Nr. 4 Prokuratuur

Hof van Justitie 2 maart 2021
ECLI:EU:C:2021:152

In zaak C-746/18,

betreffende een verzoek om een prejudiciële beslissing krachtens artikel 267 VWEU, ingediend door de Riigikohus (hoogste rechterlijke instantie, Estland) bij beslissing van 12 november 2018, ingekomen bij het Hof op 29 november 2018, in de strafzaak tegen

H. K.,
in tegenwoordigheid van:
Prokuratuur

wijst

HET HOF (Grote kamer),
samengesteld als volgt: K. Lenaerts, president, R. Silva de Lapuerta, vicepresident, J.-C. Bonichot, A. Arabadjiev, A. Prechal en L. Bay Larsen, kamerpresidenten, T. von Danwitz (rapporteur), M. Safjan, K. Jürimäe, C. Lycourgos en P. G. Xuereb, rechters,
advocaat-generaal: G. Pitruzzella,
griffier: C. Strömholm, administrateur,
gezien de stukken en na de terechtzitting op 15 oktober 2019,
gelet op de opmerkingen van:
- H. K., vertegenwoordigd door S. Reinsaar, vandeadvokaat,
- de Prokuratuur, vertegenwoordigd door T. Pern en M. Voogma als gemachtigden,
- de Estse regering, vertegenwoordigd door N. Grünberg als gemachtigde,
- de Deense regering, vertegenwoordigd door J. Nymann-Lindegren en M.S. Wolff als gemachtigden,
- Ierland, vertegenwoordigd door M. Browne, G. Hodge, J. Quaney en A. Joyce als gemachtigden, bijgestaan door D. Fennelly, barrister,
- de Franse regering, aanvankelijk vertegenwoordigd door D. Dubois, D. Colas, E. de Moustier en A.-L. Desjonquères, vervolgens door D. Dubois, E. de Moustier en A.-L. Desjonquères als gemachtigden,
- de Letse regering, aanvankelijk vertegenwoordigd door V. Kalniņa en I. Kucina, vervolgens door V. Soņeca en V. Kalniņa als gemachtigden,
- de Hongaarse regering, vertegenwoordigd door M. Z. Fehér en A. Pokoraczki als gemachtigden,
- de Poolse regering, vertegenwoordigd door B. Majczyna als gemachtigde,
- de Portugese regering, vertegenwoordigd door L. Inez Fernandes, P. Barros da Costa, L. Medeiros en I. Oliveira als gemachtigden,
- de Finse regering, vertegenwoordigd door J. Heliskoski als gemachtigde,
- de regering van het Verenigd Koninkrijk, vertegenwoordigd door S. Brandon en Z. Lavery als gemachtigden, bijgestaan door G. Facenna, QC, en C. Knight, barrister,
- de Europese Commissie, aanvankelijk vertegenwoordigd door H. Kranenborg, M. Wasmeier, P. Costa de Oliveira en K. Toomus, vervolgens door H. Kranenborg, M. Wasmeier en E. Randvere als gemachtigden,

gehoord de conclusie van de advocaat-generaal ter terechtzitting van 21 januari 2020,
het navolgende

Arrest

1 Het verzoek om een prejudiciële beslissing betreft 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, 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 tegen de achtergrond van de artikelen 7, 8 en 11 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 strafrechtelijke procedure tegen H. K. wegens diefstal, gebruik van de bankpas van een ander en geweldpleging tegen betrokkenen bij een gerechtelijke procedure.

Toepasselijke bepalingen

Unierecht

3 De overwegingen 2 en 11 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/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)] 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 een 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."

4 Artikel 2 van richtlijn 2002/58, met als opschrift „Definities", 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:
a) ‚gebruiker': natuurlijke persoon die gebruikmaakt van een openbare elektronische-communicatiedienst 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 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;
[…]"

5 In artikel 5 van richtlijn 2002/58, met als opschrift „Vertrouwelijk karakter van de communicatie", wordt bepaald:
„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. 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 elektronische- 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."

6 Artikel 6 van richtlijn 2002/58, met als opschrift „Verkeersgegevens", bepaalt:
„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.
3. De aanbieder van een openbare elektronische-communicatiedienst mag ten behoeve van de marketing van elektronische-communicatiediensten 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 elektronische-communicatiediensten 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.
[…]"

7 Artikel 9 van richtlijn 2002/58, met als opschrift „Andere locatiegegevens dan verkeersgegevens", bepaalt in lid 1:
„Wanneer andere locatiegegevens dan verkeersgegevens die betrekking hebben op gebruikers of abonnees van elektronische-communicatienetwerken 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. […]"

8 Artikel 15 van richtlijn 2002/58, 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 [Unierecht], met inbegrip van de beginselen als bedoeld in artikel 6, leden 1 en 2, van het Verdrag betreffende de Europese Unie."

Ests recht

Wet inzake elektronische communicatie

9 § 111[1] van de elektroonilise side seadus (wet inzake elektronische communicatie, RT I 2004, 87, 593; RT I, 22.05.2018, 3), in de versie die van toepassing is op de feiten van het hoofdgeding (hierna: „wet inzake elektronische communicatie"), met als opschrift „Verplichting tot gegevensbewaring", bepaalt:
„[…]
(2) Aanbieders van vaste- en mobieletelefoniediensten en van vaste- en mobieletelefonienetwerkdiensten zijn verplicht de volgende gegevens te bewaren:
1) het oproepende nummer alsmede de naam en het adres van de abonnee;
2) het opgeroepen nummer alsmede de naam en het adres van de abonnee;
3) bij het gebruik van aanvullende diensten, zoals het doorsturen of doorschakelen van gesprekken: het gekozen nummer alsmede de naam en het adres van de abonnee;
4) de datum en het tijdstip van het begin en het einde van de telefonische oproep;
5) de gebruikte vaste- of mobieletelefoniedienst;
6) de *International Mobile Subscriber Identity* (IMSI) (internationaal identificatienummer voor mobieletelefoongebruikers) van de oproepende en de opgeroepen persoon;
7) de *International Mobile Equipment Identity* (IMEI) (internationaal identificatienummer voor mobiele apparaten) van de oproepende en de opgeroepen persoon;
8) de locatieaanduiding bij het begin van de oproep;
9) gegevens voor het bepalen van de geografische locatie van cellulaire toegangspunten middels verwijzing naar de locatieaanduidingen ervan gedurende de periode dat communicatiegegevens worden bewaard;
10) in geval van prepaid anonieme diensten, de datum en het tijdstip van de eerste activering van de dienst en aanduiding van de locatie vanwaaruit de dienst is geactiveerd.
[…]
(4) De in de leden 2 en 3 van deze paragraaf genoemde gegevens worden gedurende een periode van een jaar vanaf het tijdstip van de communicatie bewaard, indien deze gegevens zijn gegenereerd of verwerkt in het kader van de levering van een communicatiedienst.
[…]
[…]
(11) De in de leden 2 en 3 van deze paragraaf genoemde gegevens worden doorgegeven
1) volgens het kriminaalmenetluse seadustik [(wetboek van strafvordering)], aan de met het onderzoek belaste instantie, de voor observatiemaatregelen gemachtigde dienst, het openbaar ministerie en de rechter;
[…]"

Wetboek van strafvordering

10 § 17 van het wetboek van strafvordering (RT I 2003, 27, 166; RT I, 31.05.2018, 22) bepaalt:
„(1) Partijen in de procedure zijn het openbaar ministerie, […].
[…]"

11 § 30 van dat wetboek luidt als volgt:
„(1) Het openbaar ministerie leidt de onderzoeksprocedure, waarborgt de rechtmatigheid en geldigheid daarvan en treedt op als openbaar aanklager tijdens het proces.
(2) De bevoegdheden van het openbaar ministerie in de strafprocedure worden in naam van het openbaar ministerie uitgeoefend door een openbaar aanklager, die onafhankelijk handelt en uitsluitend gebonden is aan de wet."

