ANNOTATIE

HvJEU La Quadrature du Net (HvJ EU, C-511/18 e.a.) – Het Hof van Justitie en de voorwaarden voor dataretentie

J. Schroers

Annotatie bij Hof van Justitie van de Europese Unie, 06-10-2020, ECLI:EU:C:2020:791 (EHRC-2020-0253)

Feitenrelaas/wettelijk kader

1. Zowel in Frankrijk als in België werd wetgeving ingevoerd die aanbieders van elektronische-communicatiediensten ertoe verplicht om informatie te bewaren en door te geven aan bijvoorbeeld inlichtingendiensten en politie. Verschillende organisaties (inclusief La Quadrature du Net, een Franse NGO) hebben hiertegen klachten ingediend waarna de nationale rechters rechtsvragen aan het Europees Hof van Justitie (HvJ) hebben gesteld.

2. Een belangrijke vraag in de verschillende gevoegde zaken was in hoeverre artikel 15 (1) van de e-Privacy Richtlijn[1] in de weg staat van nationale wetgeving die aanbieders van elektronische-communicatiediensten een verplichting oplegt tot de algemene en ongedifferentieerde bewaring van verkeer- en locatiegegevens.

3. Artikel 15 (1) van de e-Privacy Richtlijn bepaalt dat lidstaten wettelijke maatregelen mogen treffen ter beperking van sommige bepalingen in de e-Privacy Richtlijn, '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/EG.' Het artikel vermeldt specifiek dat lidstaten voor deze redenen

wetgevingsmaatregelen mogen treffen om gegevens gedurende een beperkte periode te bewaren. Deze maatregelen moeten in overeenstemming zijn met de algemene beginselen van het Gemeenschapsrecht, en dus ook het Handvest van de grondrechten van de Europese Unie (Hv) en het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM).

4. Nadat het HvJ verduidelijkt heeft dat nationale wetgeving die aanbieders van elektronische-communicatiediensten ertoe verplicht verkeers- en locatiegegevens te bewaren onder het toepassingsgebied van de e-Privacy Richtlijn valt, verklaart het dat dataretentie een afwijking inhoudt op het verbod in artikel 5 (1) e-Privacy Richtlijn om de gegevens te bewaren en een inmenging uitmaakt op de fundamentele rechten vastgelegd in artikelen 7 en 8 Hv. Voor de interpretatie van artikel 15 (1) van de Richtlijn moeten echter ook de artikelen 3, 4 en 6 Hv in acht genomen worden, alsmede het belang van de doelstellingen van bescherming van de nationale veiligheid en bestrijding van zware criminaliteit. Tussen deze verschillende verplichtingen moet het Hof een evenwicht zien te vinden.

5. Vervolgens werd ook gevraagd of het 'recht op veiligheid' geen positieve verplichting inhoudt voor overheidsinstanties. Artikel 6 Hv, dat bepaalt dat eenieder recht op vrijheid en veiligheid van zijn persoon heeft, komt overeen met de rechten gegarandeerd in artikel 5 EVRM. Het Hof maakt duidelijk dat artikel 5 EVRM bedoeld is tegen vrijheidsbenemingen door een overheidsinstantie en aldus niet kan worden geïnterpreteerd als verplichting op de overheid om specifieke maatregelen te nemen om bepaalde strafbare feiten te voorkomen en te bestraffen.

