Annotatie bij HR 5 april 2022, ECLI:NL:HR:2022:475

HR 5 april 2022, ECLI:NL:HR:2022:475, *Computerrecht* 2022/186, m.nt. J.J. Oerlemans en A. Berlee

1. Het *Prokuratuur*-arrest van 2 maart 2021 van het Hof van Justitie[1] is voor het Openbaar Ministerie (OM) aanleiding geweest om vanaf 19 augustus 2021 een machtiging van een rechter-commissaris te vragen, bij het vorderen van verkeers- en locatiegegevens in het kader van een opsporingsonderzoek naar misdrijven als omschreven in artikel 67 Wetboek van Strafvordering (Sv).[2] Onduidelijkheid over – onder andere – het begrip 'ernstige criminaliteit' leidde tot cassatie in het belang der wet door de procureur-generaal bij de Hoge Raad. In het arrest bevestigt de Hoge Raad dat een machtiging van een rechter-commissaris is vereist voor een vordering van verkeers- en locatiegegevens en het bevel tot bevriezing van deze gegevens. Ook stelt de Hoge Raad drie prejudiciële vragen aan het Hof van Justitie (HvJ EU). In deze annotatie gaan wij in op de gevolgen van het arrest en betogen wij dat het uitgangspunt dat uit *Prokuratuur* dat verkeersgegevens en locatiegegevens bijzonder privacygevoelig zijn een bredere gelding moet krijgen.

2. De feiten van de specifieke casus waren als volgt. De aanleiding vormde het vorderen van gegevens in het kader van een strafrechtelijk onderzoek naar de diefstal van een shovel (een grondverzetmachine (ook wel 'bulldozer') genoemd), ter waarde van ongeveer EUR 18.000,-. De officier van justitie vroeg een schriftelijke machtiging van de rechter-commissaris voor het vorderen van verkeers- en locatiegegevens op basis van artikel 126n lid 1 Sv. De r-c weigerde, omdat de toegang tot verkeers- en locatiegegevens met betrekking tot communicatie in navolging van Europese rechtspraak beperkt is tot procedures ter bestrijding van *zware* criminaliteit en ter voorkoming van ernstige bedreigingen van de openbare veiligheid. De diefstal van een shovel voldoet daar niet aan, volgens de r-c. De officier van justitie ging in beroep en de rechtbank vernietigde de beschikking van de r-c. De rechtbank oordeelde dat het wel degelijk ging om zware criminaliteit, omdat diefstal van een shovel kwalificeert als diefstal door twee of meer personen, waarvoor een maximale gevangenisstraf van zes jaar staat en voorlopige hechtenis op van grond artikel 67 Sv is toegelaten. Tegen de verdachte was bovendien een bevel van bewaring verleend.

3. Meer dan vijf maanden na de publicatie van het *Prokuratuur*-arrest werd door het OM de werkwijze aangepast en een machtiging van een rechter-commissaris aangevraagd voor vorderingen van verkeers- en locatiegegevens van aanbieders van communicatiediensten.[3] Het Hof van Justitie maakte in *Prokuratuur* duidelijk dat aangezien een officier van justitie tevens aanklager is in een later proces, deze niet kan voldoen aan de eis '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'.[4] Wij vinden het vreemd dat deze beslissing van het Openbaar Ministerie over de aanpassing van de procedure niet openbaar is gemaakt. In de rechtsliteratuur werd al reeds de conclusie getrokken dat een machtiging van een rechter-commissaris of een andere onafhankelijke autoriteit bij de vordering

[1] HvJ EU 2 maart 2021, C-746/18, ECLI:EU:C:2021:152, *EHRC-Updates.nl*, m.nt. D.A.G. van Toor (*Prokuratuur*).
[2] Zie in dit kader ook G.P. Sholeh, 'De betekenis van het Prokuratuur-arrest: digitale opsporing en privacy onder loep', *DD* 2022/15, nr. 3, p. 227-247.
[3] Het gaat daarbij om vorderingen in de zin van 126n, 126na, 126ni, 126u, 126ua, 126ui, 126zi, 126zja, 126zo Sv.
[4] HvJ EU 2 maart 2021, C-746/18, ECLI:EU:C:2021:152, r.o. 54 (*Prokuratuur*).

van dit soort gegevens in Nederland noodzakelijk was, omdat een officier van justitie niet als onafhankelijke autoriteit kan worden gezien.[5] Het had meteen duidelijk moeten zijn dat de wettelijke procedure voor het vorderen van verkeers- en locatiegegevens, waarvoor alleen een bevel van een officier van justitie was vereist, moest worden aangepast naar aanleiding van het arrest.

