MASTER'S THESIS

Vertrouwelijkheid, inmenging en waarborgen: het gebruik van verkeersgegevens in strafrechtelijk onderzoek getoetst aan de artikelen 7 en 8 van het Handvest van de grondrechten van de EU

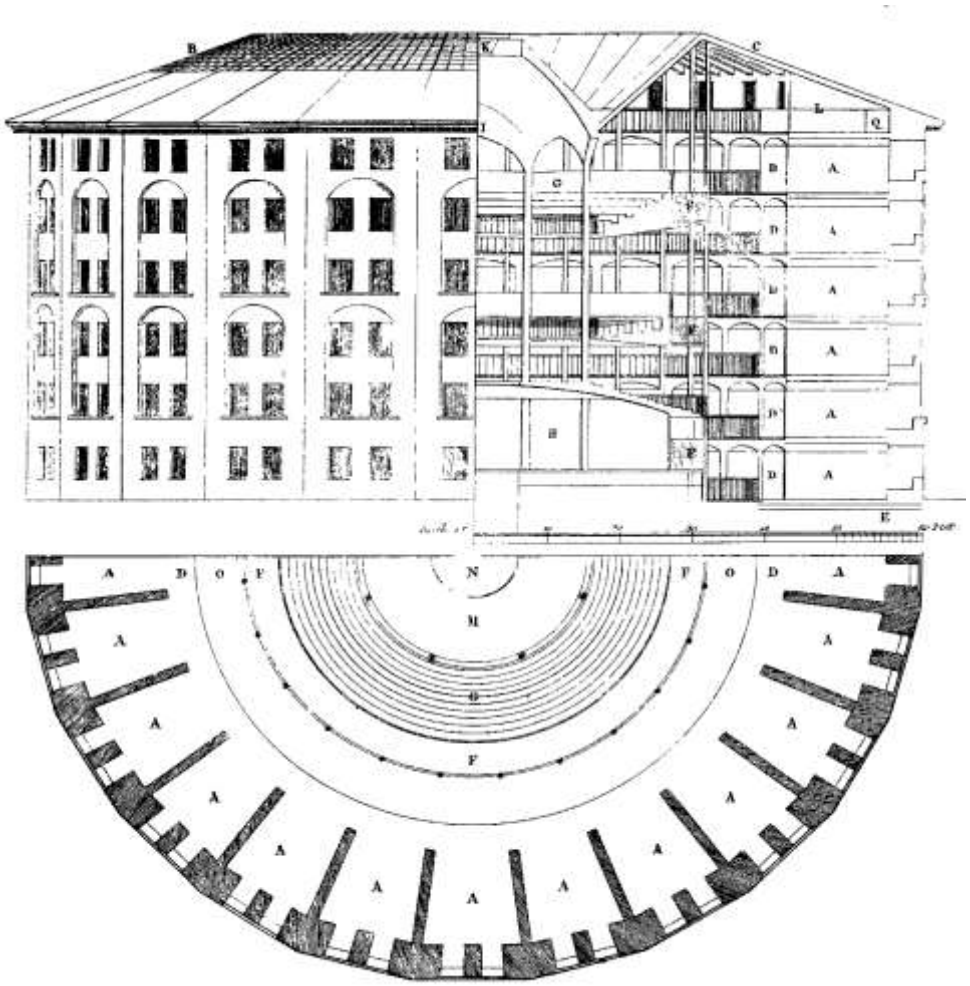
Keuker, C.P.

Award date:
2022

Awarding institution:
Department of Public Law

Link to publication

Vertrouwelijkheid, inmenging en waarborgen: het gebruik van verkeersgegevens in strafrechtelijk onderzoek getoetst aan de artikelen 7 en 8 van het Handvest van de grondrechten van de EU



Masterscriptie geschreven door C.P. Keuker, ter afronding van de studie rechtsgeleerdheid aan de Open Universiteit

Studentnummer: 851652961

Begeleider: dhr. prof. dr. mr. S. Brinkhoff

Examinator: dhr. prof. dr. mr. G.K. Sluiter

Aantal woorden: 13034

Inleverdatum: 19 januari 2022

Illustratie voorkant: ontwerp van een panopticum door Jeremy Bentham

INHOUDSOPGAVE

HOOFDSTUK 1: INLEIDING ……4

HOOFDSTUK 2: DE REGELING VOOR HET VORDEREN VAN VERKEERSGEGEVENS …...8

2.1 Verkeersgegevens: een nadere omschrijving …….....8

2.2 Grenzen aan het bewaren van verkeersgegevens ……..9

2.3 Van het "vorderen van inlichtingen omtrent het telefonieverkeer" tot de Wet bob ……10

2.3.1 Het vorderen van verkeersgegevens in het Wetboek van Strafvordering ..……11

2.3.2 De vereisten "belang van het onderzoek" en "voorlopige hechtenis toegestaan" .13

HOOFDSTUK 3: DE ARTIKELEN 7 EN 8 VAN HET EU-HANDVEST ……..…..16

3.1 Grondrechtenbescherming door de artikelen 7 en 8 van het Handvest ……16

3.2 De vereisten aan beperkingen op de grondrechten van de artikelen 7 en 8 ……17

3.2.1 Bij wet gesteld ……18

3.2.2 Een "doelstelling van algemeen belang" of "bescherming van de rechten en vrijheden van anderen" ……18

3.2.3 Evenredigheid, noodzakelijkheid en het respecteren van de essentie van het recht: de proportionaliteitstest ……19

3.3 Een nadere invulling van het proportionaliteitsvereiste ……..20

3.3.1 Niet verdergaand dan het strikt noodzakelijke om het gestelde doel te realiseren: de arresten Digital Rights Ireland en Seitlinger e.a. en Tele2 Sverige …….……21