6. Het Hof maakt in zijn beoordeling van de toepassing van artikel 15 e-Privacy Richtlijn vooral gebruik van het evenredigheidsbeginsel. Het beantwoordt de vraag door de ernst van de inmenging veroorzaakt door een dergelijke beperking te meten, en door na te gaan of het gewicht van het doel van algemeen belang dat met die beperking wordt nagestreefd evenredig is aan de ernst van de inmenging. Om aan het evenredigheidsbeginsel te voldoen, moet de wetgeving duidelijke en precieze regels bevatten die de reikwijdte en de toepassing van de maatregel in kwestie uiteenzetten en minimumwaarborgen opleggen, zodat de personen van wie de persoonsgegevens worden bewaard voldoende garanties hebben dat de gegevens effectief worden beschermd tegen het risico op misbruik. Die wetgeving moet naar nationaal recht juridisch bindend zijn en met name aangeven onder welke omstandigheden en voorwaarden een maatregel voor de verwerking van dergelijke gegevens kan worden vastgesteld, zodat de inmenging beperkt blijft tot het strikt noodzakelijke. De behoefte aan dergelijke waarborgen is des te groter waar persoonsgegevens worden onderworpen aan geautomatiseerde verwerkingen, in het bijzonder wanneer er een aanzienlijk risico bestaat op onrechtmatige toegang tot die gegevens. Die overwegingen zijn met name van toepassing

wanneer de bescherming van gevoelige persoonsgegevens op het spel staat. Wetgeving die het bewaren van persoonsgegevens verplicht, moet altijd voldoen aan objectieve criteria die een verband leggen tussen de te bewaren gegevens en het nagestreefde doel.

Uitspraak van het HvJ en Analyse

Vraag: Bewaring gegevens & artikel 15 (1) e-Privacy Richtlijn

7. Het Hof geeft in zijn uitspraak richtlijnen mee voor welke doeleinden en onder welke voorwaarden wetgeving opgesteld mag worden voor de bewaring van bepaalde soorten gegevens. De hoogste bescherming verkrijgen daarbij verkeers- en locatiegegevens. Gezien hun gevoelige aard en het feit dat de vertrouwelijkheid van de gegevens essentieel is voor het recht op eerbiediging van het privéleven, vergt een bewaring ervan bijzonder zwaarwegende doeleinden als reden. IP-adressen en burgerlijke informatie, zoals naam en adres ter identificatie van personen, worden als minder gevoelig gezien. Het belang van de doeleinden kan worden gerangschikt van hoog naar laag als volgt: 1) Het beschermen van nationale veiligheid, 2) het bestrijden van zware criminaliteit/bescherming openbare veiligheid, en 3) het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten. In dit overzicht zal de analyse van de uitspraak onderverdeeld worden volgens deze drie doeleinden.

Doel: bescherming nationale veiligheid

8. De doelstelling om de nationale veiligheid te waarborgen werd nog niet eerder door het Hof beoordeeld (maar wel in het gelijktijdig gepubliceerde *Privacy International*[2]). Het Hof legt uit dat de verantwoordelijkheid van de lidstaten voor nationale veiligheid overeenkomt met het primaire belang van de bescherming van de essentiële functies van de staat en de fundamentele belangen van de samenleving. Deze verplichting omvat het voorkomen en bestraffen van activiteiten die de fundamentele constitutionele, politieke, economische of sociale structuren van een land ernstig kunnen destabiliseren en, in het bijzonder, die direct de samenleving, de bevolking of de staat zelf bedreigen, zoals terroristische activiteiten. Het doel van de bescherming van de nationale veiligheid (gelezen in het licht van artikel 4, lid 2, VEU) gaat verder dan misdaadbestrijding en de bescherming van de openbare veiligheid. Het algemene risico van spanningen of ongeregeldheden, zelfs van ernstige aard, die de *openbare* veiligheid aantasten, vormt niet automatisch een bedreiging van de *nationale* veiligheid, die zich bij wijze van de aard en bijzondere ernst hiervan onderscheidt.

9. Onder voorbehoud van het voldoen aan de andere vereisten van artikel 52, lid 1 Hv, kan de doelstelling van het beschermen van de nationale veiligheid derhalve maatregelen rechtvaardigen die ernstigere inmenging in de grondrechten meebrengen dan degene die gerechtvaardigd zouden kunnen worden door andere doelstellingen. Een wettelijke maatregel

die de bevoegde autoriteiten de opdracht geeft aanbieders van elektronische-communicatiediensten te gelasten verkeers- en locatiegegevens van alle gebruikers van elektronische-communicatiesystemen gedurende een beperkte periode te bewaren is dus mogelijk. Desalniettemin moeten er voldoende zwaarwegende redenen zijn om aan te nemen dat de betrokken lidstaat geconfronteerd wordt met een ernstige bedreiging voor de nationale veiligheid waarvan moet worden aangetoond dat deze reëel en aanwezig of voorzienbaar is.

