlichtingendiensten, moet worden opgemerkt dat volgens de definitie in artikel 4, punt 2, van verordening 2016/679, die volgens artikel 2 van richtlijn 2002/58, gelezen in samenhang met artikel 94, lid 2, van die verordening, van toepassing is, het begrip „verwerking van persoonsgegevens” doelt op „een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, [...], opslaan, [...], raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen [...]”.
- 41 Hieruit volgt dat het verstrekken van persoonsgegevens door middel van doorzending, net zoals het opslaan of het op andere wijze ter beschikking stellen van gegevens, een verwerking in de zin van artikel 3 van richtlijn 2002/58 vormt en dus binnen de werkingssfeer van deze richtlijn valt (zie in die zin arrest van 29 januari 2008, *Promusicae*, C-275/06, EU:C:2008:54, punt 45).
- 42 Bovendien zou, gelet op de overwegingen in punt 38 van het onderhavige arrest en op de algemene opzet van richtlijn 2002/58, een uitlegging van deze richtlijn volgens welke de in artikel 15, lid 1, ervan bedoelde wettelijke maatregelen van de werkingssfeer van de richtlijn zijn uitgesloten omdat de doelstellingen die dergelijke maatregelen moeten nastreven, grotendeels overeenstemmen met de doelstellingen van de in artikel 1, lid 3, van diezelfde richtlijn bedoelde activiteiten, artikel 15, lid 1, elk nuttig effect ontnemen (zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punten 72 en 73).
- 43 Bijgevolg kan het begrip „activiteiten” in artikel 1, lid 3, van richtlijn 2002/58, zoals de advocaat-generaal in wezen heeft opgemerkt in punt 75 van zijn conclusie in de gevoegde zaken *La Quadrature du Net e.a.* (C-511/18 en C-512/18, EU:C:2020:6), waarnaar hij in punt 24 van zijn conclusie in de onderhavige zaak verwijst, niet aldus worden uitgelegd dat daaronder ook de in artikel 15, lid 1, van die richtlijn bedoelde wettelijke maatregelen vallen.
- 44 Artikel 4, lid 2, VEU, waaraan de in punt 32 van het onderhavige arrest genoemde regeringen hebben gerefereerd, kan niet afdoen aan deze conclusie. Volgens vaste rechtspraak van het Hof staat het immers weliswaar aan de lidstaten om hun wezenlijke veiligheidsbelangen te definiëren en om passende maatregelen te nemen teneinde hun binnenlandse en buitenlandse veiligheid te verzekeren, maar kan het enkele feit dat een nationale maatregel is genomen met het oog op de bescherming van



de nationale veiligheid, niet ertoe leiden dat het Unierecht niet van toepassing is en dat de lidstaten worden ontheven van de verplichting om dit recht te eerbiedigen [zie in die zin arresten van 4 juni 2013, ZZ, C-300/11, EU:C:2013:363, punt 38 en aldaar aangehaalde rechtspraak; 20 maart 2018, Commissie/Oostenrijk (Staatsdrukkerij), C-187/16, EU:C:2018:194, punten 75 en 76, en 2 april 2020, Commissie/Polen, Hongarije en Tsjechië (Tijdelijk herplaatsingsmechanisme voor aanvragers van internationale bescherming), C-715/17, C-718/17 en C-719/17, EU:C:2020:257, punten 143 en 170].