3.3.2 Het vereiste van de verdenking van een ernstig misdrijf: La Quadrature du Net en de conclusie bij het arrest Ministerio Fiscal ……..24

3.3.3 Voorafgaande controle door een rechterlijke autoriteit bij het vorderen van verkeersgegevens: het arrest Prokuratuur ……26

HOOFDSTUK 4: HET GEBRUIK VAN VERKEERSGEGEVENS GETOETST …….30

4.1 Deel uitmakend van een formele wet …….31

4.2 Met een doelstelling van algemeen belang …….31

4.3 De proportionaliteitstest doorstaan …….32
4.3.1 Wat betreft de strikte noodzakelijkheid van de inbreuk ……32
4.3.2 Wat betreft de verdenking van een (zwaar) misdrijf ……34
4.3.3 Wat betreft de onafhankelijke rechterlijke instantie ……35

4.4 Het vorderen van verkeersgegevens in overeenstemming met het Handvest …….37
4.4.1 Opvragen van verkeersgegevens voor het onderzoek “dringend vereist” ……37
4.4.2 Een ernstige inbreuk op de rechtsorde ……..38
4.4.3 Machtiging van de rechter-commissaris vereist ……...40

HOOFDSTUK 5: CONCLUSIE …….42

GERAADPLEEGDE LITERATUUR, JURISPRUDENTIE EN STUKKEN ……..46

BIJLAGE BIJ HOOFDSTUK 2 ……...54

HOOFDSTUK 1: INLEIDING

Elektronische gegevens afkomstig van telecomaanbieders zijn voor de opsporing en het bewijzen van strafbare feiten van groot belang. In de huidige samenleving vindt immers zeer veel communicatie plaats met behulp van mobiele telefoon en computer. Niet alleen de inhoud van deze communicatie kan bij de opsporing en als bewijsmiddel een grote rol spelen, ook alle door telecomaanbieders vastgelegde gegevens die zien op zaken als tijdstip, duur, plaats en deelnemers van de communicatie - niet-inhoudelijke gegevens dus - dragen in een zeer grote mate bij aan opsporing en bewijsvoering.[1] "In een toenemend aantal gevallen vormen gebruikers- en verkeersgegevens het enige aanknopingspunt voor de opsporing", stellen Ferdinandusse, Hendriks en Laheij daarbij nog.[2] Gebruikers- en verkeersgegevens worden door telecomaanbieders voor een zekere tijd en met een bepaald doel bewaard. Telecomaanbieders hebben zich hierbij aan de ene kant te houden aan privacywaarborgen, maar dienen aan de andere kant gegevens te leveren aan justitie wanneer die van ze worden gevorderd.[3]

De niet-inhoudelijke elektronische gegevens (hierna: verkeersgegevens) dienen uiteraard bewaard te zijn, voordat ze gevorderd kunnen worden. Op grond van de artikelen 11.5 jo. 11.13 van de Telecommunicatiewet is toegestaan dat telecomaanbieders bepaalde verkeersgegevens bewaren en vervolgens - in nader omschreven gevallen - de vertrouwelijkheid van de bewaring doorbreken.[4] Wanneer deze soort gegevens gevorderd wordt ten behoeve van strafrechtelijk onderzoek moet voldaan worden aan de vereisten van de artikelen 126n, 126u of 126zh van het Wetboek van Strafvordering (hierna: Sv). De hier beschreven mogelijkheid verkeersgegevens te bewaren en te vorderen is echter geen rustig bezit: in de afgelopen 6 jaar zijn er op het gebied van de wetgeving die het bewaren van verkeersgegevens betreft en de rechtspraak over het vorderen ervan de nodige ontwikkelingen geweest.

[1] In een recent onderzoek in 10 lidstaten van de EU gaf meer dan de helft van de wetshandhavingsinstanties die bevraagd werden aan dat zij in de afgelopen twee jaar in tenminste 60% van de opsporingsonderzoeken deze zogenaamde verkeersgegevens hadden opgevraagd. Zie *Study on the retention of electronic communications non-content data* 2020, p. 17.
[2] Ferdinandusse, Hendriks & Laheij 2015, p. 3; zie ook *Rapport Commissie-Koops* 2018, p. 10-11.
[3] Recent nog overwoog de Rechtbank Rotterdam dat een telecomaanbieder verplicht kon worden zijn klantgegevens ter beschikking te stellen en dat na een weigering dit te doen een last onder dwangsom kon worden opgelegd. Het nakomen van de verplichting werd geacht "belangrijk voor de bestrijding van criminaliteit en de bescherming van de nationale veiligheid" te zijn, en er was daarbij sprake van "noodzakelijk[heid] voor de effectieve opsporing van strafbare feiten. De opsporing van strafbare feiten zou [anders] ernstig worden bemoeilijkt". Zie: Rb. Rotterdam 27 mei 2021, ECLI:NL:RBROT:2021:4427, r.o. 13.3.
[4] Hierover meer in hoofdstuk 2.

