EHRC EUROPEAN HUMAN RIGHTS CASES UPDATES

ANNOTATIE

Prokuratuur (HvJ EU, C-746/18) – Differentiatie en beperkingen van dataretentie door telecommunicatieaanbieders en de vorderingsvoorwaarden

D.A.G. van Toor

Annotatie bij Hof van Justitie van de Europese Unie, 02-03-2021, ECLI:EU:C:2021:152 (EHRC-2021-0088)

1. In strafzaken is het verzamelen van elektronisch bewijsmateriaal vaak essentieel voor de waarheidsvinding.[1] Niet alleen in *cybercrime*-onderzoeken, maar ook in klassieke strafonderzoeken speelt digitaal bewijs een cruciale rol.[2] Het is derhalve niet verwonderlijk dat dataretentie een belangrijk thema is. Richtlijn 2002/58/EG[3] biedt lidstaten daarom de mogelijkheid om privacybeperkende wetgeving te creëren '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' (art. 15). Met Richtlijn 2006/24/EG[4] verplichtte en harmoniseerde de EU zelfs de dataretentie door telecommunicatieaanbieders (art. 1). Art. 5 en 6 van die Richtlijn tezamen bezien, verplichten telecommunicatieaanbieders *alle* data over hun klanten voor ten minste zes maanden en ten hoogste twee jaar te bewaren.

2. Sinds die bepalingen van kracht zijn en lidstaten telecommunicatieaanbieders verplichten data te bewaren, is een strijd losgebarsten over de precieze spelregels rond de opslag van de data en, nog belangrijker, de mogelijkheid voor de strafvorderlijke autoriteiten om die data te vorderen ten behoeve van de opsporing.[5] De onderhavige zaak is de volgende zaak waarin het om de interpretatie van het hierboven aangehaalde art. 15 Richtlijn 2002/58/EG in het licht

van de bescherming van de privésfeer van burgers gaat.

3. In *Digital Rights Ireland* werd de toon door het Hof van Justitie EU gezet: dataretentie en de mogelijkheid om data te gebruiken voor de in art. 15 Richtlijn 2002/58/EG genoemde doelen is van evident belang (par. 44), maar dat betekent nog niet dat ongedifferentieerde en ongelimiteerde opslag van die data door telecommunicatieaanbieders en toegang tot die data door de autoriteiten door de beugel kan (par. 51). De gehele Richtlijn werd door het Hof van Justitie EU ongeldig verklaard.

Eén (!) dag later besloot Tele2 in Zweden te stoppen met zijn dataretentie en bracht de Zweedse Telecommunicatieautoriteit (PTS) hiervan op de hoogte. De Zweedse autoriteiten waren echter van mening dat de omzetting van Richtlijn 2006/24/EG in zijn nationale wetgeving niet in strijd is met de mensenrechtelijke bescherming volgend uit het EU-recht en het EVRM. Uit *Digital Rights Ireland* zou niet volgen dat de ongelimiteerde en ongedifferentieerde opslag problemen oplevert omdat Richtlijn 2002/58/EG dataretentie mogelijk maakt, maar slechts dat Richtlijn 2006/24/EG ongeldig zou zijn.

Deze argumentatie snijdt (natuurlijk) geen hout. In *Tele2* oordeelde het Hof van Justitie dat het feit dat lidstaten op grond van art. 15 Richtlijn 2002/58/EG telecommunicatieaanbieders mogen verplichten data te bewaren hen geen vrijbrief geeft. Lidstaten moeten ook recht doen aan de bescherming van grondrechten (artt. 7, 8 en 11 Hv) en de voor inbreukmakende wetgeving geldende rechtvaardigingscriteria (art. 52 Hv) (par. 112). Vervolgens geeft het Hof van Justitie de lidstaten huiswerk, ondanks dat het vormgeven van de precieze spelregels aan de nationale wetgevers wordt overgelaten (par. 118): zo moet in ieder geval een systeem van voorafgaande onafhankelijke controle op vorderingen tot toegang tot de data worden ingericht (par. 120). Het is deze waarborg die centraal staat in *Prokuratuur*.

