NJ 2020/232

HOF VAN JUSTITIE VAN DE EUROPESE UNIE
2 oktober 2018, nr. C-207/16
(K. Lenaerts, A. Tizzano, R. Silva de Lapuerta, T. von Danwitz, J.L. da Cruz Vilaça, C.G. Fernlund, C. Vajda, E. Juhász, A. Borg Barthet, C. Toader, M. Safjan, D. Šváby, M. Berger, E. Jarašiūnas, E. Regan; A-G H. Saugmandsgaard Øe)
m.nt. E.J. Dommering

Art. 1, 3, 5, 15 lid 1 e-Privacyrichtlijn; art. 7, 8 Handvest Grondrechten EU

Module Privacy & AVG 2020/3406
RvdW 2019/383
ECLI:EU:C:2018:300
ECLI:EU:C:2018:788

Verzoek om een prejudiciële beslissing ingediend door de Audiencia Provincial de Tarragona (provinciaal gerecht Tarragona, Spanje) bij beslissing van 6 april 2016.

Elektronische communicatie. Verwerking van persoonsgegevens. Werkingssfeer. Vertrouwelijk karakter van elektronische communicatie. Bescherming in het kader van de levering van elektronische-communicatiediensten verwerkte gegevens. Toegang van nationale autoriteiten tot gegevens voor onderzoeksdoeleinden. Drempel waarboven het delict voldoende ernstig is om de toegang tot gegevens te rechtvaardigen.

Art. 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), zoals gewijzigd bij Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009, gelezen in samenhang met de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie, moet aldus worden uitgelegd dat de toegang van overheidsinstanties tot de identificatiegegevens van houders van met een gestolen mobiele telefoon geactiveerde simkaarten — zoals hun naam, voornaam en, in voorkomend geval, adres — geen zodanig ernstige inmenging in de door die artikelen van het Handvest gewaarborgde grondrechten van laatstgenoemden oplevert dat die toegang — op het gebied van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten — moet worden beperkt tot de bestrijding van zware criminaliteit.

Ministerio Fiscal

Hof van Justitie EU:

Arrest

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

2 Dit verzoek is ingediend in het kader van een door het Ministerio Fiscal (openbaar ministerie, Spanje) ingesteld beroep tegen de beslissing van de Juzgado de Instrucción nr. 3 de Tarragona (onderzoeksrechtbank nr. 3 Tarragona, Spanje; hierna: 'onderzoeksrechter') waarbij de gerechtelijke politie toegang wordt geweigerd tot persoonsgegevens die worden bewaard door aanbieders van elektronische-communicatiediensten.

Toepasselijke bepalingen

Richtlijn 95/46

3 Volgens artikel 2, onder b), van richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (*PB* 1995, L 281, blz. 31), moet voor de toepassing van deze richtlijn onder 'verwerking van persoonsgegevens' worden verstaan, 'elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op enigerlei andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens'.

4 Artikel 3 van die richtlijn, met als opschrift 'Werkingssfeer', bepaalt:

"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 van het Verdrag betreffende de Europese Unie 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

5 Overwegingen 2, 11, 15 en 21 van richtlijn 2002/58 luiden als volgt:

"(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 dit Handvest] bedoelde rechten.

[…]

(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 Gemeenschapsrecht vallende activiteiten. Zij verandert bijgevolg niets aan het bestaande evenwicht tussen het recht van personen op persoonlijke levenssfeer en de mogelijkheid voor de lidstaten om de in artikel 15, lid 1, van deze richtlijn bedoelde maatregelen te nemen, die nodig zijn voor de bescherming van de openbare veiligheid, defensie, staatsveiligheid (met inbegrip van het economisch welzijn van de staat wanneer de activiteit verband houdt met de staatsveiligheid) en de wetshandhaving op strafrechtelijk gebied. Bijgevolg doet deze richtlijn geen afbreuk aan de mogelijkheid voor de lidstaten om wettelijk toegestane interceptie van elektronische communicatie uit te voeren of andere maatregelen vast te stellen, wanneer dat voor één van voornoemde doeleinden noodzakelijk is, mits zij daarbij het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, zoals geïnterpreteerd in de uitspraken van het Europees Hof voor de Rechten van de Mens, in acht nemen. Zulke maatregelen dienen passend te zijn voor, en strikt evenredig met, het beoogde doel en noodzakelijk in een democratische samenleving en moeten adequate waarborgen bevatten overeenkomstig het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden.

[…]

(15) Een communicatie kan naamgevings-, nummerings- of adresseringsgegevens omvatten die door de verzender van een communicatie of door de gebruiker van een verbinding worden verstrekt om de communicatie tot stand te brengen. Wanneer deze gegevens door het netwerk waarover de communicatie wordt doorgegeven, worden omgezet om de transmissie tot stand te brengen, behoren zij ook tot de verkeersgegevens. […]

[…]

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

6 Artikel 1 van richtlijn 2002/58, met als opschrift 'Werkingssfeer en doelstelling', luidt:

"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 elektronische-communicatieapparatuur en -diensten in de Gemeenschap.

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

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

7 Artikel 2 van richtlijn 2002/58 heeft als opschrift 'Definities' en bepaalt:

"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 elektronische-communicatienetwerken en -diensten (kaderrichtlijn) [(*PB* 2002, L 108, blz. 33)] van toepassing.