Wat betreft het *bewaren* van verkeersgegevens vormde het buitenwerking stellen van de Wet bewaarplicht telecommunicatiegegevens (hierna: Wet bewaarplicht) in maart 2015 een belangrijke ontwikkeling: de bewaring mocht vanaf dat moment niet meer ongericht plaatsvinden.[5] De "voorraad" aan bewaarde verkeersgegevens waaruit justitie vanaf toen kon putten werd daarmee een stuk kleiner. Wat betreft het *vorderen* van verkeersgegevens, oftewel het vorderen van gegevens zoals bedoeld in de artikelen 126n, 126 u en 126zh Sv, leek er geen verandering op te treden na de buitenwerkingstelling van de Wet bewaarplicht, afgezien van de kleinere hoeveelheid bewaarde verkeersgegevens waaruit gevorderd kon worden. Mits werd voldaan aan de in de artikelen 126n, 126u en 126zh Sv genoemde vereisten leek men dus gewoon te kunnen doorgaan met het gebruikmaken van de elektronische gegevens zoals bedoeld in deze artikelen.

Te beginnen met het arrest Tele2 Sverige heeft het Hof van Justitie van de Europese Unie (hierna: HvJ) echter sinds 2016 een serie arresten gewezen waarin de toelaatbaarheid van het bewaren én vorderen van verkeers- en locatiegegevens getoetst wordt aan met name de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie (hierna: Handvest). In deze arresten werd overwogen dat er sprake moet zijn van een strikte noodzakelijkheid voor het opvragen en gebruiken van verkeersgegevens voor strafrechtelijk onderzoek en dat er een toetsing door een "onafhankelijke toetsingsautoriteit" aan vooraf dient te gaan. Een officier van justitie kan niet als zo'n onafhankelijke autoriteit worden aangemerkt. Het HvJ oordeelde daarnaast dat het verlenen van toegang tot verkeersgegevens alleen toegestaan kan worden in het kader van procedures ter bestrijding van zware criminaliteit.[6]

Nederland dient de Europese grondrechten uiteraard te respecteren, ook als het om het bewaren en opvragen van persoonsgegevens ten behoeve van de opsporing en vervolging van strafbare feiten gaat. Het Nederlandse Wetboek van Strafvordering bepaalt dat de officier van justitie bevoegd is een vordering tot het vertrekken van verkeersgegevens te doen. Men kan zich afvragen of daarmee wel voldaan wordt aan het Europeesrechtelijke vereiste van de onafhankelijke toetsing. Verder doet de rechtspraak van het HvJ de vraag rijzen of er in de Nederlandse wetsartikelen die het gebruik van elektronische gegevens betreffen wel werkelijk gewaarborgd wordt dat een vordering van verkeersgegevens alleen gedaan kan worden als er sprake is van zware of ernstige criminaliteit en een strikte noodzakelijkheid voor dat vorderen.

[5] Rb. Den Haag (vzr.) 11 maart 2015, ECLI:NL:RBDHA:2015:2498, r.o. 3.10-3.12.
[6] HvJ 21 december 2016, ECLI:EU:C:2016:970 (*Tele2 Sverige*), r.o. 115-119; HvJ 6 oktober 2020, gev. zaken C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net*), r.o. 140, 146; HvJ 2 maart 2021, C-746/18, ECLI:EU:C:2021:152 (*Prokuratuur)*.

Met andere woorden: zijn de artikelen 126n, 126 u en 126zh Sv wel voldoende gespecificeerd om aan het Europees recht te voldoen? Rekening houdend met de hiervoor beschreven regelgeving en ontwikkelingen wil ik in deze scriptie dan ook trachten een antwoord te geven op de volgende vraag:

Kan het gebruik van elektronische gegevens (verkeersgegevens) zoals bedoeld in de artikelen 126n, 126u en 126zh Sv nog wel worden toegestaan in strafrechtelijk onderzoek, gelet op de artikelen 7 en 8 van het Handvest?

Om deze vraag te beantwoorden zal ik eerst in hoofdstuk 2 een overzicht geven van de bestaande mogelijkheden en bevoegdheden voor het vorderen van verkeersgegevens voor opsporings- en vervolgingsdoeleinden. Vervolgens zal ik in hoofdstuk 3 bespreken wat de artikelen 7 en 8 van het Handvest inhouden en aan welke vereisten (nationale) maatregelen dienen te voldoen indien zij de grondrechten uit het Handvest beperken. Daarna zal ik in dit hoofdstuk weergeven hoe deze vereisten aan een beperking voor wat betreft het gebruik van verkeersgegevens in de rechtspraak nader vorm hebben gekregen. De vereisten zoals die in hoofdstuk 3 worden zullen in hoofdstuk 4 als toetsingskader dienen. Met behulp van deze vereisten zal in dit hoofdstuk een toetsing plaatsvinden van de artikelen 126n, 126u en 126zh Sv aan de grondrechten uit de artikelen 7 en 8 van het Handvest. Mocht na deze toetsing de conclusie luiden dat de huidige wetgeving niet voldoende specifiek geformuleerd is om in overeenstemming te zijn met de Europese grondrechten, of dat deze anderszins veranderd zou moeten worden, dan zal ik daarna trachten aan te geven op welke wijze de relevante artikelen aangepast zouden moeten worden.

