EHRC EUROPEAN HUMAN RIGHTS CASES UPDATES

ANNOTATIE

SpaceNet en VD (HvJ EU, C-793/19 en C-339/20) – Here we go again: Duitse en Franse dataretentieregeling(en) in strijd met Unierecht

D.A.G. van Toor

Annotatie bij Hof van Justitie van de Europese Unie, , ECLI:EU:C:2022:703 (EHRC-2022-0244)

Annotatie bij Hof van Justitie van de Europese Unie, , ECLI:EU:C:2022:854 (EHRC-2022-0244)

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 daarom niet verwonderlijk dat dataretentie een belangrijk thema is: na analyse van historische locatie- en verkeersgegevens kan een overzicht worden verkregen *waar* een persoon is geweest en met *wie* (althans met welk telefoonnummer) hij contact heeft gelegd. Zo leidde de gevorderde gegevens in de recent in dit tijdschrift geannoteerde zaak *An Garda* naar de dader, terwijl de moord zonder de toevallige vondst van de telefoon van het slachtoffer en de daaropvolgende uitgevaardigde gegevensvorderingen hoogstwaarschijnlijk onopgelost zou zijn gebleven.[3] Richtlijn 2002/58/EG[4] 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[5] trachtte de EU de dataretentie door

telecommunicatieaanbieders te verplichten en te harmoniseren (art. 1). Artikelen 5 en 6 van die Richtlijn tezamen bezien, leidt tot de conclusie dat *alle* metadata die telecommunicatieaanbieders over hun klanten verkrijgen voor ten minste zes maanden en ten hoogste twee jaar *moeten* worden bewaard. Ook in de onderhavige zaken gaat het om de interpretatie van het hierboven aangehaalde artikel 15 Richtlijn 2002/58/EG.

2. Sinds die bepalingen – met ongebreidelde overheidsmacht, waarbij telecommunicatieaanbieders tot lakeien van handhavingsautoriteiten zijn "verheven" – 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.[6] Met het eerder aangehaalde arrest *Digital Rights Ireland* werd de toon door het Hof van Justitie EU gezet: dataretentie en de mogelijkheid om data te gebruiken voor de in artikel 15 Richtlijn 2002/58/EG genoemde doelen is van evident belang (par. 44, *Digital Rights Ireland*), 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, *Digital Rights Ireland*). De gehele Richtlijn wordt door het Hof van Justitie EU ongeldig verklaard. Een (!) dag later besloot Tele2 in Zweden te stoppen met zijn dataretentie en bracht de Zweedse Telecommunicatieautoriteit (PTS) hiervan op de hoogte. De Zweedse autoriteiten zijn echter van mening dat de omzetting van Richtlijn 2006/24/EG in zijn nationale wetgeving – de ongelimiteerde en ongedifferentieerde dataretentie – 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 op problemen stoot 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* oordeelt het Hof van Justitie EU dat het feit dat lidstaten op grond van artikel 15 Richtlijn 2002/58/EG telecommunicatieaanbieders mogen verplichten data te bewaren niet betekent dat geen recht moet worden gedaan aan de bescherming van mensenrechten (artt. 7, 8 en 11 Hv) en de voor inbreukmakende wetgeving geldende rechtvaardigingscriteria (art. 52 Hv) (par. 112, *Tele2*). Vervolgens geeft het Hof van Justitie EU de lidstaten huiswerk, ondanks dat het vormgeven van de precieze spelregels aan de nationale wetgevers wordt overgelaten (par. 118, *Tele2*): zo moet in ieder geval een systeem van voorafgaande onafhankelijke controle op vorderingen tot toegang tot de data worden ingericht (par. 120, *Tele2*).

3. Dat huiswerk is door vele lidstaten echter nog steeds niet correct gemaakt. Zo werd in *Prokuratuur* duidelijk uiteengezet dat de vervolgende autoriteit (onder omstandigheden) onvoldoende onafhankelijk is om *a priori* te oordelen over toegang tot bewaarde data, omdat het 'openbaar ministerie immers niet tot taak (heeft) 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.'[7] In de recente zaak die Dwyer aanspande tegen de vergaande toegang tot gegevens door de Ierse *An Garda* oordeelt het Hof van Justitie EU dat toetsing *a posteriori* via een klachtenregeling een onvoldoende waarborg tegen misbruik vormt.[8] Verder oordeelt het Hof van Justitie EU in *An Garda* dat gerichte bewaring van verkeers- en locatiegegevens mogelijk niet in strijd is met het recht, terwijl identificerende gegevens zoals een IP-adres wel ongedifferentieerd kunnen worden opgeslagen.[9] In beide gevallen mag de data wel alleen zo lang als strikt noodzakelijk worden opgeslagen.[10] Juist dat punt staat in de onderhavige Duitse zaak (*Spacenet*) centraal: Duitsland kent wel een ongedifferentieerde opslag, maar die is – in vergelijking met alle in deze annotatie hierboven aangehaalde zaken – kort te noemen, namelijk slechts enkele weken (par. 33, *Spacenet*). Ter vergelijk, in *VD* – waarin het Hof van Justitie EU voor het eerst oordeelt dat ook als het gaat om toegang tot gegevens door de Autoriteit Financiële Markt op basis van de Richtlijn en Verordening Marktmisbruik dit onder de e-Privacy Richtlijn moeten worden beoordeeld – stond namelijk een retentieperiode van één jaar centraal.