Daarnaast wordt in deze richtlijn verstaan onder:

[…]

b) 'verkeersgegevens': gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronische-communicatienetwerk of voor de facturering ervan;

c) 'locatiegegevens': gegevens die in een elektronische-communicatienetwerk of door een elektronische-communicatiedienst worden verwerkt, waarmee de geografische positie van de eindapparatuur van een gebruiker van een

openbare elektronische-communicatiedienst wordt aangegeven;

d) 'communicatie': informatie die wordt uitgewisseld of overgebracht tussen een eindig aantal partijen door middel van een openbare elektronische-communicatiedienst. Dit omvat niet de informatie die via een omroepdienst over een elektronische-communicatienetwerk wordt overgebracht, behalve wanneer de informatie kan worden gerelateerd aan de identificeerbare abonnee of gebruiker die de informatie ontvangt;

[…]"

8 Artikel 3 van richtlijn 2002/58, met als opschrift 'Betrokken diensten', bepaalt:

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

9 Artikel 5 van die richtlijn, met als opschrift 'Vertrouwelijk karakter van de communicatie', bepaalt:

"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 elektronische-communicatiediensten. 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. […]

[…]

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. […]"

10 Artikel 6 van richtlijn 2002/58 heeft als opschrift 'Verkeersgegevens' en luidt:

"1. Verkeersgegevens met betrekking tot abonnees en gebruikers die worden verwerkt en opgeslagen door de aanbieder van een openbaar elektronische-communicatienetwerk 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.

[…]"

11 Artikel 15 van die richtlijn, met als opschrift 'Toepassing van een aantal bepalingen van richtlijn [95/46]', 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 onbevoegd 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 Gemeenschapsrecht, met inbegrip van de beginselen als bedoeld in artikel 6, leden 1 en 2, van het Verdrag betreffende de Europese Unie."

Spaans recht

Wet 25/2007

12 Artikel 1 van Ley 25/2007 de conservación de datos relativos a las comunicaciones electrónicas y a la redes públicas de comunicaciones (wet 25/2007 inzake de bewaring van gegevens betreffende elektronische communicatie en openbare communicatienetwerken) van 18 oktober 2007 (BOE nr. 251 van 19 oktober 2007, p. 42517), bepaalt:

"1. Deze wet strekt tot regulering van de verplichting van de aanbieders tot bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van elektronische-communicatiediensten of van openbare communicatienetwerken, alsook van de verplichting tot verstrekking van die gegevens aan bevoegde ambtenaren, mits ze worden opgevraagd met rechterlijke toestemming met het oog op het opsporen, onderzoeken en vervolgen van ernstige delicten als bedoeld in de Código Penal (Spaans strafwetboek) of in de bijzondere strafwetten.

2. Deze wet heeft betrekking op verkeers- en locatiegegevens van natuurlijke en rechtspersonen, evenals op de daarmee verband houdende gegevens die nodig zijn om de abonnee of geregistreerde gebruiker te identificeren.

[…]"

Strafwetboek

13 Artikel 13 van Ley Orgánica 10/1995 del Código Penal (strafwetboek) van 23 november 1995 (BOE nr. 281 van 24 november 1995, p. 33987) bepaalt in lid 1:

"Ernstige delicten zijn die waarop de wet een zware straf stelt."

14 Artikel 33 van dat wetboek bepaalt:

"1. De straffen zijn naar hun aard en duur ingedeeld in zware, minder zware en lichte straffen.

2. Zware straffen zijn:

a) de herzienbare levenslange gevangenisstraf.

b) de gevangenisstraf van meer dan vijf jaar.

[…]"

Wetboek van strafvordering

15 Na de feiten in het hoofdgeding is de Ley de Enjuiciamiento Criminal (wetboek van strafvordering) gewijzigd door Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica (organieke wet 13/2015 tot wijziging van het wetboek van strafvordering ter versterking van de procedurele waarborgen en regulering van technologische onderzoeksmethodes) van 5 oktober 2015 (BOE nr. 239 van 6 oktober 2015, p. 90192).

16 Deze wet is in werking getreden op 6 december 2015 en heeft aan het wetboek van strafvordering bepalingen toegevoegd inzake de toegang tot door aanbieders van elektronische-communicatiediensten bewaarde gegevens over telefonische en elektronische communicatie.

17 Artikel 579, lid 1, van het wetboek van strafvordering, in de versie na de organieke wet 13/2015, luidt:

"1. De rechter kan toestemming geven voor de interceptie van de privécorrespondentie die de verdachte per post, telegraaf, fax, Burofax of internationale postwissels verzendt of ontvangt, alsook voor het openen en onderzoeken hiervan indien er aanwijzingen zijn dat hiermee een voor de zaak relevant feit of relevante factor aan het licht kan worden gebracht of kan worden nagetrokken, indien het onderzoek zich op één van de volgende delicten richt:

1º) doleuze delicten waarop een maximumgevangenisstraf van ten minste drie jaar is gesteld;

2º) delicten gepleegd door een criminele groep of organisatie;

3º) terroristische delicten.

[…]"

18 Artikel 588 ter, onder j), van dat wetboek bepaalt:

"1. Elektronische gegevens die uit hoofde van de wetgeving betreffende de bewaring van gegevens inzake elektronische communicatie dan wel eigener beweging om commerciële of andere redenen worden bewaard door aanbieders van communicatiediensten of personen die communicatie faciliteren, en verband houden met communicatieprocessen, mogen uitsluitend met rechterlijke toestemming worden verstrekt voor gebruik in de procedure.

2. Wanneer kennisneming van deze gegevens onontbeerlijk is voor het onderzoek, wordt de bevoegde rechter verzocht om toestemming voor het verzamelen van de informatie die zich bevindt in de geautomatiseerde bestanden van de aanbieders van telecommunicatiediensten, waaronder het zoeken naar kruisverbanden of intelligent opsporen van gegevens, mits de aard van de bekend te maken gegevens en de redenen voor de verstrekking van die gegevens worden gepreciseerd."

Hoofdgeding en prejudiciële vragen

19 Hernández Sierra heeft bij de politie een klacht ingediend wegens diefstal met geweld waarvan hij op 16 februari 2015 slachtoffer was geworden en waarbij zijn portefeuille en mobiele telefoon waren gestolen en hij gewond was geraakt.

20 Op 27 februari 2015 heeft de gerechtelijke politie de onderzoeksrechter verzocht om verschillende aanbieders van elektronische-communicatiediensten te gelasten de telefoonnummers door te geven die tussen 16 en 27 februari 2015 waren geactiveerd met het internationaal identificatienummer voor mobiele apparaten (hierna: 'IMEI-nummer') van de gestolen mobiele telefoon, alsook de persoonsgegevens betreffende de civiele identiteit van de houders of gebruikers van de telefoonnummers die overeenkwamen met de met dat IMEI-nummer geactiveerde simkaarten, zoals hun naam, voornaam en, in voorkomend geval, adres.