4. Ook de wetgever had kunnen ingrijpen door stappen te zetten om een nieuwe onafhankelijke autoriteit op te richten die de aanvragen voor het vorderen van verkeers- en locatiegegevens kan beoordelen, maar hier is geen debat over gevoerd. Het conceptwetsvoorstel tot modernisering van het wetboek van strafvordering en boek 2 met betrekking tot het opsporingsonderzoek bevat nog geen onafhankelijke voorafgaande toets bij het vorderen van verkeersgegevens en locatiegegevens. De Raad van State stelde in haar advies (afgegeven vóór de uitspraak van de Hoge Raad, maar gepubliceerd daarna) al vraagtekens bij de verenigbaarheid van deze bepaling met het de Europese regelgeving en rechtspraak van het Hof van Justitie.[6] Ten slotte heeft ook de rechtspraak niet te kennen gegeven welke gevolgen het arrest voor hen heeft en mogelijk tot capaciteitsproblemen in de rechtspraak leidt. De minister van Justitie & Veiligheid publiceert helaas geen statistieken over het aantal vorderingen. Het is alleen bekend dat in 2012 in totaal 41.658 vorderingen plaatsvonden die betrekking hadden op de categorie 'historische verkeersgegevens telecommunicatie'.[7] Het arrest van de Hoge Raad zou daarmee toch tot enig effect moeten leiden voor de rechtspraak.

5. Het is dan ook niet bepaald verassend dat de Hoge Raad in het onderhavige arrest beslist dat voor het vorderen en bevriezen van verkeers- en locatiegegevens een machtiging van een rechter-commissaris noodzakelijk is (r.o. 6.13.2). De rechter-commissaris controleert daarbij aan de eisen van de wet en of er is voldaan aan het evenredigheidsbeginsel (6.13.3). Daarbij moet worden meegewogen: (1) de ernst van het strafbare feit in algemene zin, (2) de ernst van het concrete strafbare feit waarop de verdenking betrekking heeft, (3) de specifiek gevorderde gegevens, (4) het belang van het verkrijgen van die gegevens voor het strafrechtelijke onderzoek en (5) de vraag of en, zo ja, in welke mate aan de hand van die gegevens conclusies kunnen worden getrokken over het privéleven (r.o. 6.8.3).[8] Laatstelijk dienen ook (6) de 'wettelijke garanties die bestaan dat de gegevens die worden verkregen, niet anders worden gebruikt dan voor het strafvorderlijke onderzoek, en (7) de voorschriften met betrekking tot de bewaring en de vernietiging van de verkregen gegevens' worden meegewogen (6.8.3). Wij merken hierbij op dat deze laatste twee uitgangspunten ook al in de Wet politiegegevens zijn te vinden.

6. De reden dat een toets een van een rechterlijke of andere onafhankelijke instantie bij het vorderen van verkeers- en locatiegegevens noodzakelijk wordt geacht, is dat deze gegevens als zeer

---

[5] Zie HvJ EU 2 maart 2021, C-746/18, ECLI:EU:C:2021:152 (*Prokuratuur*), *EHRC-Updates.nl*, m.nt. D.A.G. van Toor en R.M. te Molder, 'Het bewaren en vorderen van metagegevens ten behoeve van de opsporing: meer duidelijkheid van het HvJ EU gewenst', *DD* 2021/66, nr. 9, p. 844-869.

[6] Afdeling advisering van de Raad van State, *Advies over het nieuwe Wetboek van Strafvordering*, W16.21.0105/II, 6 april 2022, p. 136-138.