10. Ook al lijkt het bij een dergelijke maatregel die zonder onderscheid wordt toegepast op alle gebruikers van elektronische-communicatiesystemen op het eerste gezicht dat de opgeslagen gegevens niet noodzakelijk een verband met het nagestreefde doel hebben, toch ziet het Hof het nodige verband in het bestaan van die dreiging voor de nationale veiligheid op zichzelf. Het Hof plaatst hierbij echter een paar kanttekeningen. Zo mag, aangezien dit een redelijk verregaande inbreuk is, de opslag van de gegevens niet van nature systematisch zijn: de opslag moet in tijd beperkt zijn tot wat strikt noodzakelijk is, aan beperkingen onderhevig zijn en worden omgeven door strikte waarborgen die het mogelijk maken de persoonsgegevens van de betrokken personen doeltreffend te beschermen tegen het risico van misbruik. Verder moeten zulke maatregelen onderhevig zijn aan een effectieve controle, om zeker te zijn dat er inderdaad een dergelijke situatie bestaat en de voorwaarden en waarborgen in acht worden genomen. Deze controle kan worden uitgevoerd door een rechtbank, of door een onafhankelijk administratief orgaan waarvan de beslissing bindend is.

Geautomatiseerde analyse van verkeers- en locatiegegevens

11. Ook het gebruik van geautomatiseerde analyse is beperkt tot situaties waarin een lidstaat wordt geconfronteerd met een ernstige bedreiging van de nationale veiligheid waarvan is aangetoond dat deze reëel en aanwezig of voorzienbaar is. Verder moet een beroep op een dergelijke analyse kunnen worden onderworpen aan een effectieve toetsing. Het doel ervan is om na te gaan of er een situatie bestaat die een dergelijke maatregel rechtvaardigt en of de voorwaarden en waarborgen die moeten worden gesteld, worden nageleefd. Dit kan gedaan worden door een rechtbank, of door een onafhankelijk administratief orgaan waarvan de beslissing bindend is.

Real-time verzameling verkeers- en locatiegegevens

12. Het Hof geeft ook uitleg over het real-time verzamelen van gegevens. Bij het real-time verzamelen van gegevens worden de gegevens, bijvoorbeeld de locatie van gsm's, in real time doorgegeven en moeten door de aanbieders niet langer worden opgeslagen dan wat noodzakelijk is voor de facturering en commercialisering van hun diensten. Dit soort van real time 'tracking' is een zelfs nog ernstigere inmenging dan het achteraf toegang krijgen tot

gegevens, vooral wanneer ook nog de verkeersgegevens ingezien worden. Daarom geeft het Hof aan dat het real-time verzamelen van verkeers- en locatiegegevens dient te worden beperkt tot personen bij wie er een gegronde reden is om te vermoeden dat zij op de een of andere manier betrokken zijn bij terroristische activiteiten. Het is onderworpen aan een voorafgaand onderzoek dat wordt uitgevoerd door een rechtbank of door een onafhankelijk administratief orgaan waarvan de beslissing bindend is. Dit is om ervoor te zorgen dat een dergelijke real-time inzameling alleen wordt toegestaan binnen de grenzen van wat strikt noodzakelijk is. In gevallen van naar behoren gemotiveerde urgentie moet het onderzoek binnen korte tijd plaatsvinden. Personen van wie gegevens in real-time zijn verzameld of geanalyseerd, moeten worden geïnformeerd zodra die kennisgeving de taken waarvoor die autoriteiten verantwoordelijk zijn, niet langer in gevaar kan brengen. Die kennisgeving is noodzakelijk om de betrokken personen in staat te stellen hun rechten uit te oefenen.