- 45 Het is juist dat het Hof in het arrest van 30 mei 2006, Parlement/Raad en Commissie (C-317/04 en C-318/04, EU:C:2006:346, punten 56-59), heeft geoordeeld dat de doorgifte van persoonsgegevens door luchtvaartmaatschappijen aan overheidsdiensten van een derde land met het oog op het voorkomen en bestrijden van terrorisme en andere ernstige misdrijven, ingevolge artikel 3, lid 2, eerste streepje, van richtlijn 95/46 niet binnen de werkingssfeer van deze richtlijn viel, aangezien die doorgifte geschiedde binnen een door de overheid ingesteld kader dat betrekking had op de openbare veiligheid.
- 46 Gelet op de overwegingen in de punten 36, 38 en 39 van het onderhavige arrest, kan die rechtspraak echter niet worden toegepast op de uitlegging van artikel 1, lid 3, van richtlijn 2002/58. Zoals de advocaat-generaal in wezen heeft opgemerkt in de punten 70 tot en met 72 van zijn conclusie in de gevoegde zaken La Quadrature du Net e.a. (C-511/18 en C-512/18, EU:C:2020:6), sloot artikel 3, lid 2, eerste streepje, van richtlijn 95/46, waarop die rechtspraak betrekking heeft, „verwerkingen die betrekking hebben op de openbare veiligheid, defensie, de veiligheid van de staat” immers in het algemeen van de werkingssfeer van deze richtlijn uit, zonder onderscheid te maken naar de persoon die de gegevensverwerkingshandeling uitvoerde. In het kader van de uitlegging van artikel 1, lid 3, van richtlijn 2002/58 moet dat onderscheid echter wel worden gemaakt. Zoals uit de punten 37 tot en met 39 en 42 van het onderhavige arrest blijkt, valt immers elke verwerking van persoonsgegevens door aanbieders van elektronische communicatiediensten binnen de werkingssfeer van die richtlijn, inclusief de verwerking die het gevolg is van door de overheid aan die aanbieders opgelegde verplichtingen, terwijl laatstgenoemde verwerking eventueel onder de uitzondering kon vallen van artikel 3, lid 2, eerste streepje, van richtlijn 95/46, gelet op de ruimere formulering van deze bepaling, die zag op elke verwerking die betrekking had op de openbare veiligheid, defensie of de veiligheid van de staat, ongeacht de persoon die de handeling uitvoerde.
- 47 Bovendien moet worden opgemerkt dat richtlijn 95/46, die aan de orde was in de zaak die heeft geleid tot het arrest van 30 mei 2006, Parlement/Raad en Commissie (C-317/04 en C-318/04, EU:C:2006:346), overeenkomstig artikel 94, lid 1, van verordening 2016/679 met ingang van 25 mei 2018 is ingetrokken en vervangen door deze verordening. Verordening 2016/679 is volgens artikel 2, lid 2, onder d), weliswaar niet van toepassing op verwerkingen die „door de bevoegde autoriteiten” worden verricht met het oog op onder meer de voorkoming en de opsporing van strafbare feiten, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid, maar uit artikel 23, lid 1, onder d) en h), van deze verordening blijkt dat verwerkingen van persoonsgegevens die voor diezelfde doeleinden worden verricht door particulieren, binnen de werkingssfeer van deze verordening vallen. Hieruit volgt dat bovenstaande uitlegging van artikel 1, lid 3, artikel 3 en artikel 15, lid 1, van richtlijn 2002/58 in overeenstemming is met de afbakening van de werkingssfeer van verordening 2016/679, die door deze richtlijn wordt aangevuld en gespecificeerd.
- 48 Wanneer de lidstaten daarentegen rechtstreeks maatregelen toepassen die inbreuk maken op het beginsel van de vertrouwelijkheid van elektronische communicatie, zonder dat zij verwerkingsverplichtingen opleggen aan aanbieders van elektronische communicatiediensten, wordt de bescherming van de gegevens van de betrokken personen niet beheerst door richtlijn 2002/58, maar uitsluitend door nationaal recht, behoudens de toepassing van richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van

kaderbesluit 2008/977/JBZ van de Raad (PB 2016, L 119, blz. 89), wat betekent dat de betrokken maatregelen met name in overeenstemming moeten zijn met het nationale constitutionele recht en met de vereisten van het EVRM.

- 49 Gelet op een en ander moet op de eerste vraag worden geantwoord dat artikel 1, lid 3, artikel 3 en artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van artikel 4, lid 2, VEU, aldus moeten worden uitgelegd dat een nationale regeling op grond waarvan een overheidsorgaan ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronischecomunicatiediensten een verplichting tot doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten kan opleggen, binnen de werkingssfeer van die richtlijn valt.