12 § 90[1] van voornoemd wetboek bepaalt:
„[…]
(2) De met het onderzoek belaste instantie kan in de onderzoeksprocedure met toestemming van het openbaar ministerie of in de gerechtelijke procedure met toestemming van de rechter bij een aanbieder van elektronische-communicatiediensten de in § 111[1], leden 2 en 3, van de wet inzake elektronische communicatie bedoelde gegevens opvragen die in lid 1 van de onderhavige paragraaf niet worden genoemd. Die toestemming vermeldt de periode waarvoor de gegevens mogen worden opgevraagd, met opgave van de precieze data.
(3) Overeenkomstig de onderhavige paragraaf mogen gegevens alleen worden opgevraagd indien dit absoluut noodzakelijk is om het met de strafprocedure beoogde doel te bereiken."

13 § 211 van dit wetboek bevat de volgende bepaling:
„(1) Het doel van de onderzoeksprocedure is het verzamelen van bewijzen en het vaststellen van de overige noodzakelijke voorwaarden voor het voeren van een proces.
(2) Tijdens de onderzoeksprocedure worden door de onderzoeksinstantie en het openbaar ministerie de voor de verdachte of vervolgde persoon ontlastende en belastende omstandigheden onderzocht."

Wet inzake het openbaar ministerie

14 § 1 van de prokuratuuriseadus (wet inzake het openbaar ministerie, RT I 1998, 41, 625; RT I, 06.07.2018, 20), in de op de feiten van het hoofdgeding toepasselijke versie, bepaalt:
„(1) Het openbaar ministerie is een overheidsinstantie die valt onder de verantwoordelijkheid van het ministerie van justitie en die betrokken is bij de planning van de voor de bestrijding en opsporing van strafbare feiten noodzakelijke observatiemaatregelen, het strafrechtelijk onderzoek leidt, de rechtmatigheid en doeltreffendheid daarvan waarborgt, als openbaar aanklager in rechte optreedt en de overige bij wet aan het openbaar ministerie toegewezen taken vervult.
(1^1) Het openbaar ministerie is bij het vervullen van zijn wettelijke taken onafhankelijk en handelt in overeenstemming met de onderhavige wet, met overige wetten en met op basis van deze wetten vastgestelde regelingen.
[…]"

15 In § 2, lid 2, van die wet wordt bepaald:
„De openbaar aanklager handelt bij het vervullen van zijn taken onafhankelijk en uitsluitend in overeenstemming met de wet en zijn eigen overtuiging."

Hoofdgeding en prejudiciële vragen

16 Op 6 april 2017 heeft de Viru Maakohus (rechter in eerste aanleg Viru, Estland) H. K. veroordeeld tot een vrijheidsstraf van twee jaar wegens het plegen, tussen 17 januari 2015 en 1 februari 2016, van meerdere diefstallen van goederen (ter waarde van 3 tot 40 EUR) en van contant geld (te weten bedragen tussen 5,20 en 2 100 EUR), wegens het gebruiken van de bankkaart van een ander – die daardoor schade leed ten belope van 3 941,82 EUR – en wegens het plegen van geweld tegen betrokkenen bij de gerechtelijke procedure tegen haar.

17 Om H. K. schuldig te verklaren aan deze feiten, heeft de Viru Maakohus zich onder meer gebaseerd op meerdere processen-verbaal die waren opgesteld op basis van elektronische-communicatiegegevens in de zin van § 111^1, lid 2, van de wet inzake elektronische communicatie. Deze gegevens waren door de met het onderzoek belaste instantie in de loop van de onderzoeksprocedure verzameld bij een aanbieder van elektronische-communicatiediensten. Die opsporingsinstantie had daarvoor telkens op grond van § 90^1 van het wetboek van strafvordering toestemming verkregen van de Viru Ringkonnaprokuratuur (openbaar ministerie van het arrondissement Viru, Estland). Die toestemming, die was verleend op 28 januari, 2 februari en 2 november 2015 en op 25 februari 2016, had betrekking op gegevens betreffende meerdere telefoonnummers en verschillende IMEI-codes van H. K. voor de periode van 1 januari tot en met 2 februari 2015, voor 21 september 2015, en voor de periode van 1 maart 2015 tot en met 19 februari 2016.

18 H. K. heeft tegen het vonnis van de Viru Maakohus hoger beroep ingesteld bij de Tartu Ringkonnakohus (rechter in tweede aanleg Tartu, Estland), die dat hoger beroep bij beslissing van 17 november 2017 heeft verworpen.

19 H. K. heeft tegen deze laatste beslissing cassatieberoep ingesteld bij de Riigikohus (hoogste rechterlijke instantie, Estland), waarbij zij onder meer de toelaatbaarheid betwistte van de processen-verbaal die waren opgesteld op basis van de gegevens die waren verkregen van de aanbieder van de elektronische-communicatiediensten. Volgens haar volgt 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"), dat de regels van § 111^1 van de wet inzake elektronische communicatie die aanbieders van diensten verplichten om communicatiegegevens te bewaren, alsook het gebruik van deze gegevens om haar te veroordelen, in strijd zijn met 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.

20 Volgens de verwijzende rechter rijst de vraag of processen-verbaal die zijn opgesteld op basis van de in § 111^1, lid 2, van de wet inzake elektronische communicatie bedoelde gegevens, kunnen worden aangemerkt als toelaatbaar bewijs. Deze rechter merkt op dat het antwoord op de vraag of de processen-verbaal die in het hoofdgeding aan de orde zijn, kunnen worden toegelaten als bewijsmiddel, afhangt van de vraag in hoeverre de gegevens op basis waarvan die processen-verbaal zijn opgesteld, werden verzameld in overeenstemming met 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.

21 De verwijzende rechter is van oordeel dat er, om antwoord te kunnen geven op deze vraag, moet worden vastgesteld of voornoemd artikel 15, lid 1, gelezen in het licht van het Handvest, aldus moet worden uitgelegd dat de toegang van nationale instanties tot gegevens die het mogelijk maken om de plaats van verzending en ontvangst van een communicatie vanaf een vaste of mobiele telefoon van een verdachte te identificeren, alsmede om de datum, het tijdstip, de duur en de aard van deze communicatie, de gebruikte communicatieapparatuur en de locatie van de gebruikte mobiele-communicatieapparatuur vast te stellen, een dusdanig ernstige inmenging vormt in de betrokken grondrechten, dat deze toegang moet worden beperkt tot gevallen waarin zware criminaliteit wordt bestreden, ongeacht de periode waarvoor die nationale instanties om toegang tot de bewaarde gegevens hebben verzocht.

22 De verwijzende rechter is evenwel van oordeel dat de duur van deze periode van wezenlijk belang is voor de beoordeling van de ernst van de inmenging die bestaat in de toegang tot de verkeers- en locatiegegevens. Wanneer die periode zeer kort, of de hoeveelheid verzamelde gegevens zeer beperkt is, rijst dus de vraag of het doel van bestrijding van de criminaliteit in het algemeen, en niet enkel de bestrijding van zware criminaliteit, een dergelijke inmenging kan rechtvaardigen.

23 Ten slotte betwijfelt de verwijzende rechter of het Estse openbaar ministerie kan worden beschouwd als een onafhankelijke bestuurlijke entiteit in de zin van punt 120 van het arrest Tele2 die de met het onderzoek belaste instantie toegang kan verlenen tot gegevens over elektronische communicatie als bedoeld in § 111^1, lid 2, van de wet inzake elektronische communicatie.