21 De onderzoeksrechter heeft dit verzoek bij beschikking van 5 mei 2015 afgewezen. Hij heeft om te beginnen geoordeeld dat de gevraagde maatregel niet geschikt was om de daders van het delict te identificeren, en voorts dat gegevens die door aanbieders van elektronische-communicatiediensten werden bewaard, volgens wet 25/2007 slechts mochten worden verstrekt voor ernstige delicten. In het strafwetboek stonden op ernstige delicten vrijheidsstraffen van meer dan vijf jaar, en de feiten in het hoofdgeding leken geen dergelijk delict te vormen, aldus de onderzoeksrechter.

22 Het openbaar ministerie heeft tegen deze beschikking hoger beroep ingesteld bij de verwijzende rechter, aangezien het van oordeel was dat toestemming had moeten worden gegeven voor het verstrekken van de betrokken gegevens, gelet op de aard van de feiten en gezien een arrest van de Tribunal Supremo (hoogste rechterlijke instantie, Spanje) van 26 juli 2010 in een vergelijkbare zaak.

23 De verwijzende rechter geeft aan dat de Spaanse wetgever het wetboek van strafvordering ná de voormelde beschikking heeft gewijzigd met de organieke wet 13/2015. Deze wet, die naar verluidt pertinent is voor de uitkomst in het hoofdge-

ding, heeft volgens de verwijzende rechter twee nieuwe, alternatieve criteria ingevoerd om de ernst van een delict te bepalen. Het eerste is een materieel criterium, waarbij wordt nagegaan of de strafbaar gestelde gedragingen specifiek en ernstig van aard zijn en individuele en collectieve juridische belangen in bijzondere mate aantasten. Het tweede criterium dat de nationale wetgever heeft ingevoerd is formeel-normatief, namelijk de straf die op het betrokken delict staat. De drempel van drie jaar gevangenisstraf die daarin sindsdien wordt bepaald, bestrijkt echter de overgrote meerderheid van delicten. Overigens kan het belang dat de staat heeft bij het bestraffen van strafbare gedragingen, volgens de verwijzende rechter geen onevenredige inmenging in de in het Handvest verankerde grondrechten rechtvaardigen.

24 In dit verband meent de verwijzende rechter dat in het hoofdgeding de richtlijnen 95/46 en 2002/58 de aanknopingspunten vormen met het Handvest. De nationale regeling in het hoofdgeding valt dus overeenkomstig artikel 51, lid 1, van het Handvest binnen de werkingssfeer ervan, ook al is richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van richtlijn 2002/58/EG (*PB* 2006, L 105, p. 54), bij arrest van 8 april 2014, *Digital Rights Ireland e.a.* (C-293/12 en C-594/12, EU:C:2014:238 (*NJ* 2016/446, m.nt. E.J. Dommering; *red.*)), ongeldig verklaard.

25 Volgens de verwijzende rechter heeft het Hof in dat arrest erkend dat het bewaren en verstrekken van verkeersgegevens bijzonder zware inmengingen vormen in de door de artikelen 7 en 8 van het Handvest gewaarborgde rechten, en heeft het de criteria bepaald voor de beoordeling of het evenredigheidsbeginsel is nageleefd, waaronder de ernst van een delict, die de bewaring van en de toegang tot die gegevens voor onderzoeksdoeleinden rechtvaardigt.

26 In die omstandigheden heeft de Audiencia Provincial de Tarragona (provinciaal gerecht Tarragona, Spanje) de behandeling van de zaak geschorst en het Hof verzocht om een prejudiciële beslissing over de volgende vragen:

> "1) Geldt als criterium om te bepalen of een delict voldoende ernstig is om inmenging in de door de artikelen 7 en 8 van het [Handvest] erkende grondrechten te rechtvaardigen, uitsluitend de straf die kan worden opgelegd ter zake van het onderzochte delict of is het bovendien noodzakelijk dat door de strafbaar gestelde gedraging individuele en/of collectieve rechtsgoederen in bijzondere mate worden aangetast?
>
> 2) Indien het verenigbaar is met de constitutionele beginselen van de Unie die het Hof in zijn arrest [van 8 april 2014, *Digital Rights Ireland e.a.*, C-293/12 en C-594/12, EU:C:2014:238 (*NJ* 2016/446, m.nt. E.J. Dommering; *red.*)] heeft toegepast als maatstaven voor de strikte toetsing van richtlijn [2002/58], dat de ernst van het delict uitsluitend wordt vastgesteld op basis van de op te leggen straf, wat zou dan het minimumniveau van de straf moeten zijn? Zou een algemeen vereiste van minimaal drie jaar voldoen?"

Procedure bij het Hof

27 Bij beslissing van de president van het Hof van 23 mei 2016 werd de procedure bij het Hof geschorst in afwachting van de uitspraak in de gevoegde zaken *Tele2 Sverige en Watson e.a.*, C-203/15 en C-698/15 (arrest van 21 december 2016, EU:C:2016:970 (*NJ* 2017/186, m.nt. E.J. Dommering; *red.*); hierna: 'arrest *Tele2 Sverige en Watson e.a.*'). Na de uitspraak in deze zaken werd de verwijzende rechter gevraagd of hij zijn verzoek om een prejudiciële beslissing wenste te handhaven dan wel in te trekken. In antwoord daarop heeft de verwijzende rechter bij brief van 30 januari 2017, ingekomen bij het Hof op 14 februari 2017, te kennen gegeven dat dat arrest hem zijns inziens niet toeliet om de in het hoofdgeding aan de orde zijnde nationale regeling met voldoende zekerheid te toetsen aan het Unierecht. Vervolgens is de procedure bij het Hof hervat op 16 februari 2017.