4. In de onderhavige zaak zijn door het Hooggerechtshof van Estland prejudiciële vragen gesteld over de interpretatie van het eerder aangehaalde art. 15 Richtlijn 2002/58/EG. Dat artikel bepaalt dat lidstaten beperkingen in de vertrouwelijkheid van allerlei informatie die telecommunicatieaanbieders verkrijgen van hun klanten mogen aanbrengen. In *Prokuratuur* gaat het om de vraag of de Estse wet voldoende waarborgen kent tegen de ongebreidelde toegang van politiële en justitiële autoriteiten tot de gegevens die telecommunicatieaanbieders op moeten slaan. Deze zaak is dus een vervolg op de eerder aangehaalde zaken *Digital Rights Ireland* – waarin de harmonisatie van dataretentie ongeldig werd verklaard – en *Tele2* – dat ongelimiteerde en ongedifferentieerde dataretentie een schending van het Hv oplevert. In *Prokuratuur* staan de precieze waarborgen die in een lidstaat gelden voor de toegang tot verkeers- en locatiegegevens door strafvorderlijke autoriteiten centraal en dus niet inhoudelijke communicatie![6]

5. Voor het strafrecht is deze informatie van essentieel belang. Met de opgeslagen locatiegegevens kan de positie en de beweging van een verdachte via zijn SIM-kaart in kaart worden gebracht.[7] In *Prokuratuur* heeft het Estse Openbaar Ministerie gegevens gevorderd bij een telecommunicatieaanbieder die, volgens de Estse variant van de Wet Vorderen Gegevens, verplicht zijn alle informatie één jaar te bewaren. Art. 90 van de Estse Sv beperkt de toegang tot die gegevens verder niet: in het vooronderzoek kan het Openbaar Ministerie, dat de leiding heeft over de opsporing en vervolging van strafbare feiten en volgens de Estse wet een partij in het geding is, zelfstandig bepalen dat hij toegang tot gegevens noodzakelijk acht voor het bereiken van het doel van het strafproces, namelijk waarheidsvinding. Aan de veroordeling waarop de prejudiciële vragen zijn gebaseerd, liggen zulke gegevensanalyses ten grondslag. Niet duidelijk wordt echter welke gegevens precies zijn gevorderd en gebruikt (par. 16-18). In cassatie neemt de veroordeelde het standpunt in dat de Estse wet niet in overeenstemming met het EU-recht is, omdat uit *Tele2* en *Digital Rights Ireland* blijkt dat de toegang tot gegevens beperkt moet worden tot zaken waarin het gaat om *serious crimes* en dat een onafhankelijk (administratieve) autoriteit de vordering moet toetsen (par. 20 e.v.).

6. Omdat toegang tot (zelfs in tijd beperkte en een beperkte hoeveelheid) gegevens kan leiden tot precieze conclusies over iemands privéleven moeten lidstaten voor dataretentie en het vorderen van gegevens voldoende waarborgen tegen ongelimiteerde en ongedifferentieerde opslag en toegang te bieden. Dit geldt ook voor verkeers- en locatiegegevens (par. 40). Een van de waarborgen waaraan voldoen moet zijn, is de eis van proportionaliteit (par. 38). De ongedifferentieerde en ongelimiteerde dataretentie levert volgens het Hof een ernstige inbreuk op op art. 7 en 8 Hv en is alleen mogelijk *to combat serious crime* (par. 33). Bij lichte (*non-serious*) inbreuken op dezelfde grondrechten is een meer algemene dataretentie wel gerechtvaardigd (par. 33). Aangezien het bij verkeers- en locatiegegevens alsmede inhoudelijke communicatie al snel gaat om informatie waarmee precieze conclusies over iemands privéleven getrokken kunnen worden, ligt het niet voor de hand dat bij deze gegevens sprake is van een *non-serious interference*. Dit zou dan alleen mogelijk kunnen zijn bij gebruikersgegevens of in tijd en hoeveelheid zeer beperkte verkeers- en locatiegegevens. Het is in ieder geval zonneklaar dat het Hof van Justitie, anders dan veel lidstaten en de Commissie (ten tijde van Richtlijn 2006/24/EG), de bescherming van privébelangen bij dataretentie serieus neemt en de teugels bij de toetsing van de waarborgen stevig aanhaalt.