24 Het openbaar ministerie leidt de onderzoeksprocedure en waarborgt de wettigheid en doeltreffendheid daarvan. Het doel van deze procedure is met name het verzamelen van bewijsmateriaal, en de met het onderzoek belaste instantie en het openbaar ministerie onderzoeken de belastende en ontlastende gegevens die over een verdachte of vervolgde persoon zijn verzameld. Indien het openbaar ministerie ervan overtuigd is dat alle noodzakelijke bewijzen zijn verzameld, kan het strafvervolging tegen de verdachte instellen. De bevoegdheden van het openbaar ministerie worden uitgeoefend door een openbaar aanklager, die zijn taken onafhankelijk uitvoert, zoals volgt uit § 30, leden 1 en 2, van het wetboek van strafvordering en de §§ 1 en 2 van de wet inzake het openbaar ministerie.

25 In deze context merkt de verwijzende rechter op dat zijn twijfels over de door het Unierecht vereiste onafhankelijkheid hoofdzakelijk zijn toe te schrijven aan het feit dat het openbaar ministerie niet alleen de onderzoeksprocedure leidt, maar tijdens het proces ook optreedt als openbaar aanklager, aangezien deze instantie volgens het nationale recht partij is in de strafprocedure.

26 In deze omstandigheden heeft de Riigikohus de behandeling van de zaak geschorst en het Hof verzocht om een prejudiciële beslissing over de volgende vragen:
„1) Dient artikel 15, lid 1, van richtlijn [2002/58], in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het [Handvest], aldus te worden uitgelegd dat de toegang van overheidsinstanties, in het kader van een strafprocedure, tot gegevens die het mogelijk maken om de plaats van verzending en ontvangst van een telefonische communicatie vanaf de vaste of mobiele telefoon van een verdachte te traceren en te identificeren, alsmede om de datum, het tijdstip, de duur en de aard van die communicatie, de gebruikte communicatieapparatuur en de locatie van de gebruikte mobiele-communicatieapparatuur vast te stellen, een dusdanig ernstige inmenging vormt in de grondrechten, zoals gewaarborgd door de voornoemde artikelen van het Handvest, dat, bij het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, deze toegang moet worden beperkt tot gevallen waarin zware criminaliteit wordt bestreden, ongeacht de periode waarop de bewaarde gegevens waartoe de nationale instanties toegang hebben betrekking hebben?

2) Dient artikel 15, lid 1, van richtlijn [2002/58], uitgaande van het in het arrest [van 2 oktober 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788)], punten 55 tot en met 57, geformuleerde evenredigheidsbeginsel, aldus te worden uitgelegd dat, als de hoeveelheid van de in de eerste vraag bedoelde gegevens waartoe de overheidsinstanties toegang hebben, (zowel naar de aard van de gegevens als gezien de betrokken periode) niet groot is, de inmenging in de grondrechten die deze toegang met zich brengt in het algemeen gerechtvaardigd kan zijn door de doelstelling van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten en dat, naarmate de hoeveelheid van de gegevens waartoe de overheidsinstanties toegang hebben groter is, de strafbare feiten die met deze inmenging moeten worden bestreden ernstiger moeten zijn?
3) Betekent het in punt 2 van het dictum van [het arrest Tele2] gestelde vereiste dat de toegang van de bevoegde overheidsinstanties tot gegevens wordt onderworpen aan een voorafgaande toetsing door een rechterlijke instantie of een onafhankelijke bestuurlijke autoriteit, dat artikel 15, lid 1, van richtlijn [2002/58] aldus dient te worden uitgelegd dat het openbaar ministerie, dat de onderzoeksprocedure leidt – waarbij het krachtens de wet verplicht is tot onafhankelijk handelen, uitsluitend gebonden is aan de wet en in het kader van die procedure zowel de voor de verdachte belastende als ontlastende omstandigheden onderzoekt – maar dat in de latere gerechtelijke procedure optreedt als openbaar aanklager, kan worden beschouwd als een onafhankelijke bestuurlijke autoriteit?"

Beantwoording van de prejudiciële vragen

Eerste en tweede vraag

27 Met zijn eerste en tweede prejudiciële vraag, die samen moeten worden onderzocht, wenst de verwijzende rechter in wezen te vernemen of 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, aldus moet worden uitgelegd dat het zich verzet tegen een nationale regeling die de mogelijkheid biedt om overheidsinstanties met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten toegang te verlenen tot een reeks verkeers- of locatiegegevens die informatie kunnen verschaffen over de communicaties van een gebruiker van een elektronische-communicatiemiddel of over de locatie van de door hem gebruikte eindapparatuur en waaruit precieze conclusies kunnen worden getrokken over zijn persoonlijke levenssfeer – zonder dat die toegang beperkt is tot procedures ter bestrijding van zware criminaliteit –, en dit ongeacht de duur van de periode waarvoor om toegang tot dergelijke gegevens wordt verzocht en ongeacht de hoeveelheid en de aard van de gegevens die voor die periode beschikbaar zijn.

28 In dit verband blijkt uit het verzoek om een prejudiciële beslissing dat, zoals de Estse regering ter terechtzitting heeft bevestigd, de gegevens waartoe de met het onderzoek belaste nationale instantie in het hoofdgeding toegang heeft gehad, gegevens zijn die waren verzameld krachtens § 111[1], leden 2 en 4, van de wet inzake elektronische communicatie, welke bepaling aanbieders van elektronische-communicatiediensten verplicht om de verkeers- en locatiegegevens met betrekking tot vaste en mobiele telefonie gedurende een jaar algemeen en ongedifferentieerd te bewaren. Deze gegevens maken het met name mogelijk om de plaats van verzending en ontvangst van een communicatie vanaf de vaste of mobiele telefoon van een persoon te traceren en te identificeren, alsmede om de datum, het tijdstip, de duur en de aard van die communicatie, de gebruikte communicatieapparatuur en de locatie van de mobiele telefoon vast te stellen, zonder dat er noodzakelijkwijs een communicatie moet zijn verzonden. Bovendien bieden zij de mogelijkheid om de frequentie van de communicaties van de gebruiker met bepaalde personen gedurende een bepaalde periode vast te stellen. Bovendien kan, zoals de Estse regering ter terechtzitting eveneens heeft bevestigd, op het gebied van de bestrijding van criminaliteit worden verzocht om toegang tot die gegevens voor alle soorten strafbare feiten.

29 Met betrekking tot de voorwaarden waaronder bij een krachtens artikel 15, lid 1, van richtlijn 2002/58 genomen maatregel aan overheidsinstanties met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten toegang kan worden verleend tot verkeers- en locatiegegevens die zijn opgeslagen door aanbieders van elektronische-communicatiediensten, heeft het Hof al geoordeeld dat een dergelijke toegang alleen kan worden verleend voor zover die gegevens door deze aanbieders zijn bewaard op een wijze die in overeenstemming is met voornoemd artikel 15, lid 1 (zie in die zin arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punt 167).

30 In dit verband heeft het Hof tevens geoordeeld dat genoemd artikel 15, lid 1, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, zich verzet tegen wettelijke maatregelen die voor dergelijke doeleinden, als preventieve maatregel, voorzien in de algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens (zie in die zin arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punt 168).

31 Wat de doelstellingen betreft die kunnen rechtvaardigen dat overheidsinstanties toegang krijgen tot de gegevens die door aanbieders van elektronische-communicatiediensten op grond van een maatregel die in overeenstemming is met die bepalingen worden bewaard, volgt uit de rechtspraak van het Hof enerzijds dat een dergelijke toegang enkel kan worden gerechtvaardigd door de doelstelling van algemeen belang met het oog waarop de verplichting tot bewaring van die gegevens aan die aanbieders is opgelegd (zie in die zin arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punt 166).