Beantwoording van de prejudiciële vragen

28 De Spaanse regering stelt enerzijds dat het Hof niet bevoegd is om het verzoek om een prejudiciële beslissing te beantwoorden, en anderzijds dat dit verzoek niet-ontvankelijk is.

Bevoegdheid van het Hof

29 In haar bij het Hof ingediende schriftelijke opmerkingen heeft de Spaanse regering — hierin ter terechtzitting gesteund door de regering van het Verenigd Koninkrijk — gesteld dat het Hof niet bevoegd is om op de prejudiciële vragen te antwoorden, omdat het hoofdgeding volgens artikel 3, lid 2, eerste streepje, van richtlijn 95/46 en artikel 1, lid 3, van richtlijn 2002/58 uitgesloten is van de werkingssfeer van deze twee richtlijnen. Het geding valt dus niet binnen de werkingssfeer van het Unierecht, zodat het Handvest — volgens artikel 51, lid 1, ervan — niet van toepassing is.

30 Volgens de Spaanse regering heeft het Hof in het arrest *Tele2 Sverige en Watson e.a.* weliswaar geoordeeld dat een wettelijke maatregel die de toegang van de nationale autoriteiten tot door aanbieders van elektronische-communicatiediensten bewaarde gegevens regelt, binnen de werkingssfeer van richtlijn 2002/58 valt, maar gaat het in casu om een verzoek van een overheidsinstantie om, krachtens een rechterlijke beslissing in het kader van een strafrechtelijk onderzoek, toegang te verkrijgen tot door aanbieders van elektronische-communicatiediensten bewaarde persoonsgegevens. De Spaanse regering leidt daaruit af dat het indienen van een dergelijk verzoek om toegang tot de uitoefening door nationale autoriteiten van het ius puniendi be-

hoort, en dus een activiteit van de staat op strafrechtelijk gebied betreft die onder de uitzondering valt van artikel 3, lid 2, eerste streepje, van richtlijn 95/46 en artikel 1, lid 3, van richtlijn 2002/58.

31 Bij de beoordeling van deze exceptie van onbevoegdheid zij erop gewezen dat artikel 1 van richtlijn 2002/58 in lid 1 ervan bepaalt dat deze richtlijn voorziet in de harmonisering van de regelgeving van de lidstaten die nodig is om onder meer 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. Lid 2 van artikel 1 van die richtlijn bepaalt dat deze richtlijn voor de doelstellingen van lid 1 een specificatie van en een aanvulling op richtlijn 95/46 vormt.

32 Volgens artikel 1, lid 3, van richtlijn 2002/58 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 (arrest *Tele2 Sverige en Watson e.a.*, punt 69 en aldaar aangehaalde rechtspraak). 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 ontplooien (zie naar analogie, met betrekking tot artikel 3, lid 2, eerste streepje, van richtlijn 95/46, arrest van 10 juli 2018, *Jehovan Todistajat*, C-25/17, EU:C:2018:551, punt 38 en aldaar aangehaalde rechtspraak).

33 Volgens artikel 3 van richtlijn 2002/58 is deze richtlijn van toepassing 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 *Tele2 Sverige en Watson e.a.*, punt 70).

34 Met betrekking tot artikel 15, lid 1, van richtlijn 2002/58 heeft het Hof reeds geoordeeld dat de daarin bedoelde wettelijke maatregelen binnen de werkingssfeer van die richtlijn vallen, ook al betreffen zij specifieke activiteiten van staten of overheidsdiensten die niets van doen hebben met de gebieden waarop particulieren activiteiten ontplooien, en zelfs al stemmen de met die maatregelen nagestreefde doelstellingen grotendeels overeen met de doelstellingen van de in artikel 1, lid 3, van richtlijn 2002/58 bedoelde activiteiten. Artikel 15, lid 1, van deze richtlijn vooronderstelt immers noodzakelijkerwijs dat de daarin bedoelde nationale maatregelen binnen de werkingssfeer van die richtlijn vallen, aangezien deze richtlijn uitdrukkelijk bepaalt dat lidstaten die maatregelen slechts met inachtneming van de in de richtlijn geformuleerde voorwaarden mogen treffen. Bovendien regelen de in artikel 15, lid 1, van richtlijn 2002/58 bedoelde wettelijke maatregelen de activiteit van aanbieders van elektronische-communicatiediensten voor de in die bepaling vermelde doeleinden (zie in die zin arrest *Tele2 Sverige en Watson e.a.*, punten 72–74).

35 Het Hof is tot de slotsom gekomen dat artikel 15, lid 1, gelezen in samenhang met artikel 3 van richtlijn 2002/58, aldus moet worden uitgelegd dat binnen de werkingssfeer van deze richtlijn niet alleen wettelijke maatregelen vallen die aanbieders van elektronische-communicatiediensten de verplichting opleggen om verkeers- en locatiegegevens te bewaren, maar ook wettelijke maatregelen inzake de toegang van nationale autoriteiten tot door die aanbieders bewaarde gegevens (zie in die zin arrest *Tele2 Sverige en Watson e.a.*, punten 75–76).

36 De door artikel 5, lid 1, van richtlijn 2002/58 gewaarborgde bescherming van de vertrouwelijkheid van communicatie en daarmee verband houdende verkeersgegevens, geldt immers voor de door alle andere personen dan de gebruikers getroffen maatregelen, ongeacht of het daarbij gaat om particuliere personen of entiteiten dan wel om overheidsentiteiten. Zoals in overweging 21 van die richtlijn wordt bevestigd, beoogt deze richtlijn 'elke' onbevoegde 'toegang' tot communicatie, daaronder begrepen de toegang tot 'gegevens over die communicatie', te verhinderen teneinde het vertrouwelijke karakter van elektronische communicatie te beschermen (arrest *Tele2 Sverige en Watson e.a.*, punt 77).