7. Dit wordt nog duidelijker bij de laatste prejudiciële vraag, die de status van de officier van justitie bij het vorderen van gegevens betreft. Hier komen twee lijnen uit de rechtspraak van het Hof van Justitie samen: de rechtspraak over de rol van de officier van justitie in het uitvaardigen van een EAB en de waarborgen bij dataretentie.

In de zaken *OG en PI* en *AZ* bepaalde het Hof van Justitie dat een openbaar ministerie in

onvoldoende mate onafhankelijk is als hij kan worden aangestuurd door de uitvoerende macht, zoals een minister van Justitie.[8] Hierdoor valt zo'n openbaar ministerie niet langer onder het begrip *rechterlijke* autoriteit zoals bedoeld in het Kaderbesluit EAB. Dit heeft als gevolg dat officieren van justitie in Nederland niet langer EAB's kunnen uitvaardigen. De Overlevingswet is op basis van deze rechtspraak aangepast.

In *Tele2* oordeelde het Hof van Justitie dat bij de afweging of de inbreuk op de belangen van burgers bij het vorderen van gegevens opweegt tegen *inter alia* een effectieve bijdrage aan het bestrijden van strafbare feiten, *voorafgaande* toetsing van de vordering 'either by a court or by an independent administrative body' noodzakelijk is.[9]

8. In de onderhavige uitspraak komen deze twee lijnen dus samen: in Estland kan het openbaar ministerie zelfstandig oordelen over de toegang tot door telecommunicatieaanbieders opgeslagen gegevens, terwijl uit de rechtspraak van het Hof van Justitie EU blijkt dat toetsing door een rechtbank of een onafhankelijke autoriteit noodzakelijk is *en* dat het openbaar ministerie onder omstandigheden geen onafhankelijke autoriteit is. Dat laatste oordeelt het Hof van Justitie ook in de onderhavige zaak, maar op andere gronden. De mogelijke politieke inmenging – die eventueel belangrijk kan zijn bij het uitvaardigen en beoordelen van EAB's – speelt bij dataretentie geen rol van betekenis, maar de officier van justitie is natuurlijk betrokken bij de opsporing en vervolging van strafbare feiten. In de meeste strafvorderlijke systemen is de officier van justitie zowel de leidinggevende over de opsporing als de persoon die tot vervolging overgaat. Het is dan natuurlijk al snel dat het verkrijgen van (veel) data in de ogen van de officier van justitie van belang is voor zijn zaak, en dat een wat meer magistratelijke toets mogelijk niet van hem kan worden verwacht. Vanwege de betrokkenheid van de officier van justitie in de procedure in Estland acht het Hof van Justitie hem onvoldoende onafhankelijk, ongeacht het feit dat de officier van justitie wettelijk gezien aan waarheidsvinding doet en dus zowel belastend als ontlastend bewijs dient te verzamelen (par. 55-56). De toetsende instantie bij het vorderen van gegevens moet een derde zijn, die geen verband heeft met de autoriteit die de vordering indient (par. 54).

9. Dit arrest heeft grote impact voor strafvorderlijke systemen waarbij de officier van justitie de spil in het opsporingsonderzoek is en grotendeels zelf verantwoordelijk is voor het vergaren van het bewijs. Dit geldt in ieder geval voor Nederland. Bij omzetting van art. 15 Richtlijn 2002/58/EG dienen lidstaten als waarborg tegen potentieel machtsmisbruik en om een onafhankelijke beoordeling van de belangen te garanderen een systeem te creëren waarbij de vorderende autoriteit wordt gecontroleerd. De Nederlandse wetgever heeft gekozen voor de officier van justitie als centrale autoriteit en heeft sommige, lichtere, bevoegdheden bij opsporingsambtenaren gelegd,[10] meestal zonder voorafgaande toetsing.