32 Anderzijds heeft het Hof geoordeeld dat er bij de beoordeling of de lidstaten een beperking van de omvang van de met name in de artikelen 5, 6 en 9 van richtlijn 2002/58 bedoelde rechten en plichten kunnen rechtvaardigen, moet worden bepaald wat de ernst is van de inmenging die een dergelijke beperking met zich brengt, en moet worden nagegaan of het belang van de met die beperking nagestreefde doelstelling van algemeen belang in verhouding staat tot die ernst (arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punt 131 en aldaar aangehaalde rechtspraak).

33 Wat de doelstelling van voorkoming, onderzoek, opsporing en vervolging van strafbare feiten betreft die door de in het hoofdgeding aan de orde zijnde regeling wordt nagestreefd, kunnen overeenkomstig het evenredigheidsbeginsel alleen de bestrijding van zware criminaliteit en het voorkomen van ernstige bedreigingen van de openbare veiligheid een rechtvaardiging vormen voor ernstige inmengingen in de in de artikelen 7 en 8 van het Handvest erkende grondrechten, zoals inmengingen die voortvloeien uit de bewaring van verkeers- en locatiegegevens, ongeacht of deze algemeen en ongedifferentieerd dan wel gericht zijn. Derhalve kunnen met de door de in het hoofdgeding aan de orde zijnde regeling nagestreefde doelstelling om strafbare feiten in het algemeen te voorkomen, te onderzoeken, op te sporen en te vervolgen, enkel niet-ernstige inmengingen in die grondrechten worden gerechtvaardigd (zie in die zin arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punten 140 en 146).

34 In dit verband is met name geoordeeld dat wettelijke maatregelen met betrekking tot de verwerking van gegevens inzake de burgerlijke identiteit van gebruikers van elektronische-communicatiemiddelen als zodanig, met name de bewaring ervan en de toegang daartoe, uitsluitend met het oog op de identificatie van de betrokken gebruiker en zonder dat deze gegevens verband kunnen houden met informatie over de verrichte communicaties, kunnen worden gerechtvaardigd door de in artikel 15, lid 1, eerste volzin, van richtlijn 2002/58 genoemde doelstelling om strafbare feiten in het algemeen te voorkomen, te onderzoeken, op te sporen en te vervolgen. Met die gegevens alleen is het immers niet mogelijk om de datum, het tijdstip, de duur en de ontvangers van de communicaties, de plaats waar die communicaties hebben plaatsgevonden of het aantal malen dat in een specifieke periode met bepaalde personen is gecommuniceerd te achterhalen. Zij verschaffen dus, afgezien van de contactgegevens van de gebruikers van elektronische-communicatiemiddelen, zoals hun adressen, geen enkele informatie over bepaalde communicaties en, bijgevolg, ook niet over hun persoonlijke levenssfeer. De inmenging die een maatregel strekkende tot bewaring van die gegevens met zich brengt, kan derhalve niet als „ernstig" worden aangemerkt (zie in die zin arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punten 157 en 158 en aldaar aangehaalde rechtspraak).

35 In die omstandigheden kunnen alleen de doelstellingen van bestrijding van zware criminaliteit en van voorkoming van ernstige bedreigingen van de openbare veiligheid rechtvaardigen dat overheidsinstanties toegang hebben tot een reeks verkeers- of locatiegegevens die informatie kunnen verschaffen over de communicaties van een gebruiker van een elektronische-communicatiemiddel of

over de locatie van de door die gebruiker gehanteerde eindapparatuur en op grond waarvan precieze conclusies kunnen worden getrokken over de persoonlijke levenssfeer van de betrokkenen (zie in die zin arrest van 2 oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punt 54), zonder dat andere factoren die de evenredigheid van een verzoek om toegang bepalen, zoals de duur van de periode waarvoor om toegang tot dergelijke gegevens wordt verzocht, tot gevolg kunnen hebben dat de doelstelling van voorkoming, onderzoek, opsporing en vervolging van strafbare feiten in het algemeen een dergelijke toegang rechtvaardigt.

36 Opgemerkt zij dat de toegang tot een reeks verkeers- of locatiegegevens zoals die welke krachtens § 111[1] van de wet inzake elektronische communicatie worden bewaard, het inderdaad mogelijk maakt precieze, ja zelfs zeer nauwkeurige conclusies te trekken over de persoonlijke levenssfeer van de personen van wie de gegevens zijn bewaard, bijvoorbeeld met betrekking tot hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren (zie in die zin arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punt 117).

37 Het is juist dat, zoals de verwijzende rechter suggereert, hoe langer de bovengenoemde periode waarvoor om toegang wordt gevraagd is, des te groter in beginsel de hoeveelheid gegevens over de elektronische communicaties, verblijfplaatsen en verplaatsingen van de gebruiker van een elektronisch-communicatiemiddel zal zijn die door de aanbieders van elektronische-communicatiediensten kan worden bewaard, zodat uit de geraadpleegde gegevens over de persoonlijke levenssfeer van die gebruiker meer conclusies kunnen worden getrokken. Een soortgelijke vaststelling kan ook worden getrokken voor wat betreft de categorieën van de gevraagde gegevens.

38 Om te voldoen aan het evenredigheidsvereiste, dat inhoudt dat afwijkingen van en beperkingen op de bescherming van persoonsgegevens binnen de grenzen van het strikt noodzakelijke moeten worden gehandhaafd (arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punt 130 en aldaar aangehaalde rechtspraak), is het derhalve aan de bevoegde nationale instanties om er in elk afzonderlijk geval voor te zorgen dat zowel de categorie of categorieën gegevens waarnaar wordt verwezen als de duur waarvoor om toegang tot die gegevens is verzocht, afhankelijk van de omstandigheden van het geval, beperkt blijven tot hetgeen strikt noodzakelijk is voor het betrokken onderzoek.

39 De inmenging in de grondrechten die zijn verankerd in de artikelen 7 en 8 van het Handvest, welke inmenging voortvloeit uit de toegang van een overheidsinstantie tot een reeks verkeers- of locatiegegevens die informatie kunnen verschaffen over de communicaties van een gebruiker van een elektronische-communicatiemiddel of over de locatie van de door hem gebruikte eindapparatuur, is echter hoe dan ook ernstig van aard, ongeacht de duur van de periode waarvoor toegang wordt gevraagd tot die gegevens en ongeacht de hoeveelheid of de aard van de gegevens die voor een dergelijke periode beschikbaar zijn, wanneer, zoals in het hoofdgeding, uit deze gegevens nauwkeurige conclusies kunnen worden getrokken met betrekking tot de persoonlijke levenssfeer van de betrokkene(n).

40 In dit verband kan zelfs de toegang tot een beperkte hoeveelheid verkeers- of locatiegegevens of de toegang tot gegevens voor een korte periode nauwkeurige informatie over de persoonlijke levenssfeer van een gebruiker van een elektronische-communicatiemiddel verschaffen. Bovendien zijn de hoeveelheid beschikbare gegevens en de daaruit voortvloeiende concrete informatie over de persoonlijke levenssfeer van de betrokkene omstandigheden die pas na inzage van die gegevens kunnen worden beoordeeld. De door de rechterlijke instantie of de bevoegde onafhankelijke instantie verleende toestemming vindt echter noodzakelijkerwijs plaats voordat de daaruit voortvloeiende gegevens en informatie kunnen worden geraadpleegd. De beoordeling van de ernst van de inmenging die de toegang voor de persoonlijke levenssfeer van de betrokken personen met zich brengt, gebeurt dus noodzakelijkerwijs aan de hand van het algemene risico dat verband houdt met de categorie van de gevraagde gegevens, waarbij het overigens niet van belang is of de daaruit voortvloeiende informatie betreffende de persoonlijke levenssfeer al dan niet concreet gevoelig is.