HOOFDSTUK 2: DE REGELING VOOR HET VORDEREN VAN VERKEERSGEGEVENS

In dit hoofdstuk wordt allereerst beschreven welke gegevens kunnen worden geschaard onder de noemer "verkeersgegevens", de meer gangbare benaming voor de elektronische gegevens zoals bedoeld in de artikelen 126n, 126u en 126zh Sv. Daarna wordt kort een beeld geschetst van de voorwaarden waaronder telecomaanbieders deze verkeersgegevens mogen bewaren. Dit bewaren van gegevens gaat immers vooraf aan een latere eventuele vordering van de verkeersgegevens ten behoeve van strafrechtelijk onderzoek: alleen als deze op legitieme wijze plaatsvindt kan een latere vordering legitiem zijn.[7] Vervolgens worden de artikelen uit het Wetboek van Strafvordering toegelicht die zien op de bevoegdheid tot het vorderen van deze soort digitale gegevens. Tenslotte zal er preciezer worden ingegaan op de voorwaarden die verbonden zijn aan het mogen opvragen van verkeersgegevens.

2.1 Verkeersgegevens: een nadere omschrijving

Verkeersgegevens zijn - kort gezegd - alle digitale gegevens die door telecommunicatieaanbieders (hierna zal het woord "telecomaanbieders" worden gebruikt) kunnen worden vastgelegd die géén betrekking hebben op de inhoud van de communicatie.[8] Een "positievere" omschrijving van het begrip verkeersgegevens lijkt te ontbreken in de parlementaire stukken bij de wetswijziging die leidde tot het invoeren van de artikelen 126n, 126u en 126zh.[9] In artikel 2 van het Besluit vorderen gegevens telecommunicatie, de algemene maatregel van bestuur waarnaar wordt verwezen in de artikelen, wordt een opsomming gegeven van de gegevens die als gegevens in de zin van artikel 126n, artikel 126u en artikel 126zh beschouwd moeten worden. Uit het eerste lid, tweede volzin van de drie artikelen blijkt dat dit een uitputtende lijst is. Naast naam, adres en nummers van de gebruiker worden hier onder meer de naam- en adresgegevens van de personen met wie de gebruiker verbinding heeft gehad, data en tijdstippen van de (pogingen tot) verbindingen, de locatiegegevens van de netwerkaansluitpunten en de nummers van de randapparatuur die de gebruiker heeft gebruikt genoemd.[10]

---

[7] Hierop zal nader ingegaan worden in paragraaf 3.3.2.
[8] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 80.
[9] Ook toen in 1971 de inlichtingenplicht voor verkeersgegevens naar artikel 125f werd overgeheveld, werd de bepaling nauwelijks toegelicht, zie Koops 2003, p. 70. Dit lijkt in ieder geval te maken te hebben met de wens om flexibel te kunnen inspelen op nieuwe ontwikkelingen in de communicatie, zie *Kamerstukken II* 2001/02, 28059, nr. 5, p. 17.
[10] *Stb.* 2004, 394, laatstelijk gewijzigd *Stb*. 2016, 411. Zie de bijlage voor de volledige opsomming.

In het Wetboek van Strafvordering wordt onderscheid gemaakt tussen *verkeersgegevens*, dat wil zeggen gegevens "over het communicatieverkeer met betrekking tot die gebruiker" (artikelen 126n, 126u en 126zh Sv) en *gebruikersgegevens*, zijnde gegevens "ter zake van naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van een communicatiedienst" (artikelen 126na, 126ua en 126zi Sv)".[11] Aangenomen wordt echter dat wanneer er een bevoegdheid tot het vorderen van verkeersgegevens is, deze óók de bevoegdheid tot het vorderen van gebruikersgegevens inhoudt.[12] Uit het Besluit vorderen gegevens telecommunicatie valt op te maken dat ook van een telecomaanbieder verkregen *gegevens over de locatie* van een apparaat tot de verkeersgegevens behoren.[13] Belangrijk om te onderscheiden is dat het in het geval van verkeersgegevens om de uiterlijke kenmerken van de telecommunicatie gaat en niet om de inhoud van hetgeen wordt uitgewisseld. Het opnemen van de inhoud van communicatie dient bijvoorbeeld plaats te vinden op grond van de artikelen 126m, 126t en 126zg Sv, die daartoe de bevoegdheid regelen. De op die wijze verkregen inhoudelijke communicatie valt dus buiten het juridische begrip "verkeersgegevens".

2.2 Grenzen aan het bewaren van verkeersgegevens

Wanneer door justitie op grond van één van de artikelen 126n, 126u of 126zh Sv een vordering verkeersgegevens wordt gedaan is het aan de verlener van de telecommunicatiedienst om deze gegevens te leveren. Door telecomaanbieders verworven gegevens mogen echter niet allemaal bewaard worden. De regeling voor het bewaren van verkeersgegevens is gedurende een paar jaar zeer ruim geweest ten tijde van de Europese dataretentierichtlijn[14] De dataretentierichtlijn werd in 2006 in het leven geroepen als reactie op de aanslagen in de metro van Londen en Madrid van 2004 en 2005 en verplichtte telecom- en internetaanbieders om veelsoortige gegevens over alle klanten te bewaren, bijvoorbeeld hun naam en adres, gegevens over de tijd, duur en soort communicatie en IP-adressen van de gebruikers van