### *Tweede vraag*

- 50 Met zijn tweede vraag wenst de verwijzende rechter in wezen te vernemen of artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van artikel 4, lid 2, VEU en de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, aldus moet worden uitgelegd dat het zich verzet tegen een nationale regeling op grond waarvan een overheidsorgaan ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronischecomunicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten kan opleggen.
- 51 Om te beginnen zij eraan herinnerd dat section 94 van de wet van 1984 volgens de informatie in het verzoek om een prejudiciële beslissing de Secretary of State de mogelijkheid biedt om aanbieders van elektronischecomunicatiediensten door middel van aanwijzingen de verplichting op te leggen om bulkcommunicatiegegevens door te zenden aan de veiligheids- en inlichtingendiensten, indien hij dit noodzakelijk acht in het belang van de nationale veiligheid of de betrekkingen met een buitenlandse regering. Deze gegevens omvatten verkeers- en locatiegegevens alsmede informatie over de gebruikte diensten, in de zin van section 21, leden 4 en 6, RIPA. Deze laatste bepaling ziet onder meer op de gegevens die nodig zijn om de bron en de bestemming van een communicatie te identificeren, de datum, het tijdstip, de duur en de aard van die communicatie te bepalen, het gebruikte materiaal te identificeren en de eindapparatuur en de communicatie te lokaliseren. Tot die gegevens behoren met name de naam en het adres van de gebruiker, het telefoonnummer van de beller en het gebelde nummer, het bron- en het doel-IP-adres en de adressen van de bezochte websites.
- 52 Een dergelijke verstrekking van gegevens door middel van doorzending betreft alle gebruikers van elektronischecomunicatiemiddelen, zonder dat wordt gespecificeerd of die doorzending wel of niet in real time moet plaatsvinden. De doorgezonden gegevens worden volgens de informatie in het verzoek om een prejudiciële beslissing door de veiligheids- en inlichtingendiensten bewaard en blijven ter beschikking van deze diensten ten behoeve van hun activiteiten, net zoals de andere databases van deze diensten. Met name kunnen de aldus verworven gegevens, waarop automatische bulkverwerking en -analyse worden toegepast, worden onderworpen aan kruiscontroles met andere databases die verschillende categorieën bulkpersoonsgegevens bevatten, of buiten die diensten worden bekendgemaakt, ook aan derde staten. Tot slot is voor die bewerkingen geen voorafgaande toestemming van een rechterlijke instantie of een onafhankelijk bestuursorgaan vereist en geldt er geen verplichting om de betrokkenen te informeren.
- 53 Zoals met name uit de overwegingen 6 en 7 van richtlijn 2002/58 volgt, heeft deze richtlijn tot doel om de gebruikers van elektronischecomunicatiediensten te beschermen tegen de gevaren die de nieuwe technologieën en, met name, de steeds grotere mogelijkheden van geautomatiseerde opslag en verwerking van gegevens voor de persoonsgegevens en de persoonlijke levenssfeer van die gebruikers meebrengen. Zoals in overweging 2 van richtlijn 2002/58 wordt verklaard, beoogt deze richtlijn in het bijzonder de volledige eerbiediging van de in de artikelen 7 en 8 van het Handvest bedoelde rechten te waarborgen. Dienaangaande blijkt uit de toelichting bij het voorstel voor een richtlijn van het Europees

Parlement en de Raad betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie [COM(2000) 385 definitief], waaruit richtlijn 2002/58 is voortgekomen, dat de Uniewetgever heeft willen „zorgen voor een hoge mate van bescherming van de persoonsgegevens en van de persoonlijke levenssfeer voor alle elektronischecommunicatiediensten, ongeacht de gebruikte technologie”.