41 Ten slotte moet – gelet op het feit dat de verwijzende rechter is verzocht de op basis van verkeers- en locatiegegevens opgestelde processen-verbaal niet toelaatbaar te verklaren omdat de bepalingen van § 111[1] van de wet inzake elektronische communicatie, wat zowel de bewaring van als de toegang tot gegevens betreft, in strijd zijn met artikel 15, lid 1, van richtlijn 2002/58 – in aanmerking worden genomen dat het bij de huidige stand van het Unierecht in beginsel uitsluitend aan het nationale recht staat om de regels vast te stellen betreffende de toelaatbaarheid en de beoordeling, in het kader van strafprocedures tegen personen die van strafbare feiten worden verdacht, van informatie en bewijsmateriaal die zijn verkregen door de algemene en ongedifferentieerde bewaring van dergelijke gegevens, in strijd met het recht van de Unie (arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punt 222), of door een met dat recht strijdige toegang van de nationale instanties tot die gegevens.

42 Volgens vaste rechtspraak is het, bij gebreke van regels van de Unie ter zake, aan de nationale rechtsorde van elke lidstaat om, overeenkomstig het beginsel van procedurele autonomie, de procedurele regelingen voor gerechtelijke procedures vast te stellen ter vrijwaring van de rechten die de justitiabelen aan het recht van de Unie ontlenen, op voorwaarde evenwel dat zij niet minder gunstig zijn dan die welke gelden voor soortgelijke situaties die onder het nationale recht vallen (gelijkwaardigheidsbeginsel) en dat zij de uitoefening van de door het recht van de Unie verleende rechten in de praktijk niet onmogelijk of uiterst moeilijk maken (doeltreffendheidsbeginsel) (arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punt 223 en aldaar aangehaalde rechtspraak).

43 Wat meer in het bijzonder het doeltreffendheidsbeginsel betreft, zij eraan herinnerd dat de nationale regels inzake aanvaarding en gebruik van informatie en bewijzen tot doel hebben om in overeenstemming met de in het nationale recht gemaakte keuzen te voorkomen dat onrechtmatig verkregen informatie en bewijzen ongerechtvaardigd nadeel toebrengen aan een persoon die ervan wordt verdacht strafbare feiten te hebben gepleegd. Dit doel kan volgens het nationale recht niet alleen worden bereikt door een verbod op het gebruik van dergelijke informatie en bewijselementen, maar ook door nationale regels en praktijken met betrekking tot de beoordeling en de weging van de informatie en de bewijzen, of door de inaanmerkingneming van het onrechtmatige karakter ervan bij de straftoemeting (arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punt 225).

44 Bij de beoordeling of informatie en bewijzen die in strijd met de voorschriften van het Unierecht zijn verkregen, moeten worden uitgesloten, moet met name worden nagegaan of de aanvaarding van dergelijke informatie en bewijzen schending van het beginsel van hoor en wederhoor en dus ook van het recht op een eerlijk proces tot gevolg kan hebben. Een rechterlijke instantie die van oordeel is dat een partij niet in de gelegenheid is om doeltreffend commentaar te leveren op een bewijsmiddel dat betrekking heeft op een gebied waarvan de rechters geen kennis hebben en dat een doorslaggevende invloed kan hebben op de beoordeling van de feiten, moet vaststellen dat het recht op een eerlijk proces hierdoor wordt geschonden, en moet dat bewijsmiddel uitsluiten om die schending te voorkomen. Bijgevolg brengt het doeltreffendheidsbeginsel voor de nationale strafrechter de verplichting mee om informatie en bewijzen die door middel van een met het Unierecht onverenigbare algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens dan wel via toegang daartoe door de bevoegde instantie in strijd met dit recht zijn verkregen, in het kader van een strafrechtelijke procedure tegen personen die worden verdacht van strafbare handelingen buiten beschouwing te laten indien die personen niet in de gelegenheid zijn om doeltreffend commentaar te leveren op die informatie en die bewijzen, die betrekking hebben op een gebied waarvan de rechter geen kennis heeft en een doorslaggevende invloed kunnen hebben op de beoordeling van de feiten (zie in die zin arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punten 226 en 227).

45 Gelet op het voorgaande moet op de eerste en de tweede vraag worden geantwoord dat 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, aldus moet worden uitgelegd dat het zich verzet tegen een nationale regeling die de mogelijkheid biedt om overheidsinstanties met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten toegang te verlenen tot een reeks verkeers- of locatiegegevens die informatie kunnen verschaffen over de communicaties van een gebruiker van een elektronische-communicatiemiddel of over de locatie van de door hem gebruikte eindapparatuur en waaruit precieze conclusies kunnen worden getrokken over zijn persoonlijke levenssfeer – welke toegang niet beperkt is tot procedu-

res ter bestrijding van zware criminaliteit en ter voorkoming van ernstige bedreigingen van de openbare veiligheid –, en dit ongeacht de duur van de periode waarvoor om toegang tot dergelijke gegevens wordt verzocht en ongeacht de hoeveelheid en de aard van de gegevens die voor die periode beschikbaar zijn.

Derde vraag

46 Met zijn derde prejudiciële vraag wenst de verwijzende rechter in wezen te vernemen of 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, aldus moet worden uitgelegd dat het zich verzet tegen een nationale regeling die het openbaar ministerie, dat tot taak heeft de strafprocedure in te leiden en, in voorkomend geval, in een latere procedure op te treden als openbaar aanklager, de bevoegdheid toekent om een overheidsinstantie ten behoeve van een strafrechtelijk onderzoek toegang te verlenen tot verkeers- en locatiegegevens.

47 De verwijzende rechter preciseert in dit verband dat het Estse openbaar ministerie overeenkomstig het nationale recht weliswaar onafhankelijk moet handelen, uitsluitend onderworpen is aan de wet en tijdens de onderzoeksprocedure de belastende en ontlastende gegevens moet onderzoeken, maar dat het doel van deze procedure gelegen blijft in het verzamelen van bewijs en het vaststellen van de overige noodzakelijke voorwaarden voor het voeren van een proces. Het is diezelfde instantie die tijdens het proces optreedt als openbaar aanklager en dus ook partij is in de procedure. Bovendien blijkt uit het dossier waarover het Hof beschikt dat het Estse openbaar ministerie hiërarchisch is georganiseerd, dat verzoeken om toegang tot verkeers- en locatiegegevens niet aan een bijzonder vormvereiste zijn onderworpen en door de openbare aanklager zelf kunnen worden ingediend, en dat de personen tot wier gegevens toegang kan worden verleend niet enkel personen zijn die ervan worden verdacht betrokken te zijn bij een strafbaar feit, zoals ook de Estse regering en de Prokuratuur ter terechtzitting hebben bevestigd.

48 Het is juist dat het, zoals het Hof reeds heeft geoordeeld, aan het nationale recht staat om de voorwaarden vast te stellen waaronder de aanbieders van elektronische-communicatiediensten de bevoegde nationale instanties toegang moeten verlenen tot de gegevens waarover zij beschikken. Om aan het evenredigheidsvereiste te voldoen, dient een regeling evenwel duidelijke en nauwkeurige regels te bevatten die de reikwijdte en de toepassing van de betrokken maatregel vastleggen en minimumvereisten opleggen, 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 nationaal 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 (zie in die zin arrest Tele2, punten 117 en 118, alsmede arresten van 6 oktober 2020, Privacy International, C-623/17, EU:C:2020:790, punt 68, en 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punt 132 en aldaar aangehaalde rechtspraak).

49 Met name mag een nationale regeling die de toegang van de bevoegde instanties tot bewaarde verkeers- en locatiegegevens regelt, en die is vastgesteld op grond van artikel 15, lid 1, van richtlijn 2002/58, zich er niet toe beperken te eisen dat de instanties toegang tot de gegevens wordt verleend voor het doel dat met die regeling wordt nagestreefd, maar moet zij ook de materiële en procedurele voorwaarden voor dit gebruik bepalen (arresten van 6 oktober 2020, Privacy International, C-623/17, EU:C:2020:790, punt 77, en 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punt 176 en aldaar aangehaalde rechtspraak).