Doel: bestrijding zware criminaliteit/bescherming openbare veiligheid

13. Voor het bewaren van verkeers- en locatiegegevens vormen alleen acties ter bestrijding van zware criminaliteit en bescherming van de openbare veiligheid een voldoende zwaarwegend belang. Wetgeving die een algemene en willekeurige opslag van verkeers- en locatiegegevens voorziet met het oog op de bestrijding van zware criminaliteit, overschrijdt echter de grenzen van wat strikt noodzakelijk is en kan niet als gerechtvaardigd worden beschouwd in een democratische samenleving. Daarom moet de opslag een uitzondering zijn en niet de regel, en de gegevens mogen niet systematisch en permanent bewaard worden. Wanneer de gegevens van alle personen die elektronische-communicatiediensten gebruiken bijgehouden worden, zouden ook gegevens van personen bewaard worden die helemaal geen link hebben met het doel van de bestrijding van zware criminaliteit of de bescherming van openbare veiligheid.

14. Een gerichte opslag van verkeers- en locatiegegevens met als doelstelling zware criminaliteit te bestrijden of om ernstige bedreigingen van de openbare, en natuurlijk ook nationale, veiligheid te voorkomen is wel mogelijk. De gerichtheid zou betrekking kunnen hebben op de categorieën van personen wiens gegevens worden bewaard indien er objectief bewijs is dat de verkeers- en locatiegegevens tenminste een indirect verband met de doelstelling hebben. Maar ook een geografische restrictie is mogelijk, indien bevoegde nationale autoriteiten op basis van objectieve en niet-discriminerende factoren beslissen dat er een situatie bestaat van een hoog risico op voorbereiding op of het plegen van ernstige strafbare feiten. Als voorbeeld geeft het Hof plaatsen waar zware criminaliteit veel voorkomt; plaatsen die bijzonder kwetsbaar zijn voor het plegen van ernstige strafbare feiten, zoals plaatsen of infrastructuur die regelmatig zeer veel bezoekers ontvangen; of strategische locaties, zoals luchthavens, stations of tolkantoren. Ook een gerichte opslag moet beperkt zijn tot het strikt noodzakelijke. Dit kan betrekking hebben op de categorieën van te bewaren

gegevens, de betrokken communicatiemiddelen, de betrokken personen en de gehanteerde bewaartermijn. De duur mag niet langer zijn dan wat strikt noodzakelijk is in het licht van het nagestreefde doel en de omstandigheden die dit rechtvaardigen.

15. *'Freezing' van Verkeers- en locatiegegevens* – Gegevens die zijn opgeslagen door aanbieders van elektronische-communicatiediensten voor hun normale bedrijfsvoering moeten normaal na een bepaalde tijd worden gewist. Soms kunnen situaties voorkomen waarbij het van belang is om de gegevens ook na die tijdsperiode niet te wissen voor de vervolging van ernstige strafbare feiten of daden die de nationale veiligheid schaden. Het Hof acht dit mogelijk, zowel voor het geval waarin die strafbare feiten of handelingen met nadelige gevolgen reeds zijn vastgesteld, als het geval waarin, na een objectief onderzoek van alle relevante omstandigheden, dergelijke strafbare feiten of handelingen met nadelige gevolgen redelijkerwijs kunnen worden vermoed. Voor zulke gevallen mag de lidstaat wetgeving aannemen die de mogelijkheid biedt om, door middel van een besluit van de bevoegde autoriteit dat onderworpen is aan effectieve rechterlijke toetsing, verleners van elektronische-communicatiediensten opdracht te geven verkeers- en locatiegegevens langer te bewaren gedurende een bepaalde periode.