4. Dat maakt vooral *Spacenet* een interessante zaak in het licht van de andere dataretentie-arresten. Kan de beperkte Duitse retentie*periode*, ook al is de retentie ongedifferentieerd en algemeen (par. 83),[11] voldoen aan de in de eerder aangehaalde jurisprudentie genoemde periode van strikte noodzakelijkheid ter bestrijding van zware criminaliteit? Of anders geformuleerd: is ongerichte bewaring van gegevens gerechtvaardigd voor een korte periode (par. 85)? Het Hof van Justitie EU beoordeelt dit in het licht van de ernst van de inmenging, die nader wordt geoperationaliseerd door in hoeverre door de opgeslagen gegevens een zeer precies beeld over het privéleven van een gebruiker van een elektronisch communicatiemiddel wordt verschaft (par. 89). Let wel: het gaat daarom al om de *bewaring*, en niet om de toegang. Het is, volgens het Hof van Justitie EU, namelijk de bewaring die al een ernstige inmenging in het te beschermen privéleven veroorzaakt, doordat die bewaring de noodzakelijke voorwaarde is voor toegang tot de gegevens en door de opslag het risico ontstaat dat zeer precieze conclusies over eindgebruikers privéleven kunnen worden getrokken.

5. Het antwoord op de twee hierboven gestelde vragen is dan ook duidelijk negatief. Ten behoeve van de bestrijding van zware criminaliteit is alleen *gerichte bewaring* mogelijk, op basis van objectieve en niet-discriminatoire gronden, voor een periode niet langer dan strikt noodzakelijk (par. 131). Wel is een ongedifferentieerde en algemene bewaarplicht voor IP-adressen mogelijk ten behoeve van de bestrijding van *zware* criminaliteit en voor zo lang als strikt noodzakelijk (par. 131). Ook is een ongedifferentieerde en algemene bewaarplicht met betrekking tot identificerende gegevens mogelijk ten behoeve van de bestrijding van

criminaliteit (en dus niet slechts wanneer sprake is van de bestrijding van zware criminaliteit (par. 131)). Dit betekent dat – ook met inachtneming van het eerder aangehaalde arrest *Prokuratuur* –,[12] mocht de Nederlandse regering in de Modernisering van het Wetboek van Strafvordering wederom kiezen voor een verplichte bewaarplicht, een naar (i) de aard van de gegevens; en (ii) naar de aard van de te bestrijden criminaliteit een gedifferentieerde regeling dient te worden ontworpen.

6. Tot slot nog een opmerking over de aanhangige prejudiciële vragen die de Hoge Raad stelde naar aanleiding van het *Prokuratuur*-arrest.[13] De derde vraag uit het *Post-Prokuratuur*-arrest luidt: 'Kan het verlenen van toegang aan overheidsinstanties tot verkeers- en locatiegegevens (anders dan uitsluitend identificerende gegevens) met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten onder Richtlijn 2002/58/EG worden toegestaan als geen sprake is van ernstige strafbare feiten of ernstige criminaliteit, namelijk als in het concrete geval het verlenen van toegang tot die gegevens – naar mag worden aangenomen – 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?' Het antwoord op deze vraag ligt duidelijk besloten in het daarna gewezen arrest *An Garda* en de twee onderhavige arresten: de *bewaring* van, en niet pas de *toegang* tot, verkeers- en locatiegegevens vormen per definitie een grove inmenging op het privéleven van eindgebruikers.

Dave 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] *G.D. t. the Commissioner of the Garda Síochána e.a.*, HvJ EU 5 april 2022, C-140/20, ECLI:EU:C:2022:258, par. 112 *EHRC Updates november 2022,* m.nt. Jansen en Te Molder.

[4] 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).

[5] 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.

[6] *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; *G.D. t. the Commissioner of the Garda Síochána e.a.*, HvJ EU 5 april 2022, C-140/20, ECLI:EU:C:2022:258, *EHRC Updates november 2022,* m.nt. Jansen en Te Molder).

[7] *Prokuratuur*, HvJ EU 2 maart 2021, C-746/18, ECLI:EU:C:2021:152, par. 55 *EHRC Updates mei 2021*, m.nt. Van Toor

[8] *G.D. t. the Commissioner of the Garda Síochána e.a.*, HvJ EU 5 april 2022, C-140/20, ECLI:EU:C:2022:258, par. 112 *EHRC Updates november 2022,* m.nt. Jansen en Te Molder.

[9] *G.D. t. the Commissioner of the Garda Síochána e.a.*, HvJ EU 5 april 2022, C-140/20, ECLI:EU:C:2022:258, par. 101 *EHRC Updates november 2022,* m.nt. Jansen en Te Molder.

[10] *G.D. t. the Commissioner of the Garda Síochána e.a.*, HvJ EU 5 april 2022, C-140/20, ECLI:EU:C:2022:258, par. 112 *EHRC Updates november 2022,* m.nt. Jansen en Te Molder.

[11] Het Hof van Justitie EU is daarover niet mild: 'Uit de verwijzingsbeslissing blijkt dus dat de door deze nationale regeling voorgeschreven bewaring van verkeers- en locatiegegevens betrekking heeft op nagenoeg de hele bevolking, zonder dat de betrokkenen zich – al was het maar indirect – in een situatie bevinden die aanleiding kan geven tot strafrechtelijke vervolging. Evenzo stelt die regeling de algemene en vanuit een persoonlijk, temporeel en geografisch oogpunt ongedifferentieerde bewaring – zonder grondslag – van het merendeel van de verkeers- en locatiegegevens verplicht, waarvan de omvang in wezen overeenkomt met die van de gegevens die werden bewaard in de zaken die hebben geleid tot de in punt 78 van

dit arrest aangehaalde rechtspraak.'

[12] HR 5 april 2022, ECLI:NL:HR:2022:475.

[13] HR 5 april 2022, ECLI:NL:HR:2022:475.