50 Aangezien een algemene toegang tot alle bewaarde gegevens los van enig – zelfs ook maar indirect – verband met het nagestreefde doel niet kan worden geacht tot het strikt noodzakelijke te zijn beperkt, moet de betrokken nationale regeling dus aan de hand van objectieve criteria bepalen in welke omstandigheden en onder welke voorwaarden aan de bevoegde nationale instanties toegang tot de gegevens van de abonnees of de geregistreerde gebruikers moet worden verleend. In dit verband kan in beginsel voor het doel van bestrijding van de criminaliteit slechts toegang worden verleend tot de gegevens van personen die ervan worden verdacht een ernstig misdrijf te plannen, te plegen of te hebben gepleegd of op de een of andere wijze betrokken te zijn bij een dergelijk misdrijf. In bijzondere situaties, zoals die waarin vitale belangen van nationale veiligheid, landsverdediging of openbare veiligheid door terroristische activiteiten worden bedreigd, zou echter ook toegang tot de gegevens van andere personen kunnen worden verleend, wanneer op grond van objectieve elementen kan worden geoordeeld dat deze gegevens in het concrete geval een daadwerkelijke bijdrage tot de bestrijding van dergelijke activiteiten zouden kunnen leveren (zie in die zin arrest Tele2, punt 119, en arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punt 188).

51 Om te waarborgen dat deze voorwaarden in de praktijk ten volle in acht worden genomen, is het van wezenlijk belang dat de toegang van de bevoegde nationale instanties tot de bewaarde gegevens wordt onderworpen aan voorafgaande toetsing door een rechterlijke instantie of door een onafhankelijke bestuurlijke entiteit, en dat deze rechterlijke instantie of deze entiteit haar beslissing geeft op een met redenen omkleed verzoek van deze instanties dat met name wordt ingediend in het kader van procedures ter voorkoming, opsporing of vervolging van strafbare feiten. In naar behoren gemotiveerde urgente gevallen dient die toetsing op korte termijn plaats te vinden (zie in die zin arrest van 6 oktober 2020, La Quadrature du Net e.a., C-511/18, C-512/18 en C-520/18, EU:C:2020:791, punt 189 en aldaar aangehaalde rechtspraak).

52 Die voorafgaande toetsing vereist onder meer, zoals de advocaat-generaal in wezen heeft opgemerkt in punt 105 van zijn conclusie, dat de rechterlijke instantie of de entiteit die belast is met die toetsing, over alle bevoegdheden beschikt en alle noodzakelijke waarborgen biedt om ervoor te zorgen dat de verschillende betrokken belangen en rechten met elkaar in overeenstemming worden gebracht. In het specifieke geval van een strafrechtelijk onderzoek vereist een dergelijke toetsing dat die rechterlijke instantie of entiteit in staat is een juist evenwicht te verzekeren tussen, enerzijds, de belangen die verband houden met de behoeften van het onderzoek in het kader van de bestrijding van criminaliteit, en, anderzijds, de fundamentele rechten op eerbiediging van de persoonlijke levenssfeer en op bescherming van de persoonsgegevens van de personen op wier gegevens de toegang betrekking heeft.

53 Wanneer een dergelijke toetsing niet door een rechterlijke instantie maar door een onafhankelijke bestuurlijke entiteit wordt uitgeoefend, moet deze laatste een zodanige status hebben dat zij bij de uitoefening van haar taken objectief en onpartijdig kan handelen, en moet zij daartoe vrij zijn van elke invloed van buitenaf [zie in die zin arrest van 9 maart 2010, Commissie/Duitsland, C-518/07, EU:C:2010:125, punt 25, en advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punten 229 en 230].

54 Uit de voorgaande overwegingen volgt dat het vereiste van onafhankelijkheid waaraan moet worden voldaan door de instantie die de in punt 51 van het onderhavige arrest in herinnering gebrachte voorafgaande toetsing moet verrichten, impliceert dat deze instantie de hoedanigheid van derde moet hebben ten opzichte van degene die om toegang tot de gegevens verzoekt, zodat eerstgenoemde de toetsing objectief en onpartijdig en zonder beïnvloeding van buitenaf kan verrichten. In het bijzonder impliceert het vereiste van onafhankelijkheid op strafrechtelijk gebied, zoals de advocaat-generaal in wezen in punt 126 van zijn conclusie heeft opgemerkt, dat de instantie die belast is met die voorafgaande toetsing enerzijds niet betrokken mag zijn bij de uitvoering van het betrokken strafrechtelijk onderzoek en anderzijds neutraal moet zijn ten opzichte van de partijen in de strafprocedure.

55 Dat is niet het geval bij een openbaar ministerie dat de onderzoeksprocedure leidt en, in voorkomend geval, optreedt als openbaar aanklager. Het openbaar ministerie heeft immers niet tot taak om een geschil in volledige onafhankelijkheid te beslechten, maar om het, in voorkomend geval, als procespartij die de strafvordering instelt, voor te leggen aan de bevoegde rechter.

56 De omstandigheid dat het openbaar ministerie overeenkomstig de regels inzake zijn bevoegdheden en zijn statuut gehouden is om de belastende en ontlastende elementen te onderzoeken, de rechtmatigheid van de onderzoeksprocedure te waarborgen en uitsluitend op te treden in overeenstemming met de wet en zijn eigen overtuiging, kan niet volstaan om het ten aanzien van de betrokken belangen de hoedanigheid van derde in de zin van punt 52 van het onderhavige arrest te verlenen.

57 Hieruit volgt dat het openbaar ministerie niet in staat is om de in punt 51 van het onderhavige arrest bedoelde voorafgaande toetsing te verrichten.

58 Aangezien de verwijzende rechter bovendien de vraag heeft opgeworpen of het ontbreken van controle door een onafhankelijke instantie kan worden verholpen aan de hand van een latere, door een rechterlijke instantie verrichte toetsing van de rechtmatigheid van de toegang van een nationale instantie tot verkeers- en locatiegegevens, moet worden opgemerkt dat de onafhankelijke toetsing, zoals de in punt 51 van het onderhavige arrest in herinnering gebrachte rechtspraak vereist, voorafgaand aan elke toegang moet plaatsvinden, behalve in naar behoren gemotiveerde urgente gevallen. In laatstgenoemde gevallen dient de toetsing op korte termijn plaats te vinden. Zoals de advocaat-generaal in punt 128 van zijn conclusie heeft vastgesteld, kan met een dergelijke latere toetsing niet worden tegemoetgekomen aan het doel van een voorafgaande toetsing, dat erin bestaat te verhinderen dat tot de betrokken gegevens een toegang wordt verleend die verder gaat dan strikt noodzakelijk is.

59 In die omstandigheden moet op de derde prejudiciële vraag worden geantwoord dat 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, aldus moet worden uitgelegd dat het zich verzet tegen een nationale regeling die het openbaar ministerie, dat tot taak heeft de strafprocedure in te leiden en, in voorkomend geval, in een latere procedure op te treden als openbaar aanklager, de bevoegdheid toekent om een overheidsinstantie ten behoeve van een strafrechtelijk onderzoek toegang te verlenen tot verkeers- en locatiegegevens.