37 Hieraan moet worden toegevoegd dat wanneer wettelijke maatregelen aanbieders van elektronische-communicatiediensten de verplichting opleggen om persoonsgegevens te bewaren of om bevoegde nationale autoriteiten daar toegang toe te verlenen, dit noodzakelijkerwijs impliceert dat die aanbieders die gegevens verwerken (zie in die zin arrest *Tele2 Sverige en Watson e.a.*, punten 75–78). Dergelijke maatregelen, die dus de activiteiten van die aanbieders regelen, kunnen dan ook niet worden gelijkgesteld met de in artikel 1, lid 3, van richtlijn 2002/58 bedoelde specifieke activiteiten van staten.

38 Zoals in casu uit de verwijzingsbeslissing blijkt, is het verzoek in het hoofdgeding, waarmee de gerechtelijke politie via rechterlijke toestemming toegang wil verkrijgen tot door aanbieders van elektronische-communicatiediensten bewaarde persoonsgegevens, gebaseerd op wet 25/2007 die de toegang van overheidsinstanties tot dergelijke gegevens regelt, gelezen in samenhang met het wetboek van strafvordering zoals van toepassing ten tijde van de feiten in het hoofdgeding. Met deze regeling kan de gerechtelijke politie, wanneer zij de op grond van die regeling gevraagde rechterlijke toestemming verkrijgt, aanbieders van elektronische-communicatiediensten verplichten om persoonsgegevens ter

beschikking te stellen en om deze gegevens zodoende, gelet op de definitie in artikel 2, onder b), van richtlijn 95/46, die volgens artikel 2, lid 1, van richtlijn 2002/58 van toepassing is in de context van laatstgenoemde richtlijn, te 'verwerken' in de zin van deze twee richtlijnen. De betrokken regeling regelt dus activiteiten van aanbieders van elektronische-communicatiediensten en valt bijgevolg binnen de werkingssfeer van richtlijn 2002/58.

39 In die situatie kan de door de Spaanse regering aangevoerde omstandigheid dat het toegangsverzoek werd ingediend in het kader van een strafrechtelijk onderzoek, niet tot gevolg hebben dat richtlijn 2002/58 overeenkomstig artikel 1, lid 3, ervan niet van toepassing is op het hoofdgeding.

40 Het is dienaangaande eveneens irrelevant dat het toegangsverzoek in het hoofdgeding, zoals uit het schriftelijke antwoord van de Spaanse regering op een door het Hof gestelde vraag blijkt en zoals zowel deze regering als het openbaar ministerie ter terechtzitting hebben bevestigd, ertoe strekt toegang te verkrijgen tot uitsluitend de telefoonnummers die overeenstemmen met de met het IMEI-nummer van de gestolen mobiele telefoon geactiveerde simkaarten en de civiele-identiteitsgegevens van de houders van die kaarten, zoals hun naam, voornaam en, in voorkomend geval, adres, en niet tot gegevens betreffende de oproepen die met die simkaarten tot stand zijn gebracht of over de locatie van de gestolen mobiele telefoon.

41 Zoals de advocaat-generaal in punt 54 van zijn conclusie heeft opgemerkt, is richtlijn 2002/58 volgens artikel 1, lid 1, en artikel 3 ervan immers van toepassing op elke verwerking van persoonsgegevens in het kader van de levering van elektronische-communicatiediensten. Bovendien dekt het begrip 'verkeersgegevens' volgens artikel 2, tweede alinea, onder b), van die richtlijn alle 'gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronische-communicatienetwerk of voor de facturering ervan'.

42 Aangaande dit laatste punt, en wat meer in het bijzonder civiele-identiteitsgegevens van simkaarthouders betreft, blijkt uit overweging 15 van richtlijn 2002/58 dat verkeersgegevens onder meer naam en adres kunnen omvatten van de persoon die een communicatie verzendt of een verbinding gebruikt om een communicatie tot stand te brengen. Civiele-identiteitsgegevens van simkaarthouders kunnen overigens noodzakelijk blijken om de geleverde elektronische-communicatiediensten te kunnen factureren en maken dus deel uit van de verkeersgegevens, zoals die in artikel 2, tweede alinea, onder b), van die richtlijn worden gedefinieerd. Bijgevolg vallen die gegevens binnen de werkingssfeer van richtlijn 2002/58.

43 Het Hof is derhalve bevoegd om de vraag van de verwijzende rechter te beantwoorden.

Ontvankelijkheid

44 Volgens de Spaanse regering is het verzoek om een prejudiciële beslissing niet-ontvankelijk omdat daarin niet duidelijk wordt aangegeven op grond van welke Unierechtelijke bepalingen het Hof wordt verzocht zich uit te spreken. Bovendien is het in het hoofdgeding aan de orde zijnde verzoek van de gerechtelijke politie niet bedoeld om de oproepen die tot stand zijn gebracht via de met het IMEI-nummer van de gestolen mobiele telefoon geactiveerde simkaarten af te tappen, maar om die kaarten te linken aan de houders ervan, zodat niet wordt geraakt aan de vertrouwelijkheid van de communicatie. Het in de prejudiciële vragen genoemde artikel 7 van het Handvest is dan ook irrelevant in de onderhavige zaak, aldus de Spaanse regering.

45 Volgens vaste rechtspraak van het Hof is het uitsluitend een zaak van de nationale rechter aan wie het geschil is voorgelegd en die de verantwoordelijkheid voor de te geven rechterlijke beslissing draagt, om, rekening houdend met de bijzonderheden van het geval, zowel de noodzaak van een prejudiciële beslissing voor het wijzen van zijn vonnis als de relevantie van de vragen die hij aan het Hof voorlegt, te beoordelen. Wanneer de gestelde vragen betrekking hebben op de uitlegging van het Unierecht, is het Hof dus in beginsel verplicht om daarop te antwoorden. Het Hof kan slechts weigeren uitspraak te doen op een prejudiciële vraag van een nationale rechterlijke instantie wanneer duidelijk blijkt dat de gevraagde uitlegging van het Unierecht geen verband houdt met een reëel geschil of met het voorwerp van het hoofdgeding, of wanneer het vraagstuk van hypothetische aard is, of het Hof niet beschikt over de gegevens, feitelijk en rechtens, die noodzakelijk zijn om een nuttig antwoord te geven op de gestelde vragen (arrest van 10 juli 2018, *Jehovan Todistajat*, C-25/17, EU:C:2018:551, punt 31 en aldaar aangehaalde rechtspraak).