- 54 Daartoe bepaalt artikel 5, lid 1, van richtlijn 2002/58 dat „[d]e lidstaten [...] via nationale wetgeving het vertrouwelijke karakter van de communicatie en de daarmee verband houdende verkeersgegevens via openbare communicatienetwerken en via openbare elektronischecommunicatiediensten [garanderen]”. In diezelfde bepaling wordt benadrukt dat de lidstaten „met name het afluisteren, aftappen, opslaan of anderszins onderscheppen of controleren van de communicatie en de daarmee verband houdende verkeersgegevens door anderen dan de gebruikers [verbieden], indien de betrokken gebruikers daarin niet hebben toegestemd, tenzij dat bij wet is toegestaan overeenkomstig artikel 15, lid 1”, en gepreciseerd dat „[d]it lid [...] de technische opslag die nodig is voor het overbrengen van informatie onverlet [laat], onverminderd het vertrouwelijkheidsbeginsel”.
- 55 Artikel 5, lid 1, legt aldus het beginsel van vertrouwelijkheid van zowel de elektronische communicatie als de daarmee verband houdende verkeersgegevens vast en impliceert met name dat het anderen dan de gebruikers in beginsel moet worden verboden die communicatie en die gegevens op te slaan, indien de gebruikers daarin niet hebben toegestemd. Gelet op haar algemene bewoordingen, bestrijkt die bepaling noodzakelijkerwijs elke voor andere doeleinden dan het overbrengen van informatie uitgevoerde bewerking die derden in staat stelt om kennis te nemen van de communicatie en de daarmee verband houdende gegevens.
- 56 Het in artikel 5, lid 1, van richtlijn 2002/58 neergelegde verbod op het onderscheppen van de communicatie en de daarmee verband houdende verkeersgegevens omvat dus elke vorm van beschikbaarstelling door aanbieders van elektronischecommunicatiediensten van verkeers- en locatiegegevens aan overheidsinstanties, zoals veiligheids- en inlichtingendiensten, alsmede de bewaring van de beschikbaar gestelde gegevens door die instanties, ongeacht het latere gebruik van die gegevens.
- 57 Met de vaststelling van richtlijn 2002/58 heeft de Uniewetgever dus de in de artikelen 7 en 8 van het Handvest neergelegde rechten geconcretiseerd, zodat de gebruikers van elektronischecommunicatiemiddelen in beginsel erop mogen vertrouwen dat hun communicatie en de daarmee verband houdende gegevens anoniem blijven en niet mogen worden vastgelegd, tenzij zij daarin hebben toegestemd (arrest van 6 oktober 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 en C-520/18, punt 109).
- 58 Artikel 15, lid 1, van richtlijn 2002/58 staat de lidstaten echter toe, te voorzien in uitzonderingen op de in artikel 5, lid 1, van deze richtlijn geformuleerde principeverplichting om de vertrouwelijkheid van de persoonsgegevens te waarborgen, en op de met name in de artikelen 6 en 9 van deze richtlijn vermelde overeenkomstige verplichtingen, indien dat in een democratische samenleving een noodzakelijke, redelijke en proportionele maatregel vormt om de nationale veiligheid, de landsverdediging en de openbare veiligheid te waarborgen, of om strafbare feiten of onbevoegd gebruik van het elektronischecommunicatiesysteem te voorkomen, te onderzoeken, op te sporen en te vervolgen. Daartoe kunnen de lidstaten onder meer wettelijke maatregelen treffen om gegevens gedurende een beperkte periode te bewaren indien dat om een van die redenen gerechtvaardigd is.
- 59 De mogelijkheid om af te wijken van de in de artikelen 5, 6 en 9 van richtlijn 2002/58 vastgestelde rechten en verplichtingen kan echter niet rechtvaardigen dat de uitzondering op de principeverplichting tot waarborging van de vertrouwelijkheid van de elektronische communicatie en van de daarmee verband houdende gegevens en, in het bijzonder, op het verbod om deze gegevens op

te slaan de regel wordt (zie in die zin arresten van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punten 89 en 104, en 6 oktober 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 en C-520/18, punt 111).