Kosten

60 Ten aanzien van de partijen in het hoofdgeding is de procedure als een aldaar gerezen incident te beschouwen, zodat de verwijzende rechterlijke instantie 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 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 het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, moet aldus worden uitgelegd dat het zich verzet tegen een nationale regeling die de mogelijkheid biedt om overheidsinstanties met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten toegang te verlenen tot een reeks verkeers- of locatiegegevens die informatie kunnen verschaffen over de communicaties van een gebruiker van een elektronische-communicatiemiddel of over de locatie van de door hem gebruikte eindapparatuur en waaruit precieze conclusies kunnen worden getrokken over zijn persoonlijke levenssfeer – welke toegang niet beperkt is tot procedures ter bestrijding van zware criminaliteit en ter voorkoming van ernstige bedreigingen van de openbare veiligheid –, en dit ongeacht de duur van de periode waarvoor om toegang tot dergelijke gegevens wordt verzocht en ongeacht de hoeveelheid en de aard van de gegevens die voor die periode beschikbaar zijn.

2) Artikel 15, lid 1, van richtlijn 2002/58, zoals gewijzigd bij richtlijn 2009/136, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten, moet aldus worden uitgelegd dat het zich verzet tegen een nationale regeling die het openbaar ministerie, dat tot taak heeft de strafprocedure in te leiden en, in voorkomend geval, in een latere procedure op te treden als openbaar aanklager, de bevoegdheid toekent om een overheidsinstantie ten behoeve van een strafrechtelijk onderzoek toegang te verlenen tot verkeers- en locatiegegevens.

* Procestaal: Ests.

Noot

Quinten Kroes
Mr. Q.R. Kroes ia advocaat te Amsterdam (Brinkhof) en redacteur van dit blad.

Met dit arrest van de Grote Kamer zet het Hof van Justitie zijn kritische koers voort waar het aankomt op de toetsing van de voorwaarden waaronder opsporingsautoriteiten in lidstaten gebruik mogen maken van telecomgegevens. Veel hierover was al bekend zoals blijkt uit de veelvuldige verwijzing naar eerdere jurisprudentie; het meest recente arrest van 6 oktober 2020, *La Quadrature du Net e.a.*[1] wordt zo vaak genoemd (16 keer!) dat de vraag gerechtvaardigd is of dit arrest nog wel iets toevoegt. Die vraag kan met een volmondig ja beantwoord worden; deze nieuwe uitspraak biedt wel enkele nieuwe inzichten die ook voor de Nederlandse strafrechtsorde nog wel eens gevolgen zouden kunnen hebben.

De zaak betreft prejudiciële vragen van de Estse rechter in een strafzaak. Het ging om de strafrechtelijke veroordeling van ene mevrouw H.K. tot twee jaar gevangenisstraf vanwege herhaalde diefstal van voedingsmiddelen en andere materiële goederen ter waarde van € 3 tot € 40 en geldsommen tot € 2.100, misbruik van de bankpas van een ander waarmee bijna € 4.000 illegaal werd gepind, en geweldpleging tegen een betrokkene bij een gerechtelijke procedure. Het bewijs voor deze misdrijven was mede gebaseerd op verkeersgegevens (met welke andere nummers was gebeld en wanneer) en locatiegegevens (via welke zendmast maakte het mobiele toestel contact met het netwerk), die de opsporingsinstantie had gevorderd bij de mobiele operator. Daarmee kon belastend regelmatig contact met bepaalde personen worden bewezen, alsmede de fysieke aanwezigheid van de veroordeelde op verschillende plaatsen delict (o.a. bij de pinautomaat). Nadat haar beroep was afgewezen, voerde H.K. in cassatie aan dat de processen-verbaal waarin de door het telecommunicatiebedrijf ter beschikking gestelde gegevens waren vermeld, niet hadden mogen worden toegelaten als bewijs en dat haar veroordeling op grond van die processen-verbaal onrechtmatig was. Daarbij verwees zij naar het arrest *Tele2 Sverige en Watson e.a.*,[2] waarin het Hof zich kritisch heeft uitgelaten over de wettelijke bewaarplicht die toen in de Zweedse wet was neergelegd.

Hoewel de vragen van de verwijzende rechter dus lijken te zien op de wettelijke bewaarplicht voor telecomoperators (waarvan in Estland kennelijk ook sprake was), behandelt het Hof die – in navolging van A-G Pitruzzella in deze zaak[3] – over de boeg van de nationaalrechtelijke voorwaarden waaronder opsporingsautoriteiten toegang kunnen vorderen tot die bewaarde gegevens. Al eerder had het Hof uitgemaakt dat de e-Privacyrichtlijn hem die bevoegdheid geeft, ook al raakt dit natuurlijk aan de activiteiten van lidstaten op strafrechtelijk gebied die buiten de reikwijdte van die richtlijn vallen. De redenering van het Hof is daarbij simpel gezegd dat de vorderingen van de autoriteiten weliswaar niet door die richtlijn geharmoniseerd zijn, maar de daarvoor vereiste gegevensverwerkingen (bestaande uit opslag en verstrekking) door telecomaanbieders wel.[4] De e-Privacyrichtlijn legt daarbij aan telecomaanbieders de verplichting op om de vertrouwelijkheid te waarborgen van niet alleen de inhoud van communicatie, maar ook van verkeers- en locatiegegevens, maar staat lidstaten wel toe om die in te perken indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is voor, onder meer, het onderzoeken, opsporen en vervolgen van strafbare feiten. Deze door nationale wetgevers te maken afweging resulteert in regels die zich richten tot telecomaanbieders, en die vallen – anders dan de regels rond opsporing en strafvordering – binnen het mandaat van het Hof (aldus het Hof zelf).

De eerste twee vragen van de nationale rechter zien op de evenredigheid van de inmenging door de Estse autoriteiten in de persoonlijke levenssfeer van verdachte: waren haar misdrijven ernstig genoeg om toegang te mogen vorderen tot deze verkeers- en locatiegegevens, en maakt het in dat verband nog uit hoeveel gegevens zijn gebruikt (bijvoorbeeld hoe lang de periode was waarop deze gegevens betrekking hadden)? Hier herhaalt het Hof wat het inmiddels in verschillende arresten heeft geoordeeld, namelijk dat naarmate de inmenging in de persoonlijke levenssfeer groter is, het onderzochte strafbare feit ook ernstiger moet zijn. Een ernstige inmenging kan dus alleen

1 C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791.
2 C-203/15 en C-698/15, ECLI:EU:C:2016:970.
3 ECLI:EU:C:2020:18.
4 HvJ EU 2 oktober 2018, C-207/16, ECLI:EU:C:2018:788 (*Ministerio Fiscal*), r.o. 37.

gerechtvaardigd worden door het belang bij de bestrijding van zware criminaliteit en het voorkomen van ernstige bedreigingen van de openbare veiligheid. Daarvan was in dit geval geen sprake; de Estse regeling was gericht op de bestrijding van criminaliteit in algemene zin. Dat belang rechtvaardigt volgens het Hof hooguit een niet-ernstige inmenging in de fundamentele rechten van bescherming van de persoonlijke levenssfeer en gegevensbescherming. Dat brengt het Hof dan vanzelf bij de vervolgvraag: Wanneer is sprake van niet-ernstige inmenging? Is daar bijvoorbeeld sprake van als slechts voor één dag de telecomgegevens worden opgevraagd, zodat geen gebruikspatronen over langere tijd kunnen worden vastgesteld?

Het Hof is hier streng en duidelijk, en maakt een absoluut onderscheid naar gelang de aard van de gegevens. Zoals het al eerder had geoordeeld,[5] wordt de enkele vordering van NAW-gegevens van een gebruiker bij een telecomaanbieder beschouwd als een niet-ernstige inmenging, die dus ook voor niet ernstige misdrijven mogen worden gevorderd. Voor verkeers- en locatiegegevens geldt echter dat de opvordering daarvan categoraal als ernstige inmenging wordt aangemerkt, ongeacht de periode waarop die zien en de hoeveelheid gegevens die wordt opgevraagd. Het Hof kwalificeert dat nog wel met de toevoeging "wanneer, zoals in het hoofdgeding, uit deze gegevens nauwkeurige conclusies kunnen worden getrokken met betrekking tot de persoonlijke levenssfeer van de betrokkene(n)" (r.o. 39), maar de overige overwegingen maken wel duidelijk dat hiervan volgens het Hof in de regel sprake zal zijn.