46 In het onderhavige geval bevat de verwijzingsbeslissing voldoende feitelijke en juridische gegevens om zowel te achterhalen op welke bepalingen van Unierecht de prejudiciële vragen betrekking hebben als de draagwijdte van die vragen te begrijpen. Uit de verwijzingsbeslissing blijkt in het bijzonder dat de prejudiciële vragen ertoe strekken de verwijzende rechter in staat te stellen te beoordelen of en in welke mate de nationale regeling, waarop het in het hoofdgeding aan de orde zijnde verzoek van de gerechtelijke politie is gebaseerd, een doel nastreeft dat een aantasting van de in de artikelen 7 en 8 van het Handvest neergelegde grondrechten kan rechtvaardigen. Welnu, volgens de aanwijzingen van diezelfde rechter valt de nationale regeling binnen de werkingssfeer van richtlijn 2002/58 en is het Handvest dus van toepassing op het hoofdgeding. De prejudiciële vragen houden aldus rechtstreeks verband met het voorwerp van het hoofdgeding en kunnen dan ook niet als hypothetisch worden beschouwd.

47 In die omstandigheden zijn de prejudiciële vragen ontvankelijk.

Ten gronde

48 Met zijn twee vragen, die samen moeten worden onderzocht, wenst de verwijzende rechter in wezen te vernemen of artikel 15, lid 1, van richtlijn 2002/58, gelezen in samenhang met de artikelen 7 en 8 van het Handvest, aldus moet worden uitgelegd dat de toegang van overheidsinstanties tot de identificatiegegevens van de houders van met een gestolen mobiele telefoon geactiveerde simkaarten — zoals hun naam, voornaam en, in voorkomend geval, adres — een zodanig ernstige inmenging in de door die artikelen van het Handvest gewaarborgde grondrechten van deze laatsten vormt dat die toegang, wat het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten betreft, zou moeten worden beperkt tot de bestrijding van zware criminaliteit en, zo ja, aan de hand van welke criteria de ernst van het betrokken delict moet worden beoordeeld.

49 In dit verband blijkt uit de verwijzingsbeslissing dat, zoals de advocaat-generaal in punt 38 van zijn conclusie in wezen heeft opgemerkt, het verzoek om een prejudiciële beslissing er niet toe strekt om uit te maken of de aanbieders van elektronische-communicatiediensten de in het hoofdgeding aan de orde zijnde persoonsgegevens hebben bewaard met inachtneming van de voorwaarden van artikel 15, lid 1, van richtlijn 2002/58, gelezen in samenhang met de artikelen 7 en 8 van het Handvest. Zoals uit punt 46 van het onderhavige arrest blijkt, betreft het verzoek uitsluitend de vraag of en in welke mate het doel dat met de in het hoofdgeding aan de orde zijnde nationale regeling wordt nagestreefd, kan rechtvaardigen dat overheidsinstanties zoals de gerechtelijke politie toegang hebben tot dergelijke gegevens, en gaat het verzoek niet over de andere toegangsvoorwaarden die uit voormeld artikel 15, lid 1, voortvloeien.

50 De verwijzende rechter vraagt zich in het bijzonder af welke elementen in aanmerking moeten worden genomen bij de beoordeling of delicten waarvoor politiediensten in het kader van een onderzoek toegang kan worden verleend tot persoonsgegevens die door aanbieders van elektronische-communicatiediensten worden bewaard, voldoende ernstig zijn om de inmenging die een dergelijke toegang betekent in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten, zoals uitgelegd door het Hof in zijn arrest van 8 april 2014, *Digital Rights Ireland e.a.* (C-293/12 en C-594/12, EU:C:2014:238 (*NJ* 2016/446, m.nt. E.J. Dommering; *red.*)), en in het arrest *Tele2 Sverige en Watson e.a.*, te rechtvaardigen.

51 Wat betreft de vraag of sprake is van inmenging in die grondrechten, zij eraan herinnerd dat, zoals de advocaat-generaal in de punten 76 en 77 van zijn conclusie heeft aangegeven, de toegang van overheidsinstanties tot dergelijke gegevens inmenging in het in artikel 7 van het Handvest neergelegde grondrecht op eerbiediging van het privéleven vormt, zelfs al kan die inmenging om bepaalde redenen niet als 'ernstig' worden aangemerkt en zonder dat van belang is of de informatie over het privéleven al dan niet gevoelig is en of de betrokkenen door die inmenging enig nadeel hebben ondervonden. Een dergelijke toegang vormt tevens inmenging in het door artikel 8 van het Handvest gewaarborgde grondrecht op bescherming van persoonsgegevens, aangezien die toegang een verwerking van persoonsgegevens is [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].

52 Wat betreft de doelstellingen die een rechtvaardiging kunnen vormen voor een nationale regeling als die in het hoofdgeding, die de toegang van overheidsinstanties tot door aanbieders van elektronische-communicatiediensten bewaarde gegevens regelt en die aldus afwijkt van het beginsel van de vertrouwelijkheid van elektronische communicatie, zij eraan herinnerd dat de in artikel 15, lid 1, eerste zin, van richtlijn 2002/58 gegeven opsomming van doelstellingen exhaustief is, zodat die toegang daadwerkelijk en strikt op een van die doelstellingen moet berusten (zie in die zin arrest *Tele2 Sverige en Watson e.a.*, punten 90 en 115).

53 Aangaande de doelstelling strafbare feiten te voorkomen, te onderzoeken, op te sporen en te vervolgen, dient te worden geconstateerd dat het daarbij volgens de bewoordingen van artikel 15, lid 1, eerste zin, van richtlijn 2002/58 evenwel niet alleen over de bestrijding van ernstige delicten maar over 'strafbare feiten' in het algemeen gaat.