- 60 Bovendien volgt uit artikel 15, lid 1, derde zin, van richtlijn 2002/58 dat de lidstaten slechts wettelijke maatregelen ter beperking van de omvang van de in de artikelen 5, 6 en 9 van deze richtlijn bedoelde rechten en plichten mogen nemen voor zover deze maatregelen in overeenstemming zijn met de algemene beginselen van het Unierecht, waaronder het evenredigheidsbeginsel, en met de door het Handvest gewaarborgde grondrechten. In dit verband heeft het Hof reeds geoordeeld dat de door een lidstaat bij een nationale regeling aan aanbieders van elektronischecommunicatiediensten opgelegde verplichting om de verkeersgegevens te bewaren teneinde de bevoegde nationale autoriteiten in voorkomend geval toegang tot die gegevens te kunnen geven, niet alleen vragen doet rijzen betreffende de eerbiediging van de artikelen 7 en 8 van het Handvest, die betrekking hebben op, respectievelijk, de bescherming van het privéleven en de bescherming van persoonsgegevens, maar ook betreffende de eerbiediging van artikel 11 van het Handvest, dat betrekking heeft op de vrijheid van meningsuiting (zie in die zin arresten van 8 april 2014, *Digital Rights Ireland e.a.*, C-293/12 en C-594/12, EU:C:2014:238, punten 25 en 70, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punten 91 en 92 en aldaar aangehaalde rechtspraak).
- 61 Diezelfde vragen rijzen ook voor andere vormen van gegevensverwerking, zoals de doorzending van gegevens aan anderen dan de gebruikers of de toegang tot die gegevens met het oog op het gebruik ervan [zie naar analogie advies 1/15 (*PNR-Overeenkomst EU-Canada*) van 26 juli 2017, EU:C:2017:592, punten 122 en 123 en aldaar aangehaalde rechtspraak].
- 62 Bij de uitlegging van artikel 15, lid 1, van richtlijn 2002/58 moet derhalve zowel het belang van het door artikel 7 van het Handvest gewaarborgde recht op bescherming van het privéleven als dat van het door artikel 8 van het Handvest gewaarborgde recht op bescherming van persoonsgegevens, zoals dat blijkt uit de rechtspraak van het Hof, in aanmerking worden genomen. Hetzelfde geldt voor het recht op vrijheid van meningsuiting, aangezien dit in artikel 11 van het Handvest gewaarborgde grondrecht een van de wezenlijke grondslagen is van een democratische en pluralistische samenleving, die behoort tot de waarden waarop de Unie overeenkomstig artikel 2 VEU is gebaseerd (zie in die zin arresten van 6 maart 2001, *Connolly/Commissie*, C-274/99 P, EU:C:2001:127, punt 39, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 93 en aldaar aangehaalde rechtspraak).
- 63 De in de artikelen 7, 8 en 11 van het Handvest verankerde rechten hebben echter geen absolute gelding, maar moeten worden beschouwd in relatie tot hun functie in de samenleving (zie in die zin arrest van 16 juli 2020, *Facebook Ireland en Schrems*, C-311/18, EU:C:2020:559, punt 172 en aldaar aangehaalde rechtspraak).
- 64 Zoals blijkt uit artikel 52, lid 1, van het Handvest, staat het Handvest immers beperkingen op de uitoefening van die rechten toe, mits deze beperkingen bij wet worden gesteld, de wezenlijke inhoud van die rechten eerbiedigen en, met inachtneming van het evenredigheidsbeginsel, noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen.
- 65 Hieraan dient te worden toegevoegd dat het vereiste dat elke beperking op de uitoefening van grondrechten bij wet wordt gesteld, inhoudt dat de rechtsgrond die de inmenging in die rechten toestaat, zelf de reikwijdte van de beperking op de uitoefening van het betrokken recht moet bepalen (arrest van 16 juli 2020, *Facebook Ireland en Schrems*, C-311/18, EU:C:2020:559, punt 175 en aldaar aangehaalde rechtspraak).
- 66 Wat de eerbiediging van het evenredigheidsbeginsel betreft, staat in artikel 15, lid 1, eerste zin, van richtlijn 2002/58 te lezen dat de lidstaten een maatregel waarbij wordt afgeweken van het beginsel van vertrouwelijkheid van de communicatie en van de daarmee verband houdende verkeersgegevens

kunnen treffen wanneer een dergelijke maatregel „in een democratische samenleving noodzakelijk, redelijk en proportioneel is” in het licht van de in die bepaling genoemde doelstellingen. In overweging 11 van deze richtlijn wordt gepreciseerd dat een dergelijke maatregel „strikt” evenredig moet zijn aan het nagestreefde doel.