[7] Odinot e.a., 'De Wet bewaarplicht telecommunicatiegegevens. Over het bewaren en gebruiken van gegevens over telefoon- en internetverkeer ten behoeve van de opsporing', WODC, Den Haag: Boom Lemma Uitgevers 2013, p. 82-83. Op basis van cijfers uit 2017 gaat het daarnaast om nog eens 40.000 tap-bevelen op jaarbasis waarbij ook verkeersgegevens meekomen. Zie Memorie van Toelichting: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek, p. 255.

[8] R.o. 6.8.3.

privacygevoelig worden gezien.[9] Verkeersgegevens zijn 'gegevens *over* communicatie' (niet de inhoud).[10] In deze context betreft dat 'de datum en het tijdstip waarop de verbinding met de gebruiker tot stand is gebracht en beëindigd', de NAW-gegevens van degene met wie de verbinding is gebracht en de duur van de verbinding.[11] Locatiegegevens zijn gegevens waarmee de geografische positie kan worden bepaald aan de hand van de gebruikte zendmast(en).[12] Beiden typen gegevens worden gegenereerd als er verkeer via een telecommunicatienetwerk plaatsvindt, zoals bij het voeren van een telefoongesprek of het gebruik maken van internet. De Hoge Raad overweegt dat voor een strafrechtelijk onderzoek belangrijke aanknopingspunten kunnen zijn gelegen in informatie over telefoonnummers die zijn gebruikt, identificatienummers van telefoontoestellen, zendmasten waarmee toestellen in verbinding hebben gestaan of IP-adressen die verband houden met elektronische vormen van communicatie (r.o. 6.10.2).[13] De verzameling en verwerking van deze gegevens maken een ernstige inbreuk op het recht op privacy van betrokkenen, omdat nauwkeurige conclusies kunnen worden getrokken over de persoonlijke levenssfeer van de betrokken. Daarbij kunnen gegevens worden afgeleid 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.[14] Het heeft ook zijn weerslag op de uitoefening van vrijheid van meningsuiting.[15]

7. De rechtspraktijk worstelt klaarblijkelijk met de vraag of de begrippen 'ernstige criminaliteit' en 'zware criminaliteit' autonome begrippen van Unierecht zijn of het aan de bevoegde instanties van de lidstaten zelf is om (mede) invulling te geven aan deze begrippen. Daarom stelt de Hoge Raad hier een prejudiciële vraag over (r.o. 6.8). Volgens de Hoge Raad moeten misdrijven als omschreven in artikel 67 lid 1 Sv worden opgevat als 'ernstige criminaliteit', zoals bedoeld in de rechtspraak van het

---

[9] Aan de hand van deze gegevens kan inzicht worden verkregen in dagelijkse gewoonten, permanente of tijdelijke verblijfplaats, dagelijkse en andere verplaatsingen en activiteiten die worden uitgeoefend, even als de sociale relaties en sociale kringen waarin iemand zich begeeft worden ontwaard. Zie o.a. HvJ EU 21 december 2016, C-203/15, ECLI:EU:C:2016:970, r.o. 98-100 (*Tele2 Sverige/Watson*), HvJ EU 6 oktober 2020, C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791, r.o. 117 (*La Quadrature du Net e.a./Premier ministre e.a.*). Zelfs indien het gaat om toegang tot gegevens voor een korte periode, zie HvJ EU 2 maart 2021, C-746/18, ECLI:EU:C:2021:152, r.o. 40 (*Prokuratuur*). Vergelijk met HvJ EU 2 oktober 2018, C207/16, ECLI:EU:C:2018:788, r.o. 60, *EHRC* 2019/18, m.nt. B. van der Sloot (*Misterio Fiscal*). Hier ging het om het opvragen van de identiteit die was gekoppeld aan een geactiveerde SIM-kaart in een gestolen mobiele telefoon gedurende een korte en afgebakende tijd. Deze zeer beperkte informatie, was zonder aanvullende gegevens over de communicatie en over de locatie, onvoldoende om een nauwkeurige conclusie over het privéleven van de betrokken personen te trekken (r.o. 60).