54 Stellig heeft het Hof in dit verband geoordeeld dat ter zake van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, alleen de bestrijding van zware criminaliteit kan rechtvaardigen dat overheidsinstanties toegang krijgen tot door aanbieders van elektronische-communicatiediensten bewaarde persoonsgegevens waaruit, in hun geheel beschouwd, precieze conclusies kunnen worden getrokken over het privéleven van de betrokken personen (zie in die zin arrest *Tele2 Sverige en Watson e.a.*, punt 99).

55 Het Hof heeft die uitlegging echter gemotiveerd met de overweging dat de met een toegangsregeling nagestreefde doelstelling in verhouding moet staan tot de ernst van de inmenging in de betrokken grondrechten die deze ingreep meebrengt (zie in die zin arrest *Tele2 Sverige en Watson e.a.*, punt 115).

56 Volgens het evenredigheidsbeginsel kan ter zake van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, ernstige inmenging immers slechts worden gerechtvaardigd door de doelstelling om — eveneens 'ernstige' — criminaliteit te bestrijden.

57 Is de inmenging die een dergelijke toegang veroorzaakt daarentegen niet ernstig, dan kan die toegang worden gerechtvaardigd door de doelstelling van het voorkomen, onderzoeken, opsporen en vervolgen van 'strafbare feiten' in het algemeen.

58 Allereerst moet dus worden uitgemaakt of in casu, gelet op de omstandigheden van de onder-

havige zaak, de inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten die zou voortvloeien uit het feit dat aan de gerechtelijke politie toegang tot de in het hoofdgeding aan de orde zijnde gegevens wordt verleend, als 'ernstig' moet worden beschouwd.

59 In dit verband heeft het verzoek in het hoofdgeding, waarmee de gerechtelijke politie in een strafrechtelijk onderzoek via rechterlijke toestemming toegang wil verkrijgen tot door aanbieders van elektronische-communicatiediensten bewaarde persoonsgegevens, louter tot doel de houders te identificeren van de simkaarten die gedurende een periode van twaalf dagen met het IMEI-nummer van de gestolen mobiele telefoon zijn geactiveerd. Zoals in punt 40 van het onderhavige arrest is uiteengezet, strekt dat verzoek er enkel toe om toegang te verkrijgen tot de telefoonnummers die overeenstemmen met die simkaarten en tot de civiele-identiteitsgegevens van de houders van die kaarten, zoals hun naam, voornaam en, in voorkomend geval, adres. Zoals zowel de Spaanse regering als het openbaar ministerie ter terechtzitting heeft bevestigd, gaat het daarbij echter niet over de communicatie die met de gestolen mobiele telefoon tot stand is gebracht of over de locatie van die telefoon.

60 Met de via het toegangsverzoek in het hoofdgeding beoogde gegevens is het dus blijkbaar alleen mogelijk om, gedurende een bepaalde periode, de met de gestolen mobiele telefoon geactiveerde simkaart(en) in verband te brengen met de civiele identiteit van de houders van die simkaarten. Zonder aanvullende gegevens over de communicatie die met die simkaarten tot stand is gebracht en over de locatie, kan met die gegevens noch de datum, het uur, de duur of de ontvanger van de met de betrokken simkaart(en) verrichte oproepen worden achterhaald, noch waar die communicatie heeft plaatsgevonden of hoe vaak in een gegeven periode met bepaalde personen is gecommuniceerd. Uit die gegevens kunnen dus geen nauwkeurige conclusies over het privéleven van de betrokken personen worden getrokken.

61 In die omstandigheden kan de toegang tot de in het verzoek in het hoofdgeding bedoelde gegevens niet worden aangemerkt als een 'ernstige' inmenging in de grondrechten van de personen waarop de gegevens betrekking hebben.

62 Zoals uit de punten 53 tot en met 57 van dit arrest blijkt, kan de inmenging die een dergelijke gegevenstoegang zou veroorzaken dus worden gerechtvaardigd door de in artikel 15, lid 1, eerste zin, van richtlijn 2002/58 vermelde doelstelling om 'strafbare feiten' in het algemeen te voorkomen, te onderzoeken, op te sporen en te vervolgen, zonder dat deze strafbare feiten als 'ernstig' moeten worden aangemerkt.

63 Gelet op het voorgaande dient op de gestelde vragen te worden geantwoord dat artikel 15, lid 1, van richtlijn 2002/58, gelezen in samenhang met de artikelen 7 en 8 van het Handvest, aldus moet worden uitgelegd dat de toegang van overheidsinstanties tot de identificatiegegevens van houders van met een gestolen mobiele telefoon geactiveerde simkaarten — zoals hun naam, voornaam en, in voorkomend geval, adres — geen zodanig ernstige inmenging in de door die artikelen van het Handvest gewaarborgde grondrechten van laatstgenoemden oplevert dat die toegang — op het gebied van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten — moet worden beperkt tot de bestrijding van zware criminaliteit.

(…)

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

Noot

1. Het gaat in deze zaak om het onderzoek naar de bij aanbieders van elektronische communicatiediensten opgeslagen verkeersgegevens om te kunnen achterhalen wie de dader kan zijn geweest van een diefstal met geweld waarbij een portefeuille en mobiele telefoon waren gestolen en het slachtoffer gewond was geraakt. Om precies te zijn: om op verzoek van de politie op te geven welke nummers tussen 16 en 27 februari 2015 waren geactiveerd met het internationaal identificatienummer voor mobiele apparaten (het zogenaamde 'IMEI-nummer') van de gestolen mobiele telefoon, alsook de persoonsgegevens betreffende de civiele identiteit van de houders of gebruikers van de telefoonnummers die overeenkwamen met de met dat IMEI-nummer geactiveerde simkaarten, zoals hun naam, voornaam en, in voorkomend geval, adres. De Spaanse rechter achtte de gevraagde maatregel niet geschikt om de daders van het delict te identificeren, en hij vond het geen 'ernstig delict'. In het Spaanse strafwetboek stonden op ernstige delicten vrijheidsstraffen van meer dan vijf jaar, en de feiten in het hoofdgeding leken niet een dergelijk delict te zijn. Bij het HvJ EU ging het om de juiste uitleg van de algemene en de e-privacyrichtlijn (95/46, 2002/58). In de beantwoording van de vragen wordt voortgebouwd op de uitspraken *Digital Rights*, zaken C-293/12 en C-594/12, *NJ* 2016/446, m.nt. E.J. Dommering, en *Tele-2*, zaken C-203/15 en C-698/15, *NJ* 2017/186, m.nt. E.J. Dommering). Een soortgelijke zaak uit Estland is op het moment van het schrijven van deze noot nog aanhangig (zaak C-746/18).