- 67 In dit verband zij eraan herinnerd dat de bescherming van het grondrecht op eerbiediging van het privéleven volgens vaste rechtspraak van het Hof vereist dat de uitzonderingen op de bescherming van de persoonsgegevens en de beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven. Bovendien kan een doelstelling van algemeen belang niet worden nagestreefd zonder rekening te houden met het feit dat deze doelstelling moet worden verzoend met de door de maatregel aangetaste grondrechten, zulks via een evenwichtige afweging tussen de doelstelling en de op het spel staande belangen en rechten [zie in die zin arresten van 16 december 2008, Satakunnan Markkinapörssi en Satamedia, C-73/07, EU:C:2008:727, punt 56; 9 november 2010, Volker und Markus Schecke en Eifert, C-92/09 en C-93/09, EU:C:2010:662, punten 76, 77 en 86, en 8 april 2014, Digital Rights Ireland e.a., C-293/12 en C-594/12, EU:C:2014:238, punt 52; advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 140].
- 68 Om aan het evenredigheidsvereiste te voldoen, dient een regeling duidelijke en nauwkeurige regels te bevatten over de reikwijdte en de toepassing van de betrokken maatregel, zodat degenen van wie de persoonsgegevens aan de orde zijn, over voldoende waarborgen beschikken dat die gegevens doeltreffend worden beschermd tegen het risico van misbruik. Die regeling moet wettelijk verbindend zijn naar intern recht en in het bijzonder aangeven in welke omstandigheden en onder welke voorwaarden een maatregel die voorziet in de verwerking van dergelijke gegevens kan worden genomen, en aldus waarborgen dat de inmenging tot het strikt noodzakelijke wordt beperkt. De noodzaak om over dergelijke waarborgen te beschikken is des te groter wanneer de persoonsgegevens op geautomatiseerde wijze worden verwerkt, met name wanneer er een aanzienlijk risico bestaat dat deze gegevens op onrechtmatige wijze zullen worden geraadpleegd. Deze overwegingen gelden in het bijzonder wanneer het gaat om de bescherming van een bijzondere categorie persoonsgegevens, te weten gevoelige gegevens [zie in die zin arresten van 8 april 2014, Digital Rights Ireland e.a., C-293/12 en C-594/12, EU:C:2014:238, punten 54 en 55, en 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 117; advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 141].
- 69 Wat de vraag betreft of een nationale regeling als die van het hoofdgeding voldoet aan de vereisten van artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, dient te worden opgemerkt dat de doorzending van verkeers- en locatiegegevens aan anderen dan de gebruikers, zoals de veiligheids- en inlichtingendiensten, afwijkt van het vertrouwelijkheidsbeginsel. Wanneer die bewerking, zoals in casu, op algemene en ongedifferentieerde wijze wordt uitgevoerd, heeft zij tot gevolg dat de afwijking van de principeverplichting tot waarborging van de vertrouwelijkheid van de gegevens de regel wordt, terwijl het bij richtlijn 2002/58 ingevoerde stelsel eist dat die afwijking de uitzondering blijft.
- 70 Voorts vormt de doorzending van verkeers- en locatiegegevens aan een derde volgens vaste rechtspraak van het Hof een inmenging in de in de artikelen 7 en 8 van het Handvest verankerde grondrechten, ongeacht het latere gebruik van die gegevens. In dit verband is het van weinig belang of de gegevens betreffende het privéleven al dan niet gevoelig zijn en of de betrokkenen door die inmenging enig nadeel hebben ondervonden [zie in die zin advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punten 124 en 126 en aldaar aangehaalde rechtspraak, en arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, punten 115 en 116].
- 71 De inmenging die de doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten vormt in het door artikel 7 van het Handvest gewaarborgde recht, moet als bijzonder ernstig worden beschouwd, met name gelet op het gevoelige karakter van de informatie die deze gegevens kunnen prijsgeven, en op de mogelijkheid om aan de hand van deze gegevens het

profiel van de betrokken personen te bepalen, informatie die even gevoelig is als de inhoud zelf van de communicatie. Die inmenging kan bovendien bij de betrokken personen het gevoel opwekken dat hun privéleven constant in de gaten wordt gehouden (zie naar analogie arresten van 8 april 2014, *Digital Rights Ireland e.a.*, C-293/12 en C-594/12, EU:C:2014:238, punten 27 en 37, en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punten 99 en 100).