De derde en laatste vraag ziet op de procedure voor toegang. Uit eerdere jurisprudentie (o.a. het eerdergenoemde arrest *La Quadrature du Net e.a.*) volgt dat de toegang van de bevoegde nationale instanties tot de bewaarde gegevens moet worden onderworpen aan voorafgaande toetsing door een rechterlijke instantie of door een onafhankelijke bestuurlijke entiteit. Volgens het Estse wetboek van strafvordering diende in de fase van het voorafgaand onderzoek de openbare aanklager toestemming te geven voor de vordering van gegevens van een telecomaanbieder. De nationale rechter wenst dan ook te vernemen of de openbare aanklager (die onderdeel uitmaakt van het OM) kan kwalificeren als een onafhankelijke bestuurlijke entiteit. Het Hof oordeelt van niet: de instantie die belast is met de voorafgaande toetsing mag niet betrokken zijn bij de uitvoering van het betrokken strafrechtelijk onderzoek en moet neutraal zijn ten opzichte van de partijen in de strafprocedure. Dat is niet het geval bij een openbaar ministerie dat immers tot taak heeft de zaak, als het onderzoek daartoe aanleiding geeft, als procespartij die de strafvordering instelt, aan de bevoegde rechter voor te leggen.

De beantwoording van de derde vraag lijkt een open deur, maar dan wel een die ook in Nederland (nog) wagenwijd openstaat. Artikel 126n Sv maakt namelijk bij een verdenking van een misdrijf waarvoor voorlopige hechtenis kan worden bevolen, de officier van justitie bevoegd om in het belang van het onderzoek een vordering te doen gegevens te verstrekken niet alleen over een gebruiker van een communicatiedienst, maar ook over zijn of haar communicatieverkeer. Dat laatste omvat verkeers- en locatiegegevens.[6] Het lijkt daarbij onwaarschijnlijk dat de Nederlandse officier van justitie wel over de vereiste mate van onafhankelijkheid beschikt waaraan het de Estse aanklager ontbrak. In dat verband heeft het Hof recent in een andere zaak al geoordeeld dat onze officieren van justitie in elk geval niet als rechterlijke autoriteit kunnen worden aangemerkt, nu zij individuele instructies kunnen ontvangen van de Nederlandse minister van Justitie.[7] Diezelfde omstandigheid lijkt in de weg te staan aan een status als onafhankelijke bestuurlijke entiteit. Het EHRM heeft al eerder geoordeeld dat een officier van justitie weliswaar gebonden is aan integriteitseisen, maar niet kan gelden als objectief of onpartijdig.[8]

Over de vraag wat de gevolgen zijn voor bewijs dat is verkregen in weerwil van de door het Hof voorgeschreven waarborgen, laat het Hof zich in dit arrest ook duidelijk uit. Het ontbreken van voorafgaande toetsing door een rechterlijke instantie of onafhankelijke bestuurlijke entiteit kan niet met een toetsing achteraf worden gezuiverd. Ook laat het Hof – ondanks plichtmatige verwijzingen naar de nationale rechtsorde van lidstaten en hun procedurele autonomie – weinig twijfel bestaan over de ontoelaatbaarheid van het bewijs, waarbij het nog wel aan de lidstaten is om zelf te bepalen of dat gebeurt door een verbod op het gebruik van het bewijs, regels over de beoordeling of weging ervan, of door het mee te nemen bij de bepaling van de strafmaat.
Het gaat dus om een arrest met vergaande gevolgen voor de Nederlandse praktijk, die zich wellicht ook niet beperken tot alleen het gebruik van verkeers- en locatiegegevens in de opsporingsfase. De Vereniging voor Cassatieadvocaten in Strafzaken[9] wees al op de mogelijke implicaties van het arrest voor het onderzoek van gegevens op smartphones zelf, waarvan de Hoge Raad onlangs vrij gemakkelijk oordeelde dat de gedwongen ontgrendeling van een telefoon met een vingerafdruk slechts een 'zeer geringe mate van fysieke dwang' meebracht.[10] Dat is wellicht juist uit oogpunt van het fundamentele recht op lichamelijke integriteit en het verbod op foltering, maar vanuit het perspectief van de bescherming van de persoonsgegevens op die telefoon dienen dergelijke praktijken wellicht heroverwogen te worden.

Met dit arrest zet het Hof over de boeg van de uitleg van de e-Privacyrichtlijn, en de daaruit voortvloeiende verplichtingen voor telecomaanbieders, weer een nieuwe stap in de regulering van het gebruik van telecomgegevens door opsporingsautoriteiten, terwijl het onderwerp van nationale strafvordering formeel buiten de bevoegdheid van het Hof valt. Een ontwikkeling die niet in alle lidstaten op bijval kan rekenen, en waar ook lang niet alle lidstaten zich al bij hebben neergelegd.[11] In het arrest *La Quadrature du Net*, dat zag op Franse wetgeving (onder andere over het gebruik van verkeers- en locatiegegevens in 'real time', mede ter bescherming van de nationale veiligheid en de bestrijding van terrorisme), heeft het Hof opnieuw duidelijke grenzen gesteld en verhelderd dat nationale rechters niet vanwege de rechtszekerheid tijdelijk de rechtsgevolgen in stand mogen laten van uitspraken die gebaseerd zijn op – in strijd met de e-Privacyrichtlijn – verkregen bewijs.[12] Dat heeft in Frankrijk een zeer gevoelige snaar geraakt: de Franse overheid is inmiddels een nationale procedure begonnen om te betogen dat het Hof van Justitie met deze bemoeienis met de nationale veiligheid zijn mandaat te buiten is gegaan. Een uitspraak van de Conseil d'Etat wordt in nog in het tweede kwartaal verwacht. De grote vraag is of ook die zaak weer naar het Hof van Justitie zal worden verwezen of dat het Conseil d'Etat zal kiezen voor een confrontatie zoals het Duitse Bundesverfassungsgericht dat vorig jaar deed in de beoordeling van het noodsteunprogramma van de ECB.[13] Naar aanleiding daarvan maakte het Hof in een uitzonderlijk persbericht duidelijk dat het alleen zelf over de eigen bevoegdheid gaat.[14] Een onderwerp dus waarover het laatste woord zeker nog niet gezegd is, maar waarvan wel duidelijk is dat het niet alleen belangrijke vragen oproept voor de Estse en Nederlandse strafrechtpraktijk, maar ook over de Europese rechtsorde.

5 C-207/16, ECLI:EU:C:2018:788 (*Ministerio Fiscal*), r.o. 54.
6 Art. 2 Besluit vorderen gegevens telecommunicatie.
7 HvJ EU 24 november 2020, C-510/19, ECLI:EU:C:2020:953 (*Openbaar Ministerie en YU en ZV/AZ*).
8 EHRM 14 september 2010, nr. 38224/03, ECLI:NL:XX:2010:BO7625 (*Sanoma Uitgevers/Nederland*), r.o. 93.
9 https://www.vcas.nl/index.php/2021/03/24/onderzoek-in-smartphones-klare-taal-gewenst/.
10 HR 9 februari 2021, ECLI:NL:HR:2021:202.
11 Veel lidstaten hebben nog steeds bewaarplichten voor telecomoperators in hun nationale wetten die op gespannen voet staat met de rechtspraak van het Hof; de Commissie heeft onlangs aangegeven dit kritisch te volgen maar vooralsnog af te zien van infractieprocedures.
12 HvJ EU 6 oktober 2020, gevoegde zaken C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net e.a. II*).
13 ECLI:DE:BVerfG:2020:rs20200505.2bvr085915.
14 https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-05/cp200058en.pdf.