[11] Koops en Smits geven het verschil hiertussen duidelijk weer: "Gebruikersgegevens zijn gegevens over iemands telecommunicatiegebruik in meer algemene zin, die niet samenhangen met een concrete communicatie; het zijn gegevens die iets zeggen over de gebruiker in plaats van over de communicatie". (Koops & Smits 2014, p. 139).
[12] Odinot e.a. 2013, p. 24; zie ook Blom, in: *T&C Strafvordering*, aant. 3 (online, bijgewerkt 1 juli 2021): "Verkeersgegevens is het bredere begrip dat gebruikersgegevens omvat".
[13] Zie ook: HR 7 april 1998, ECLI:NL:HR:1998:ZD1002: r.o. 5.4.2 en Conclusie: Onder inlichtingen 'terzake van alle verkeer' vallen ook inlichtingen over de locatie van de gebruiker van een mobiele telefoon waarmee aan het telecommunicatieverkeer wordt deelgenomen: met welke en vanuit welke telefoonaansluitingen is gebeld? Voor het opvragen van locatiegegevens via zogenaamde stille sms-jes en IMSI-catchers vormt artikel 3 van de Politiewet echter de wettelijke grondslag. Dit verloopt niet via een telecomaanbieder en valt dan ook niet onder één van de artikelen 126n, 126u of 126zh.
[14] *PbEG* 2006, L105.

internetdiensten.[15] In Nederland was deze richtlijn geïmplementeerd door de Wet bewaarplicht.[16] In 2014 werd de dataretentierichtlijn echter onverbindend verklaard door het HvJ. In het kielzog van deze uitspraak werd in 2015 ook de Nederlandse Wet bewaarplicht ontoelaatbaar geacht, omdat de wet "een inbreuk maakt[e] op de in de artikelen 7 en 8 van het Handvest gewaarborgde rechten die niet [..] beperkt [was] tot het strikt noodzakelijke".[17] Hierdoor verloor artikel 13.2a van de Telecommunicatiewet zijn werking: een algemene, ongerichte, bewaring van verkeersgegevens was vanaf toen niet meer toegestaan.

Het voor het vorderen van verkeersgegevens belangrijke artikel 11.13 van de Telecommunicatiewet bleef echter wel van kracht.[18] Het bepaalt in navolging van artikel 15 van de e-privacyrichtlijn dat telecomaanbieders de artikelen 11.5, 11.5a en 11.9, eerste lid, die de vertrouwelijke behandeling van gegevens regelen, buiten toepassing mogen laten, indien dit noodzakelijk is in het belang van de nationale veiligheid of de voorkoming, opsporing en vervolging van strafbare feiten.[19] Deze bevoegdheid om het vertrouwelijkheidsvereiste te doorbreken heeft tot gevolg dat bewaarde verkeersgegevens onder bepaalde omstandigheden door justitie gevorderd mogen worden.[20] Telecomaanbieders mogen sinds de buitenwerkingtreding van de Wet bewaarplicht dan wel niet meer ongericht alle verkeersgegevens bewaren, er mogen nog wél gegevens bewaard worden die zijn verzameld in verband met het communicatiebeheer, de facturering en marktonderzoek, voor de daartoe benodigde termijn.[21] Het is op die gegevens dat bij de huidige stand van het recht en op grond van de Telecommunicatiewet dus eventueel een beroep kan worden gedaan door justitie.

2.3 Van het "vorderen van inlichtingen omtrent het telefonieverkeer" tot de Wet bob

In het voorgaande werd beschreven op welke grondslag en met welk doel verkeersgegevens door telecomaanbieders bewaard mogen worden. Dit wil niet zeggen dat deze gegevens ook te allen tijde en allemaal, in alle gevallen wanneer dat maar nuttig lijkt voor het

[15] Zie Falot & Hijmans, *NtEr* 2017, p. 45 en de considerans bij de dataretentierichtlijn.
[16] Op grond van deze wet waren telecomaanbieders tussen 2009 en 2015 verplicht identificatie-, verkeers- en locatiegegevens van gebruikers voor een zekere duur te bewaren, zodat zij beschikbaar waren voor de opsporing en vervolging van strafbare feiten (*Stb*. 2009, 333, zie met name artikel I C van deze wet en artikel 13.2a van de Telecommunicatiewet).
[17] Rb. Den Haag (vzr.) 11 maart 2015, ECLI:NL:RBDHA:2015:2498, r.o. 3.12.
[18] *Stb*. 2004, 189 en *Kamerstukken II* 2002/03, 28851, nr. 3, p. 45.
[19] De volledige naam van de e-privacyrichtlijn luidt: richtlijn betreffende privacy en elektronische communicatie. Het betreft richtlijn 2002/58/EG, zie *PbEG* 2002, L201.
[20] *Kamerstukken II* 2002/03, 28851, nr. 3, p. 165. Artikel 13.4 van de Telecommunicatiewet bepaalt dat telecomaanbieders onverwijld aan een vordering van gegevens op grond van artikel 126n, 126u of artikel 55 van de Wet op de inlichtingen- en veiligheidsdiensten 2017 (wanneer er aanwijzingen van een terroristisch misdrijf zijn) dienen te voldoen.
[21] *Kamerstukken II* 2014/15, 33542, nr. 17, p. 3.

strafrechtelijk onderzoek, gevorderd kunnen worden. Het al dan niet mogelijk zijn van vorderen van de bewaarde verkeersgegevens zal hieronder nader worden beschouwd. Eerst wordt daarbij een overzicht gegeven van de totstandkoming van de huidige regeling in het Wetboek van Strafvordering en daarna van de vereisten die gelden voor het vorderen van verkeersgegevens.