- 72 Tevens moet worden opgemerkt dat de doorzending van verkeers- en locatiegegevens aan overheidsinstanties voor veiligheidsdoeleinden op zichzelf afbreuk kan doen aan het in artikel 7 van het Handvest verankerde recht op eerbiediging van communicatie, en de gebruikers van elektronischecommunicatiemiddelen kan ontmoedigen om hun door artikel 11 van het Handvest gewaarborgde vrijheid van meningsuiting uit te oefenen. Dit laatste geldt in het bijzonder voor personen van wie de communicatie naar nationaal recht onder het beroepsgeheim valt, en voor klokkenluiders van wie de activiteiten worden beschermd door richtlijn (EU) 2019/1937 van het Europees Parlement en de Raad van 23 oktober 2019 inzake de bescherming van personen die inbreuken op het Unierecht melden (PB 2019, L 305, blz. 17). Dat ontmoedigende effect is bovendien des te ernstiger omdat de bewaarde gegevens talrijk en gevarieerd zijn (zie in die zin arresten van 8 april 2014, *Digital Rights Ireland e.a.*, C-293/12 en C-594/12, EU:C:2014:238, punt 28; 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 101, en 6 oktober 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 en C-520/18, punt 118).
- 73 Ten slotte is het zo dat, gelet op de aanzienlijke hoeveelheid verkeers- en locatiegegevens die continu kunnen worden bewaard op grond van een algemene bewaringsmaatregel, en op het gevoelige karakter van de informatie die deze gegevens kunnen prijsgeven, het enkele feit dat die gegevens door aanbieders van elektronischecommunicatiediensten worden bewaard, risico's van misbruik en onrechtmatige toegang tot de gegevens inhoudt.
- 74 Wat de doelstellingen betreft die dergelijke inmengingen kunnen rechtvaardigen, meer in het bijzonder de in het hoofdgeding aan de orde zijnde doelstelling van bescherming van de nationale veiligheid, moet om te beginnen worden opgemerkt dat de nationale veiligheid volgens artikel 4, lid 2, VEU tot de uitsluitende verantwoordelijkheid van elke lidstaat behoort. Deze verantwoordelijkheid strookt met het grote belang dat wordt gehecht aan de bescherming van de essentiële staatsfuncties en de fundamentele belangen van de samenleving, en omvat het voorkomen en bestrijden van activiteiten die de fundamentele constitutionele, politieke, economische of sociale structuren van een land ernstig kunnen destabiliseren en, met name, een rechtstreekse bedreiging kunnen vormen voor de samenleving, de bevolking of de staat als zodanig, zoals terroristische activiteiten (arrest van 6 oktober 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 en C-520/18, punt 135).
- 75 Het belang van de doelstelling van bescherming van de nationale veiligheid, gelezen in het licht van artikel 4, lid 2, VEU, overstijgt dat van de andere doelstellingen die worden genoemd in artikel 15, lid 1, van richtlijn 2002/58, met name de doelstellingen van bestrijding van – zelfs ernstige – criminaliteit in het algemeen, en van bescherming van de openbare veiligheid. Bedreigingen als die waaraan in het voorgaande punt wordt gerefereerd, verschillen door hun aard en hun bijzondere ernst immers van het algemene risico dat zich – zelfs ernstige – spanningen of wanordelijkheden zullen voordoen die de openbare veiligheid ondermijnen. Mits aan de overige in artikel 52, lid 1, van het Handvest geformuleerde vereisten wordt voldaan, kan de doelstelling van bescherming van de nationale veiligheid derhalve maatregelen rechtvaardigen die ernstigere inmengingen in de grondrechten met zich brengen dan die welke door die andere doelstellingen zouden kunnen worden gerechtvaardigd (arrest van 6 oktober 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 en C-520/18, punt 136).
- 76 Om te voldoen aan het in punt 67 van het onderhavige arrest in herinnering gebrachte evenredigheidsvereiste, dat verlangt dat uitzonderingen op de bescherming van persoonsgegevens en beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven, dient een nationale regeling

die een inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten met zich brengt, evenwel in overeenstemming te zijn met de eisen die voortvloeien uit de in de punten 65, 67 en 68 van het onderhavige arrest aangehaalde rechtspraak.