[10] Zie hierover ook J.J. Oerlemans, M. Hagens, S. Royer, 'Tijd voor een nieuwe bewaarplicht?', *Computerrecht* 2021/59, nr. 2, p. 151-159.

[11] Zie artikel 2 sub c-d Besluit vorderen gegevens telecommunicatie.

[12] Locatiegegevens worden gedefinieerd in artikel 2 onder c Richtlijn 2002/58/EG en Artikel 11.1, onder d Telecommunicatiewet (Tw). Dit zijn gegevens die worden verwerkt in een elektronische-communicatienetwerk waarmee de geografische positie van de eindapparatuur van een gebruiker van een algemeen beschikbaar elektronische-communicatiedienst wordt aangegeven.

[13] Zie over het belang van deze gegevens voor de opsporing ook: Ferdinandusse, D. Laheij, J.C. Hendriks, 'De bewaarplicht telecomgegevens en de opsporing. Het belang van historische verkeersgegevens voor de opsporing', Openbaar Ministerie & Nationale Politie 2015.

[14] HvJ EU 2 maart 2021, C-746/18, ECLI:EU:C:2021:152, r.o. 36 (*Prokuratuur*).

[15] Zie HvJ EU 8 april 2014, C-293/12 en C-594/12, ECLI:EU:C:2014:238, r.o. 26-28 (*Digital Rights Ireland en Seitlinger e.a.*); HvJ EU 21 december 2016, C-203/15, ECLI:EU:C:2016:970, r.o. 92-93 en 101 (*Tele2 Sverige/Watson*) en HvJ EU 6 oktober 2020, C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791, r.o. 118 (*La Quadrature du Net e.a./Premier ministre e.a.*).

Hof van Justitie, omdat dit misdrijven zijn door de wetgever vanwege hun aard en ernst in de opsomming van artikel 67 lid 1 Sv zijn opgenomen (r.o. 6.8.1). Het betreffen misdrijven waarop een maximumgevangenisstraf van vier jaren of meer is gesteld en daarnaast een lijst van specifieke misdrijven uit het Wetboek van Strafrecht en uit bijzondere wetgeving.

8. De Hoge Raad stelt ook een prejudiciële vraag of de vorderingsbevoegdheden onder werkingssfeer van Richtlijn 2002/58/EG vallen, als het gaat om het verlenen van toegang tot gegevens die niet worden bewaard op grond van wettelijke maatregelen als bedoeld in artikel 15 lid 1 Richtlijn 2002/58/EG, maar die door de aanbieder worden bewaard op een andere grond (r.o. 8.2).[16] Hoewel de Hoge Raad tot uitgangspunt neemt dat uit de rechtspraak van het Hof van Justitie valt af te leiden dat het in wezen niet zou moeten uitmaken op grond waarvan de gegevens zijn bewaard, worden hier toch prejudiciële vragen over gesteld. Met name omdat er geen expliciet antwoord op deze vraag blijkt uit de uitspraken van het Hof en er ook argumenten tegen deze conclusie bestaan (ro. 6.2.4.-6.2.5).[17]

9. De derde prejudiciële vraag ziet op de situatie dat verkeers- en locatiegegevens worden gevorderd waarin de verdenking van een strafbaar feit nog niet concreet betrekking heeft op een specifieke persoon. Het kan dan gaan om een situatie waarbij verkeers- en locatiegegevens worden gevorderd en later wordt gekeken of daar gegevens een verdachte, slachtoffer of getuige tussen zitten (r.o. 6.10.2-6.10.3). De Hoge Raad stelt de vraag of deze vorderingsbevoegdheden in dat geval kunnen worden toegepast als *geen* sprake is van ernstige strafbare feiten of ernstige criminaliteit en slechts een *geringe* inmenging veroorzaakt in (met name) het recht op bescherming van het privéleven van de gebruiker als bedoeld in artikel 2, onder b, Richtlijn 2002/58/EG (r.o. 8.4). Wij achten de situatie waarbij het vorderen van verkeersgegevens- en locatiegegevens een geringe inbreuk maakt op het recht op privacy lastig voorstelbaar.