Op dit moment kan de opsporingsambtenaar, zonder nadere tussenkomst van een hogere autoriteit, gebruikersgegevens (art. 126na Sv) en identificerende gegevens (art. 126nc Sv) vorderen van een telecommunicatieaanbieder. Inhoudsgegevens kunnen overigens alleen door de officier van justitie met voorafgaande rechterlijke toetsing worden gevorderd (art. 126ng Sv). De verkeers- en locatiegegevens (die onder art. 126nd Sv vallen) staan centraal in *Prokuratuur*. De toekenning van deze bevoegdheden aan de officier van justitie hebben in Nederland niet tot (politiek[11] of wetenschappelijk[12]) debat geleid. Dat debat moet nu alsnog plaatsvinden.

10. Uit het arrest volgt namelijk duidelijk dat wanneer precieze conclusies over iemands privéleven mogelijk zijn aan de hand van de gevorderde verkeers- of locatiegegevens een rechterlijke autoriteit of een onafhankelijke administratie-autoriteit over de vordering moet beslissen. Het Hof van Justitie EU bepaalt dat daarvan sprake is bij een beperkte hoeveelheid gegevens of gegevens van een in tijd beperkte periode. In ieder geval moet de vordering worden getoetst door een derde. Het ligt, gezien de privacygevoeligheid van inhoudsgegevens, voor de hand dat daarbij ook toetsing door een onafhankelijke derde moet plaatsvinden. In principe biedt *Prokuratuur* een uitweg voor de verstrekking van een geringe hoeveelheid gegevens of gegevens over een in tijd beperkte periode, maar het past niet in de idee van de toetsing van de privacybelangen door een derde om de officier van justitie of de opsporingsambtenaar zelfstandig te laten beslissen wanneer sprake is van een beperkte vordering.

11. Voor Nederland betekent dit, dat de huidige systematiek van de Wet Vorderen Gegevens op de schop moet: naast de verstrekking van gevoelige gegevens (art. 126nf Sv) en de directe doorleiding van toekomstige inhoudsgegevens (art. 126ne lid 3 Sv), waarvoor al een systeem van het toetsen van de vordering bestaat, dient op basis van het onderhavige arrest toetsing te worden voorzien voor vorderingen betreffende (i) verkeers- en locatiegegevens en, naar analogie op basis van de ernst van de privacy-inbreuk, (ii) inhoudsgegevens. Het is mogelijk, en ligt door de systematiek van de Wet Vorderen Gegevens voor de hand, de officier van justitie te verplichten een machtiging van de rechter-commissaris te verkrijgen voor het vorderen van deze gegevens. Een andere mogelijkheid is het optuigen van een onafhankelijke administratieve commissie, een soort privacy-waakhond, die alle vorderingen van de officier van justitie aan telecommunicatieaanbieders toetst. Hoe dan ook, de zelfstandige bevoegdheid van de officier van justitie om bepaalde data van telecommunicatieaanbieders te vorderen, is in strijd de Unierechtelijke privacybescherming.

D.A.G. van Toor

[1] P.A.M. Mevis, J.H.J. Verbaan & B.A. Salverda, *Onderzoek aan in beslag genomen elektronische gegevensdragers en geautomatiseerde werken ten behoeve van de opsporing en vervolging van strafbare feiten*, WODC 2016, p. 6; M. Viersma, 'Teruggeven na beslag op computers: alleen de bestanden of ook de computer?', *Strafblad* 2019, 1, p. 29.