- 77 Wat in het bijzonder de toegang van een autoriteit tot persoonsgegevens betreft, mag een regeling zich niet ertoe beperken te eisen dat de toegang tot deze gegevens wordt verleend voor het met die regeling beoogde doel, maar moet zij ook de materiële en procedurele voorwaarden voor dit gebruik bepalen [zie naar analogie advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 192 en aldaar aangehaalde rechtspraak].
- 78 Een nationale regeling die de toegang tot locatie- en verkeersgegevens regelt, moet dus aan de hand van objectieve criteria bepalen in welke omstandigheden en onder welke voorwaarden aan de bevoegde nationale autoriteiten toegang tot de betrokken gegevens moet worden verleend, aangezien een algemene toegang tot alle bewaarde gegevens, los van enig – zelfs maar indirect – verband met het nagestreefde doel, niet kan worden geacht tot het strikt noodzakelijke te zijn beperkt, (zie in die zin arrest van 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 119 en aldaar aangehaalde rechtspraak).
- 79 Die vereisten zijn a fortiori van toepassing op een wettelijke maatregel als aan de orde in het hoofdgeding, op grond waarvan de bevoegde nationale autoriteit aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten kan opleggen. Een dergelijke doorzending heeft immers tot gevolg dat die gegevens ter beschikking worden gesteld aan overheidsinstanties [zie naar analogie advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 212].
- 80 Het feit dat de doorzending van de verkeers- en locatiegegevens geschiedt op algemene en ongedifferentieerde wijze, betekent dat die doorzending algemeen alle personen betreft die gebruikmaken van elektronischecommunicatiediensten, dat wil zeggen zelfs personen voor wie er geen enkele aanwijzing bestaat dat hun gedrag – zelfs maar indirect of van ver – een verband vertoont met de doelstelling van bescherming van de nationale veiligheid. Met name is er geen enkel verband vereist tussen de gegevens die moeten worden doorgezonden en een bedreiging van de nationale veiligheid (zie in die zin arresten van 8 april 2014, Digital Rights Ireland e.a., C-293/12 en C-594/12, EU:C:2014:238, punten 57 en 58, en 21 december 2016, Tele2, C-203/15 en C-698/15, EU:C:2016:970, punt 105). Gelet op het feit dat de doorzending van dergelijke gegevens aan overheidsinstanties – overeenkomstig de vaststelling in punt 79 van het onderhavige arrest – gelijkstaat aan het verlenen van toegang tot deze gegevens, moet worden geoordeeld dat een regeling die de algemene en ongedifferentieerde doorzending van gegevens aan overheidsinstanties mogelijk maakt, een algemene toegang tot die gegevens impliceert.
- 81 Daaruit volgt dat een nationale regeling die aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten oplegt, verder gaat dan strikt noodzakelijk is en niet kan worden beschouwd als een regeling die in een democratische samenleving gerechtvaardigd is, zoals artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, eist.
- 82 Gelet op een en ander moet op de tweede vraag worden geantwoord dat artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van artikel 4, lid 2, VEU en de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, aldus moet worden uitgelegd dat het zich verzet tegen een nationale regeling op grond waarvan een overheidsorgaan ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten kan opleggen.

## Kosten

- 83 Ten aanzien van de partijen in het hoofdgeding is de procedure als een aldaar gerezen incident te beschouwen, zodat de verwijzende rechter over de kosten heeft te beslissen. De door anderen wegens indiening van hun opmerkingen bij het Hof gemaakte kosten komen niet voor vergoeding in aanmerking.

Het Hof (Grote kamer) verklaart voor recht:

- 1) Artikel 1, lid 3, artikel 3 en artikel 15, lid 1, van richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PB 2002, L 201, blz. 37), zoals gewijzigd bij richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009, gelezen in het licht van artikel 4, lid 2, VEU, moeten aldus worden uitgelegd dat een nationale regeling op grond waarvan een overheidsorgaan ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronischecommunicatiediensten een verplichting tot doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten kan opleggen, binnen de werkingssfeer van die richtlijn valt.
- 2) Artikel 15, lid 1, van richtlijn 2002/58, zoals gewijzigd bij richtlijn 2009/136, gelezen in het licht van artikel 4, lid 2, VEU en de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, moet aldus worden uitgelegd dat het zich verzet tegen een nationale regeling op grond waarvan een overheidsorgaan ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten kan opleggen.

ondertekeningen