10. Het arrest heeft geen betrekking op de vraag of het wettelijk stelsel voldoet met betrekking tot het vorderen van verkeersgegevens of locatiegegevens van *andere* bedrijven of instellingen dan aanbieders van communicatiediensten.[18] De jurisprudentie laat zien dat verkeers- en locatiegegevens van 'automatic number plate recognition' (ANPR)-camera's en 'bluetooth trackers' die verbinding maken met apparaten in auto's en mobiele telefoons een belangrijke rol kunnen spelen als bewijs in strafzaken.[19] De privacyinbreuk is wat ons betreft in ieder geval ten dele vergelijkbaar en kan als ernstig worden gekwalificeerd, omdat personen met deze gegevens gelokaliseerd kunnen worden en verplaatsingsgedrag voor een deel in kaart kan worden gebracht. Met in het achterhoofd dat op steeds meer plekken trackers worden geplaatst die telefoons en andere apparaten kunnen uitlezen (door de politie ook wel 'sensoren' genoemd), is het volgens ons

[16] Zoals voor factureringsdoeleinden op grond van art. 11.5 lid 2 Tw (verkeersgegevens).
[17] De Hoge Raad verwijst hiervoor naar de vordering van de advocaat-generaal (punten 61-63).
[18] In dit kader is het ook nog goed op de merken dat de Raad van State adviseert in de toelichting op het wetsvoorstel tot aanpassing van opsporingsbevoegdheden in te gaan op de vraag "in hoeverre het Prokuratuur-arrest zou moeten leiden tot een herijking van de normering van (digitale) opsporingsbevoegdheden" (Advies over het nieuwe Wetboek van Strafvordering, p. 139).
[19] Zie bijvoorbeeld Rb. Zeeland-West-Brabant 28 juni 2016, ECLI:NL:RBZWB:2016:3865, Rb. Midden-Nederland 10 december 2018, ECLI:NL:RBMNE:2018:6343, Rb. Midden-Nederland 12 april 2019, ECLI:NL:RBMNE:2019:1592 (met een bewijsrol van gegevens uit het navigatiesysteem auto en van de 'Verkeers Informatie Dienst' (VID)) en Rb. Zeeland-West-Brabant 29 december 2020, ECLI:NL:RBZWB:2020:6702 (met een bewijsrol d.m.v. lokalisering op basis van ANPR-gegevens).

van belang dat ook deze vraag wordt geadresseerd. Het OM en de rechtspraak kunnen hier een meer proactieve houding in aannemen en anders is het aan de wetgever daarbij de grenzen aan te geven.

11. Het arrest kan voorts aanleiding zijn nog eens goed te kijken naar de wijze waarop het verstrekken van gegevens is geregeld in de Telecommunicatiewet. Zo kunnen er vraagtekens worden gezet bij de houdbaarheid van artikel 11.13 Telecommunicatiewet (Tw) in haar huidige vorm. In dit artikel wordt een eigen bevoegdheid gegeven aan de aanbieders van openbare elektronische communicatienetwerken om de artikelen 11.5 en 11.5a Tw, waarin de voorwaarden voor verwerking van respectievelijk verkeers- en locatiegegevens is geregeld, buiten toepassing te laten als dit noodzakelijk is in het belang van (a) de nationale veiligheid of (b) de voorkoming, opsporing en vervolging van strafbare feiten.[20] Dit artikel is er gekomen om te voorkomen dat de aanbieder bij het voldoen aan een vordering op grond van bijvoorbeeld artikel 126n Sv zelf de Telecommunicatiewet overtreedt.[21] De verplichte medewerking met vorderingen op grond van artikelen 126n, 126na, 126u en 126ua Sv en artikel 55 Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017) is echter al geregeld in artikel 13.4 jo 13.2 Tw.[22] Indien het daarnaast nog noodzakelijk zou zijn om apart op te nemen dat de daarmee gepaarde inbreuk op artikelen 11.5 en/of 11.5a Tw gerechtvaardigd is, dan zou in de rede liggen om dit in artikel 13.4 Tw te regelen in plaats van in een aparte bepaling. Daarnaast is het maar de vraag of het ruim geformuleerde artikel 11.13 Tw zelfstandig bezien in overeenstemming is met het EU-recht,[23] nu de bepaling het buiten toepassing laten van artikelen 11.5 en 11.5a Tw zonder enige vorm van waarborgen of handvatten voor de aanbieder overlaat aan de aanbieder. Ook wordt er gesproken over 'strafbare feiten' en niet 'ernstig strafbare feiten' wat gelet op de mate van inmenging op het privéleven die een verwerking - anders dan op grond van artikelen 11.5 en 11.5a Tw - met zich mee brengt tenminste enige twijfel oproept met betrekking tot de houdbaarheid van die bepaling.