[2] Zoals Henseler in zijn lectorale rede heeft betoogd, maken smartphones tot wel 80 procent uit van het digitale bewijs in strafzaken: J. Henseler, 'De (R)evolutie van Digitaal Bewijs', lectorale rede 21 november 2017, Hogeschool Leiden, p. 13. Zie ook J.J. Oerlemans, 'Beschouwing rapport Commissie-Koops: strafvordering in het digitale tijdperk', *Platform Modernisering Strafvordering* 2018; B.J. Koops & J.J. Oerlemans, *Strafrecht en ICT* (Monografieën recht en informatietechnologie), Den Haag: SDU 2019, p. 125; S. Royer & J.J. Oerlemans, 'Naar een nieuwe regeling voor beslag op gegevensdragers', *Computerrecht* 2017/200, p. 277. Dat het digitale bewijs ook daadwerkelijk wordt gebruikt in niet-*cybercrime*zaken blijkt onder meer uit 'Digitaal bewijs in moordzaken', *Computerrecht* 2019/125, p. 225-226 & 'Digitaal bewijs in strafzaken', *Computerrecht* 2020/38, p. 69-70.

[3] Richtlijn 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).

[4] Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG.

[5] *Digital Rights Ireland*, HvJ EU (GK) 8 april 2014, C-293/12 en C-594/12, ECLI:EU:C:2014:238, «EHRC» 2014/140, m.nt. Koning; *Tele2*, HvJ EU (GK) 21 december 2016, C-203/15 en C-698/15, ECLI:EU:C:2016:970, «EHRC» 2017/79, m.nt. Koning; *La Quadrature du Net*, HvJ EU (GK) 6 oktober 2020, C-511/18 e.a., ECLI:EU:C:2020:791, EHRC Updates januari 2021, m.nt. Schroers.

[6] Anders *La Quadrature du Net*, HvJ EU (GK) 6 oktober 2020, C-511/18 e.a., ECLI:EU:C:2020:791, EHRC Updates januari 2021, m.nt. Schroers, waarin het Hof in meer algemene zin over de doeleinden en voorwaarden van dataretentie oordeelt.

[7] Vgl. Supreme Court of the USA 22 juni 2018, No. 16-402 (*Carpenter v. United States*), waarin via *cell-site location information* van Carpenters SIM-kaart hij op of in de buurt van locaties

van overvallen kon worden geplaatst.

[8] *OG en PI*, HvJ (GK) 27 mei 2019, C-508/18 en C-82/19 PPU, ECLI:EU:C:2019:456, «EHRC» 2019/181 m.nt. Lestrade; *AZ*, HvJ 24 november 2020, C-510/19), ECLI:EU:C:2020:953, EHRC Updates februari 2021, m.nt. Lestrade.

[9] *Tele2*, HvJ EU (GK) 21 december 2016, C-203/15 en C-698/15, ECLI:EU:C:2016:970, «EHRC» 2017/79, m.nt. Koning, par. 120.

[10] Kamerstukken *II*, vergaderjaar 2003-2004, 29 441, nr. 3, p. 7-8.

[11] In de Memorie van Toelichting staat het strafvorderlijke uitgangspunt vermeld dat naarmate 'de bevoegdheid ingrijpender is, dient het te gaan om een verdenking van een ernstiger misdrijf en komt de bevoegdheid toe aan een hogere autoriteit.' Kamerstukken *II*, vergaderjaar 2003-2004, 29 441, nr. 3, p. 5. Voor de Wet Vorderen gegevens gaat dat alleen voor de interceptie van toekomstige inhoudsgegevens en bij de verstrekking van gevoelige gegevens een machtiging van de rechter-commissaris is vereist. De lichtere bevoegdheid van het vorderen van identificerende gegevens is zelfs toegekend aan de laagste autoriteit, te weten de opsporingsambtenaar.

[12] In *Tekst & Commentaar* en het *Handboek Strafzaken* wordt besproken wie de bevoegde autoriteit is per bevoegdheid, zonder nadere kritische bespreking. Ook uit andere publicaties volgt het beeld dat het geaccepteerd is dat de minst privacygevoelige gegevens door de opsporingsambtenaar kunnen worden gevorderd en dat bij de meest ingrijpende bevoegdheden een rechterlijke machtiging noodzakelijk is. Het vorderen van locatie- en verkeersgegevens worden niet in die laatste categorie geplaatst.