2.3.1 Het vorderen van verkeersgegevens in het Wetboek van Strafvordering

Vóór februari 2002 was de mogelijkheid om verkeersgegevens te vorderen ten behoeve van strafrechtelijk onderzoek opgenomen in artikel 125f, dat viel onder de "Maatregelen ter gelegenheid van een schouw of een doorzoeking". Wanneer er sprake was van ontdekking op heterdaad of van een misdrijf waarvoor voorlopige hechtenis mogelijk mochten er gegevens van een "instelling van telefonie" gevorderd worden. De instelling moest op zijn beurt dan gehoor geven aan een vordering om inlichtingen, als die werd gedaan door een officier van justitie, of, tijdens het gerechtelijk vooronderzoek, door de rechter-commissaris.[22]

In 2000 trad de Wet bijzondere opsporingsbevoegdheden (hierna: Wet bob) in werking.[23] Een zeer belangrijke reden voor de invoering daarvan was gelegen in het feit dat er een grote behoefte was aan meer waarborgen ten aanzien van de bijzondere opsporingsbevoegdheden. De wetgever wilde voorkomen dat een debacle als de IRT-affaire, waarin het opsporingsteam drugs "doorgelaten had" om de grote drugscriminelen te kunnen aanpakken, zich nogmaals zou kunnen voordoen en besloot politie en justitie minder ruimte te geven en striktere normen in de wet op te nemen.[24] De grootste wijziging met betrekking tot het opvragen van verkeersgegevens betrof het schrappen van de mogelijkheid dat verkeersgegevens door de rechter-commissaris gevorderd werden.[25] Rechterlijke controle op het vorderen van gegevens zou na afronding van het opsporingsonderzoek, ter terechtzitting, gaan plaatsvinden.[26] Daarnaast werd als nieuw vereiste opgenomen dat de vordering in het belang van het onderzoek moet zijn.

Met de Wet bob kregen de bijzondere opsporingsmethoden een eigen plaats in het Wetboek van Strafvordering: in titel IV A voor de opsporing na een gepleegd misdrijf en in titel V voor het onderzoek op basis van een vermoeden dat er in georganiseerd verband ernstige misdrijven worden beraamd of gepleegd. De bevoegdheid tot het opvragen van

[22] *Stb*. 1971, 180.
[23] *Stb*. 1999, 245 (Voluit: Wet tot wijziging van het Wetboek van Strafvordering in verband met de regeling van enige bijzondere bevoegdheden tot opsporing en wijziging van enige andere bepalingen).
[24] Buiten, van, *DD* 2016, p. 131-132.
[25] Dit laatste in lijn met de afschaffing van het gerechtelijk vooronderzoek door de Wet versterking positie rechter-commissaris, zie *Stb.* 2011, 600.
[26] Buiten, van, *DD* 2016, p. 141.

verkeersgegevens werd "verplaatst" naar de artikelen 126n en 126u, de inhoud veranderde in de jaren daarna nog enigszins.[27] Per 1 februari 2007 werd titel VB, "Bijzondere bevoegdheden tot opsporing van terroristische misdrijven", ingevoegd.[28] Hiermee ging ook het aan de artikelen 126n en 126u complementaire artikel 126zh, dat relevant is als er aanwijzingen zijn van een terroristisch misdrijf, deel uitmaken van het Wetboek van Strafvordering.

Artikel 126n, te vinden in de zevende afdeling van Titel IV A, die het "Onderzoek van communicatie door middel van geautomatiseerde werken" betreft, biedt de officier van justitie de bevoegdheid een vordering te doen, gericht aan een telecomaanbieder, om gegevens te verstrekken over een gebruiker van een communicatiedienst en het communicatieverkeer met betrekking tot die gebruiker.[29] De vordering mag slechts betrekking hebben op de gegevens die bij algemene maatregel van bestuur zijn aangewezen en kan zowel gegevens betreffen die ten tijde van de vordering zijn verwerkt (historische gegevens) als gegevens die na het tijdstip van de vordering worden verwerkt (toekomstige gegevens).[30] In artikel 126u, te vinden onder Titel V van het Eerste Boek, wordt de mogelijkheid gecreëerd om in het belang van het onderzoek gegevens van een gebruiker van een communicatiedienst te vorderen wanneer er misdrijven als omschreven in artikel 67, eerste lid, worden beraamd of gepleegd in georganiseerd verband.[31] Deze misdrijven dienen door hun aard, of door de samenhang met andere misdrijven die in dat georganiseerd verband worden beraamd of gepleegd, een ernstige inbreuk op de rechtsorde op te leveren.[32]Artikel 126zh tenslotte bepaalt dat de officier van justitie in het geval van aanwijzingen van een terroristisch misdrijf een vordering kan doen gegevens te verstrekken over een gebruiker van een communicatiedienst in de zin van artikel 126la en het communicatieverkeer met betrekking tot die gebruiker.[33]

---

[27] Belangrijkste "modernisering" van de tekst: "[…] geeft ieder die werkzaam is bij een instelling van telefonie ter zake van alle verkeer hetwelk door tussenkomst van de instelling is geschied [..] de door deze gewenste inlichtingen" werd "[…] inlichtingen te verstrekken terzake van alle verkeer dat over een openbaar telecommunicatienetwerk, dan wel met gebruikmaking van openbare telecommunicatiediensten, heeft plaatsgevonden".

[28] *Stb.* 2006, 580.

[29] Onder de noemer "communicatiedienst" vallen zowel openbare als besloten communicatienetwerken, zoals een bedrijfsnetwerk of een schoolforum (Lassche 2021, versie 3.5, p. 33).