12. Ten slotte wijzen wij erop dat dat ook in andere wetgeving dan het Wetboek van Strafvordering bevoegdheden bestaan voor het vorderen van gegevens bij aanbieders van communicatiediensten. Zoals ook al eerder elders is betoogd naar aanleiding van het arrest *La Quadrature du Net e.a./Premier ministre e.a.*, ligt het in de rede artikel 55 Wiv 2017 aan te passen.[24] Dit artikel heeft ook betrekking op het vorderen van verkeersgegevens bij aanbieders van communicatiediensten. Volgens het wetsartikel is toestemming van de minister van Binnenlandse Zaken en Koninkrijksrelaties of de minister van Defensie vereist, waarbij zelfs mandatering aan het hoofd van

[20] Artikel 11.13, lid 1 Tw.

[21] *Kamerstukken II* 2002/03, 28 851, nr. 3, p. 165: *"Op deze wijze staat buiten kijf dat de hier bedoelde handelingen zijn geoorloofd."*

[22] Het zijn dus artikel 13.4 Tw en de daarin genoemde artikelen die moeten voldoen aan de vereisten uit artikel 15 Richtlijn 2002/58/EG, zoals uitgelegd door het HvJ EU. Indien dit het geval is, dan is daarmee de inbreuk op het vertrouwelijk karakter van de communicatie en daarmee verband houdende verkeersgegevens zoals vastgelegd in artikel 5 van de Richtlijn, ook gerechtvaardigd.

[23] In het bijzonder artikel 15 Richtlijn 2002/58/EG welke de voorwaarden uiteenzet voor een wettelijke maatregel die een uitzondering op artikel 6 en 9 van richtlijn 2002/58/EG geïmplementeerd in artikelen 11.5 en 11.5a Tw mogelijk maken.

[24] Zie HvJ EU 6 oktober 2020, C-511/18, C512/18 en C-520/18, ECLI:EU:C:2020:791 *(La Quadrature du Net e.a./Premier ministre e.a.*) en HvJ EU 6 oktober 2020, C-623/17, ECLI:EU:C:2020:790 (*Privacy International/Secretary of State for Foreign and Commonwealth Affairs e.a.*), *JBP 2021/1-2*, m.nt. J.J. Oerlemans & M. Hagens. Zie ook 'Reactie TIB op conceptwetsvoorstel Tijdelijke wet onderzoek AIVD en MIVD naar landen met een offensief cyberprogramma', 14 april 2022, *tib-ivd.nl*.

de desbetreffende inlichtingen- en veiligheidsdienst mogelijk is. Net als het openbaar ministerie staat een minister onvoldoende op afstand van de uitvoerende macht. De wet kan worden aangepast door voorafgaand toestemming van een onafhankelijke autoriteit te vereisen, zoals de Toetsingscommissie Inzet Bevoegdheden (TIB).

J.J. Oerlemans & A. Berlee[25]

[25] Jan-Jaap Oerlemans is bijzonder hoogleraar Inlichtingen en Recht bij de Universiteit Utrecht en senioronderzoeker bij de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD). Anna Berlee is hoogleraar Gegevensbescherming en Privacyrecht bij de Open Universiteit.