16. De opslag van gegevens moet niet beperkt zijn tot enkel de personen die verdacht worden van het plannen of plegen van een ernstig strafbaar feit of handelingen die de nationale veiligheid kunnen schaden. Een dergelijke maatregel kan, naar keuze van de wetgever en binnen de grenzen van wat strikt noodzakelijk is, worden uitgebreid tot verkeers- en locatiegegevens met betrekking tot andere personen. Voorwaarde is dat die gegevens, op basis van objectieve en niet-discriminerende factoren, licht kunnen werpen op een dergelijk strafbaar feit of handelingen die de nationale veiligheid nadelig beïnvloeden, zoals gegevens over het slachtoffer, zijn of haar sociale of professionele kring, of zelfs specifieke geografische gebieden, zoals de plaats waar het misdrijf of de handeling die de nationale veiligheid in kwestie aantast, is gepleegd of wordt voorbereid.

17. *IP-adressen* – Het Hof acht IP-adressen van gebruikers van elektronische-communicatiesystemen in principe minder gevoelig dan andere verkeersgegevens. Omdat het echter mogelijk is een gebruiker via een IP-adres te traceren, blijft de opslag en analyse van IP-adressen nog altijd een ernstige inbreuk. Het Hof houdt er wel ook rekening mee dat wanneer er online een misdrijf gepleegd wordt, het IP-adres vaak het enige opsporingsmiddel is voor het onderzoek, en dat zonder dit opsporing onmogelijk zou zijn. De lidstaten hadden in hun opmerkingen aan het Hof vooral naar de vervolging van kinderpornografie verwezen. Het Hof oordeelt dat, ook al mogen internetgebruikers op grond van de artikelen 7 en 8 Hv verwachten dat hun identiteit in principe niet zal worden bekendgemaakt, een wetgevingsmaatregel die enkel voorziet in de algemene en willekeurige bewaring van IP-

adressen van internetverbindingen mogelijk is. Voorwaarde is dat die mogelijkheid afhankelijk is van de strikte naleving van de inhoudelijke en procedurele voorwaarden die het gebruik van die gegevens zouden moeten regelen. Alleen maatregelen ter bestrijding van zware criminaliteit, het voorkomen van ernstige bedreigingen van de openbare veiligheid en het waarborgen van de nationale veiligheid kunnen die inmenging rechtvaardigen. Bovendien mag de bewaartermijn niet langer zijn dan wat strikt noodzakelijk is in het licht van het nagestreefde doel. Ten slotte moet een dergelijke maatregel strikte voorwaarden en waarborgen bieden aangaande het gebruik van die gegevens, met name via tracking, maar ook betreffende de communicatie en de activiteiten die online door de betrokken personen worden uitgevoerd.

Doel: voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten en het waarborgen van de openbare veiligheid

18. *Burgerlijke identiteit* – Het bewaren van identiteitsgegevens van gebruikers van elektronische-communicatiemiddelen wordt niet als een ernstige inbreuk beschouwd. Het Hof merkt op dat dit vooral contactgegevens zijn zoals naam en adres, die geen gevaar vormen zolang ze niet met andere gegevens over communicatie verbonden worden. Daarom zou een wettelijke maatregel aanvaardbaar zijn wanneer deze van aanbieders van elektronische-communicatiediensten vereist dat zij, zonder een specifieke tijdslimiet op te leggen, gegevens bewaren die betrekking hebben op de burgerlijke identiteit van alle gebruikers van elektronische-communicatiesystemen met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten en het waarborgen van de openbare veiligheid en de nationale veiligheid.

Vraag: Toepassing e-Commerce Richtlijn

19. Een andere vraag had betrekking op de e-Commerce Richtlijn[3], omdat de nationale rechter wilde weten of deze het überhaupt toelaat om aanbieders van online communicatiediensten en hosting service providers te verplichten gegevens te bewaren. Gezien het feit dat artikel 1 (5) van de e-Commerce Richtlijn bepaalt dat de richtlijn niet van toepassing is op kwesties in verband met diensten van de informatiemaatschappij die onder de Richtlijn 95/46/EG en Richtlijn 97/66/EG vallen, maakt het Hof duidelijk dat deze vragen ofwel onder de e-Privacy Richtlijn, ofwel onder de Algemene Verordening Gegevensbescherming (AVG)[4] [4] vallen. Deze twee vervangen de oude Richtlijn 95/46/EG en Richtlijn 97/66/EG. Indien de nationale wetgevers gebruik maken van de mogelijkheid tot uitzonderingen in deze wetgeving (artikel 15 (1) e-Privacy Richtlijn en artikel 23 (1) AVG) moeten deze steeds weer het evenredigheidsbeginsel in acht nemen, en de uitleg hierboven met betrekking tot de vraag: Bewaring gegevens & artikel 15 (1) e-Privacy Richtlijn kan ook in