2. Het opslaan van — en het geven van inzage in opgeslagen verkeersgegevens is uitvoerig aan de orde geweest in het genoemde arrest *Digital Rights*. Volgens de verwijzende rechter heeft het Hof in dat arrest erkend dat het bewaren van — en geven van inzage in verkeersgegevens bijzonder zware inmengingen vormen in de door de artikelen 7 en 8 van het Handvest gewaarborgde privacy rechten, en heeft het de criteria bepaald voor de beoordeling of het evenredigheidsbeginsel is nageleefd, waaronder de ernst van een delict, die de bewaring van en de toegang tot die gegevens voor onderzoeksdoelein-

den rechtvaardigen. De Spaanse regering stelde zich op het standpunt dat het Hof niet bevoegd was die vraag te beantwoorden, omdat dit een strafrechtelijke aangelegenheid betreft die artikel 3 lid 2 van Richtlijn 95/46 en artikel 1 lid 3 van Richtlijn 2002/58 (onder verwijzing naar het verdrag) uitsluiten van het Unierecht. Het Hof verwerpt dit verweer (overwegingen 34 e.v. onder verwijzing naar de onder 1 genoemde arresten, waar dezelfde kwestie was opgeworpen). De richtlijnen beogen immers de vertrouwelijkheid van de communicatie tegen iedere publieke interventie te beschermen. Daaraan kan niet afdoen dat het verzoek tot inzage in het kader van een strafrechtelijk onderzoek werd gedaan. Bovendien dekt het begrip 'verkeersgegeven' iedere verwerking van persoonsgegevens.

3. Dit zo zijnde, vat het Hof de gestelde vragen als volgt samen: "Met zijn twee vragen, die samen moeten worden onderzocht, wenst de verwijzende rechter in wezen te vernemen of artikel 15, lid 1, van richtlijn 2002/58, gelezen in samenhang met de artikelen 7 en 8 van het Handvest, aldus moet worden uitgelegd dat de toegang van overheidsinstanties tot de identificatiegegevens van de houders van met een gestolen mobiele telefoon geactiveerde simkaarten — zoals hun naam, voornaam en, in voorkomend geval, adres — een zodanig ernstige inmenging in de door die artikelen van het Handvest gewaarborgde grondrechten van deze laatsten vormt dat die toegang, wat het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten betreft, zou moeten worden beperkt tot de bestrijding van zware criminaliteit en, zo ja, aan de hand van welke criteria de ernst van het betrokken delict moet worden beoordeeld." Het gaat dus om de 'ernst van de inmenging'. Wel stelt het Hof in overweging 51 dat ook een 'niet ernstige' inmenging een inbreuk vormt op het privacyrecht.

4. De kern van de overweging van het Hof is de toepassing van het evenredigheidsbeginsel, namelijk dat de mate van inmenging evenredig moet zijn aan de ernst van het nagestreefde doel (bestrijding van zware criminaliteit). Het Hof kijkt eerst naar de ernst van de inmenging. Is de inmenging niet ernstig dan kan een algemene doelstelling als het bestrijden van strafbare feiten in het algemeen een voldoende rechtvaardiging zijn. Welnu: het Hof vindt die inmenging in dit geval niet ernstig. Waarom? Het antwoord op die vraag vinden we in overweging 61:

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

5. En dus zegt het Hof: in dit geval kon het verzoek tot inzage ter bestrijding van strafbare (niet ernstige) feiten door de beugel. Zodra die gegevens inzicht verschaffen in datum, tijd, duur van de communicatie en de identiteit van de betrokken personen met wie is gecommuniceerd wordt de inbreuk ernstig en moet een zwaardere rechtvaardiging worden aangevoerd.

6. Voor de Nederlandse providers die verkeersgegevens opslaan is artikel 13.4 Tw de basis. Dat artikel bepaalt dat zij onverwijld moeten voldoen aan de vorderingen die op grond van de artikelen 126n, na, u, ua, en zi Sv worden gedaan of de opdrachten die op grond van de artikelen 55 en 56 Wiv (Wet op de inlichtingen- en veiligheidsdiensten 2017) worden gegeven. In het geval van artikel 126n Sv mag op grond van lid 1 onder a van dat artikel een vordering worden gedaan als het gaat om verdenking van misdrijven waarop een straf van vier jaar staat. Die kunnen waarschijnlijk wel kwalificeren als 'ernstige misdrijven', maar het zal toch een concrete afweging vergen. De bevoegdheid ex artikel 126 na (en de andere genoemde artikelen) betreffen de vordering tot het verstrekken van naam, adres, postcode, woonplaats, nummer en soort dienst. Dit kan kwalificeren als een minder verdergaande bevoegdheid in de zin van dit arrest, omdat geen inzicht wordt gegeven in tijdstip, plaats en duur van de communicatie. Artikel 56 Wiv beperkt zich ook tot laatstgenoemde gegevens. Artikel 55 Wiv is de meest vergaande bevoegdheid. De beperking moet hier gevonden in de algemene doelstelling van artikel 8 van de WIV, dat omschrijft waar de veiligheidsdiensten zich mee bezig moeten en mogen houden.

E.J. Dommering