[30] De leden twee tot en met zes van artikel 126n en 126 u (ook geldend voor 126zh) bevatten nadere - meer praktische - vereisten aan de vordering. Zo dient de vordering bijvoorbeeld te worden gericht aan de aanbieder van een communicatiedienst. (Het is niet toegestaan de gegevens bij de verdachte zelf te vorderen, zoals blijkt uit de artikelen 126nd, 126nf, 126ud, 126uf, 126zl en 126zn.) Ook is het verschoningsrecht van toepassing..

[31] Overigens wordt in artikel 126u voor de omschrijving van een "gebruiker van een communicatiedienst" nog verwezen naar het vervallen artikel 126la. Per 1 maart 2019 zijn voor artikel 126la echter de artikelen 138g en 138h in de plaats gekomen, ingevoegd in de Betekenissentitel bij Boek 1. De verplaatsing werd noodzakelijk door de inwerkingtreding van de Wet Computercriminaliteit III; de tekst is, hoewel nu verdeeld over 2 artikelen, gelijk gebleven.

[32] Dit laatste volgt uit artikel 126o Sv, waarnaar verwezen wordt in 126u.

[33] Ook hier geldt dat nog wordt verwezen naar artikel 126la.

2.3.2 De vereisten “belang van het onderzoek” en “voorlopige hechtenis toegestaan”

In de drie artikelen die het vorderen van verkeersgegevens betreffen spelen twee procedurele vereisten een belangrijke rol. Ten eerste mag de bevoegdheid tot het vorderen van gegevens, blijkens het eerste lid van artikel 126n en de twee complementaire artikelen 126u en 126zh, door de officier van justitie alleen worden uitgeoefend “in het belang van het onderzoek”. Dit houdt in dat bij het vorderen van gegevens moet worden afgewogen of de bevoegdheid moet worden toegepast in het concrete onderzoek[34]. Vorderen is alleen toegestaan wanneer dit bijdraagt aan de opsporing van het omschreven misdrijf of de opsporing van in georganiseerd verband beraamde gepleegde misdrijven.[35]. Het is voor het vorderen van verkeersgegevens niet vereist dat het om de gegevens van een verdachte gaat: ook gegevens van niet-verdachte personen kunnen gevorderd worden wanneer dit in het belang van het onderzoek is.[36]

Ten tweede is in de artikelen 126n en 126u daarnaast de voorwaarde opgenomen dat voorlopige hechtenis toegestaan moet zijn voor het misdrijf waarvoor de verkeersgegevens opgevraagd werden. In de jaren ’90 van de vorige eeuw was er nog sprake van dat verkeersgegevens wellicht bij elk soort misdrijf opgevraagd zouden mogen worden, omdat het door sommigen toentertijd beschouwd werd als een veel lichtere inbreuk op de persoonlijke levenssfeer dan het aftappen van telecommunicatie.[37] De Registratiekamer merkte hier echter destijds al over op dat dit inging “tegen de geldende normen voor een dergelijke inbreuk op de privacy”.[38] Uit de memorie van toelichting bij het Wetsvoorstel bijzondere opsporingsbevoegdheden valt op te maken dat er onderscheid gemaakt wordt tussen meer ingrijpende en zeer ingrijpende bevoegdheden. Voor de eerste soort is een verdenking van een misdrijf als omschreven in artikel 67, eerste lid, vereist, voor de tweede een verdenking van een misdrijf als omschreven in artikel 67, eerste lid, dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert.[39]

---

[34] *Kamerstukken II* 2001/02, 28059, nr. 5, p. 22-23.
[35] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 7.
[36] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 23; *Kamerstukken II* 2001/02, 28059, nr. 3, par. 4.
[37] *Kamerstukken II* 1992/93, 23047, nr. 3, p. 13. Deze opvatting speelde ten tijde van de “Wijziging van het Wetboek van Strafvordering in verband met de regeling van het opnemen van gesprekken met een technisch hulpmiddel”, een in 1997 ingetrokken wetsvoorstel, dat op enkele gebieden als voorloper diende van het latere Wetsvoorstel bijzondere opsporingsbevoegdheden.
[38] Zie het Advies bijzondere opsporingsbevoegdheden uit 1997 van de Registratiekamer (de voorloper van respectievelijk het College bescherming persoonsgegevens en de Autoriteit Persoonsgegevens), geciteerd in Bokhorst, Kogel, de & Meij, van der 2002, p. 64.
[39] Vereist bijvoorbeeld voor het opnemen van telecommunicatie (126m Sv) en het vorderen van extra beschermde gegevens “bij eenieder van wie hij vermoed heeft er toegang toe te hebben” (126nf Sv).

Het vorderen van verkeersgegevens is ondergebracht onder de eerste soort.[40] Een "verdenking van een misdrijf als omschreven om artikel 67, eerste lid" is daarmee de ondergrens geworden voor het vorderen van verkeersgegevens.

Samenvattend volgt uit het bovenstaande dat het naar Nederlandse wetgeving toegestaan is dat een deel van door telecomaanbieders verzamelde digitale gegevens (die géén betrekking hebben op de inhoud van de communicatie) voor een beperkte duur bewaard wordt. Een officier van justitie mag deze gegevens op grond van de artikelen 126n, 126u en 126zh Sv vorderen, ondanks de "garantie van vertrouwelijkheid" die er in beginsel op rust. Telecomaanbieders mogen de vertrouwelijkheid van de door hen verzamelde gegevens namelijk doorbreken op grond van de Telecommunicatiewet als dit noodzakelijk is in het belang van de voorkoming, opsporing en vervolging van strafbare feiten. Voor een vordering gedaan wordt dient wel aan een aantal vereisten voldaan te zijn: de vordering dient het belang van het onderzoek te dienen en voor het betreffende misdrijf moet voorlopige hechtenis zijn toegestaan.