dat geval toegepast worden.

Vraag: nationaal recht handhaven

20. De Belgische rechters hadden ook nog gevraagd of, indien de nationale regeling onverenigbaar wordt bevonden met het Unierecht, een nationale rechter de gevolgen van die regeling tijdelijk zou kunnen handhaven. Het Hof laat dit echter niet toe, gezien handhaving van de effecten van nationale wetgeving, zoals die aan de orde in het hoofdgeding, zou betekenen dat de wetgeving aan aanbieders van elektronische-communicatiediensten verplichtingen zou blijven opleggen die in strijd zijn met het EU-recht en die een ernstige inbreuk maken op de grondrechten van de personen van wie de gegevens zijn bewaard.

21. Een vraag in dit verband was ook of het EU-recht het verbiedt om informatie en bewijsmateriaal dat verkregen werd door middel van het algemeen en willekeurig bewaren van verkeers- en locatiegegevens in strijd met het EU-recht, in strafrechtelijke procedures te gebruiken. Het Hof oordeelt dat het doeltreffendheidsbeginsel vereist dat nationale strafrechters zulke informatie en bewijsmateriaal negeren in de context van strafrechtelijke procedures tegen personen die ervan worden verdacht strafbare feiten te hebben begaan. Dit is echter enkel het geval indien deze personen niet in staat zijn om effectief commentaar te geven op deze informatie en het bewijsmateriaal, en ze betrekking hebben op een materie waarvan de rechters geen kennis hebben en die waarschijnlijk een overheersende invloed zullen hebben op de feitelijke bevindingen. Het Hof geeft geen aanwijzingen over hoe bijvoorbeeld het gevaar dat het onrechtmatig verkregen bewijs rechters zou kunnen beïnvloeden, zelfs als ze het buiten beschouwing moeten laten, exact aangepakt moet worden. Het zal aan het nationale recht zijn om de regels en waarborgen hieromtrent in het strafprocesrecht te bepalen. Het Hof geeft wel aan dat het aan de nationale rechtsorde van elke lidstaat is om, in overeenstemming met het beginsel van procedurele autonomie, procedureregels vast te stellen voor vorderingen die bedoeld zijn om de rechten te beschermen die particulieren ontlenen uit het EU-recht. Het verwijst daarbij naar het gelijkwaardigheidsbeginsel en het doeltreffendheidsbeginsel. Het doel om te voorkomen dat onrechtmatig verkregen informatie en bewijsmateriaal van een persoon die ervan wordt verdacht strafbare feiten te hebben gepleegd onrechtmatig benadelen, kan op nationaal niveau niet alleen worden bereikt door het gebruik van dergelijke informatie en bewijsmateriaal te verbieden, maar ook door middel van nationale regels en praktijken die de beoordeling en weging van dergelijk materiaal regelen, of door bij het bepalen van de straf rekening te houden met de vraag of dat materiaal onwettig is. Bij de keuze of bewijs wel of niet uitgesloten wordt, moet met name rekening worden gehouden met het risico op schending van het contradictoire beginsel en dus het recht op een eerlijk proces dat voortvloeit uit de toelaatbaarheid van dergelijke informatie en bewijs.

Conclusie

22. Sinds het Hof in Digital Rights Ireland[5] de Dataretentie Richtlijn[6] ongeldig verklaard heeft, zijn de nieuwe wetgevingspogingen en vragen rond dataretentie niet gestopt. In *Tele2/Sverige*[7] heeft het Hof duidelijk gemaakt dat de uitleg van artikel 15 (1) van de e-Privacy Richtlijn zich verzet tegen een nationale regeling die, ter bestrijding van criminaliteit, voorziet in algemene en ongedifferentieerde opslag van alle verkeersgegevens en locatiegegevens van alle abonnees en geregistreerde gebruikers van elektronische-communicatiemiddelen. Het gaf toen reeds aan dat een dergelijke nationale regeling onaanvaardbaar is indien daarin niet bepaald is dat toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens alleen wordt verleend ter bestrijding van zware criminaliteit, dat die toegang aan een voorafgaand toezicht door een rechtbank, of door een onafhankelijk administratief orgaan is onderworpen, en dat de betrokken gegevens op het grondgebied van de Unie moeten worden bewaard. In *Ministerio Fiscal*[8] had het Hof al geoordeeld dat de toegang van overheidsinstanties tot identificatiegegevens van de eigenaren van simkaarten die zijn geactiveerd met een gestolen mobiele telefoon geen ernstige inbreuk op hun grondrechten uitmaakt. De rechtmatige toegang is daarom niet beperkt tot het bestrijden van zware criminaliteit. In de tegelijkertijd met *La Quadrature du Net* gepubliceerde *Privacy International* uitspraak[9] heeft het Hof zich duidelijk uitgesproken tegen een algemene verplichting tot het doorgeven van verkeers- en locatiegegevens aan veiligheids- en inlichtingendiensten voor het doel van nationale veiligheid.

23. Ook in *La Quadrature du Net* blijft het Hof erbij dat de artikelen 7, 8 en 11 en artikel 52, lid 1 Hv in de weg staan aan wettelijke maatregelen die een algemene en willekeurige bewaring van verkeers- en locatiegegevens als preventieve maatregel voorzien. Met *La Quadrature Du Net* heeft het Hof nu echter duidelijker aangegeven onder welke omstandigheden het mogelijk is om bepaalde, maar niet algemene en willekeurige, gegevens te bewaren.

24. Wat deze uitspraak inhoudt voor de privacy-gemeenschap dient voorlopig te worden afgewacht. Positief, gezien de betere bescherming van privacy, is alvast dat het Hof duidelijk stelt dat het verwerken van gegevens door serviceproviders onder het gewone gegevensbeschermingsrecht valt en niet onder de uitzondering voor nationale veiligheid. Ook is het in principe voordelig, omdat de lidstaten altijd weer probeerden algemene bewaringsplichten in te voeren, dat het Hof nu duidelijk aangeeft onder welke voorwaarden het al dan niet mogelijk is om gegevens te bewaren. Toch zal enkel in de toekomst blijken hoe nauw deze richtlijnen door de lidstaten worden omgezet en of er uiteindelijk toch niet meer gegevens bewaard en gebruikt worden voor doelen die eigenlijk niet voorzien waren, omdat er nu geen duidelijk verbod maar een verbod met uitzonderingen is.

Jessica Schroers, Centre for IT & IP Law, KU Leuven

[1] 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) (*PbEU2002,* L 201).

[2] *Privacy International*, HvJ EU (GK) 6 oktober 2020, C|623/17, ECLI:EU:C:2020:790.

[3] Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt ("Richtlijn inzake elektronische handel") (*PbEU* 2000, L 178).

[4] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (*PbEU 2016,* L 119).

[5] *Digital Rights Ireland*, HvJ EU (GK) 8 april 2014, zaken C-293/12 en C-594/12, ECLI:EU:C:2014:238, « EHRC» 2014/140 m.nt. M.E. Koning.

[6] 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 (*PbEU* 2006, L 105).

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

[8] *Ministerio Fiscal*, HvJ EU (GK) 2 oktober 2018, C|207/16, ECLI:EU:C:2018:788, «EHRC» 2019/18 m.nt. B. van der Sloot.

[9] *Privacy International*, reeds aangehaald.