Zoals hiervoor al uit de buitenwerkingstelling van de Wet bewaarplicht bleek, rust op de EU-lidstaten de plicht om de grondrechten te eerbiedigen wanneer zij gemeenschapsregelingen uitvoeren.[41] Daarnaast beschouwt het HvJ de lidstaten óók als uitvoerders van EU-regelgeving wanneer zij verkeersgegevens gebruiken voor hun nationale strafvordering. Nationale regelingen betreffende de bewaring van en toegang tot verkeersgegevens vielen naar het oordeel van het HvJ al veelvuldig onder de werkingssfeer van het Unierecht: ware dit niet zo dan zou aan de e-privacyrichtlijn het "nuttig effect" worden ontnomen.[42] Om deze redenen dient de behandeling van verkeersgegevens dus, óók wanneer het nationale strafvorderlijke aangelegenheden betreft, door de "keuringszeef" van de Europese

[40] *Kamerstukken II* 1996/97, 25403, nr. 3, p. 23.

[41] Deze gebondenheid aan de fundamentele rechten in het geval dat nationale overheden maatregelen uitvoeren wordt ook wel de Wachauf-gebondenheid genoemd, vernoemd naar het eerste arrest waarin het HvJ stelde dat "de eisen van de bescherming van de fundamentele rechten in de communautaire rechtsorde de lidstaten ook bij de uitvoering van gemeenschapsregelingen binden" (HvJ EG 13 juli 1989, C 5/88, ECLI:EU:C:1989:321 (*Wachauf*), r.o. 19) . Zie ook Mol, de, Pahladsingh & Heijningen, van, *SEW* 2012, p. 224.

[42] HvJ 21 december 2016, ECLI:EU:C:2016:970 (*Tele2 Sverige*), r.o. 73; HvJ 6 oktober 2020, C-623/17, ECLI:EU:C:2020:790 (*Privacy International*), r.o. 44; HvJ 6 oktober 2020, gev. zaken C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net*), r.o. 99; HvJ 2 maart 2021, C-746/18, ECLI:EU:C:2021:152 (*Prokuratuur*), r.o. 42-44. In de zaken Privacy International en La Quadrature du Net werd overigens door partijen aangevoerd dat handelingen die te maken hebben met openbare veiligheid, strafrechtelijke vervolging, enz. niét binnen het toepassingsbereik van de e-privacyrichtlijn behoren. Hier ging het HvJ niet in mee (Oerlemans & Hagens, *JBP* 2021/1, p. 31).

grondrechtenbescherming te gaan, in dit geval die van de artikelen 7 en 8 van het Handvest.[43] Bij het vorderen van verkeersgegevens moet daarom ook worden voldaan aan de gronden voor en vereisten aan het begrenzen van de rechten uit deze artikelen. De artikelen 7 en 8 en deze gronden en vereisten zullen dan ook het onderwerp vormen van het volgende hoofdstuk.

[43] Dit komt overeen met het standpunt van auteurs als Oerlemans, Hagens & Royer, in *Computerrecht* 2021, p. 155: "..wanneer er sprake is van een verwerking van gegevens in de zin van de e-Privacyrichtlijn [mag] de achterliggende bescherming van de Europese regelgeving niet uitgehold worden" en Møller Pedersen, Udsen & Sandfeld Jakobsen, in *International Data Privacy Law* 2018, p. 173.

HOOFDSTUK 3: DE ARTIKELEN 7 EN 8 VAN HET EU-HANDVEST

Reeksen gegevens die het communicatieverkeer van een gebruiker van een communicatiedienst betreffen kunnen veel prijsgeven over de persoonlijke levenssfeer van een gebruiker, waardoor het bewaren en vorderen ervan een inbreuk op de grondrechten van het Handvest met zich meebrengt. Toch is nationale regelgeving toegestaan die bepaalt dat deze inbreuk op de vertrouwelijkheid in bepaalde gevallen gemaakt mag worden, zoals wanneer dat nodig is voor de bestrijding, opsporing en vervolging van strafbare feiten.[44] Het EU-recht blijft daarbij echter bescherming bieden tegen ongeoorloofde inbreuken op de grondrechten: als er sprake is van het ten uitvoer brengen van Unierecht kan op grond van artikel 51 immers de bescherming van het Handvest tegen zowel de instellingen, organen en instanties van de Unie als tegen de lidstaten worden ingeroepen.[45]

In dit hoofdstuk zal eerst de inhoud en de reikwijdte van de bescherming van de grondrechten van de artikelen 7 (recht op eerbiediging privéleven) en artikel 8 (recht op bescherming van persoonsgegevens) van het Handvest worden besproken. Hierna komen de mogelijkheden van een beperking op die grondrechten op grond van artikel 52, eerste lid van het Handvest aan de orde. De rechtspraak op Europees en nationaal niveau maakt daarnaast ook duidelijk welke waarborgen er bestaan wanneer verkeersgegevens worden gebruikt. Er zal daarom ook een nader overzicht worden gegeven van de wijze waarop deze materie nader is ingevuld door Europese en nationale rechtspraak.

3.1 Grondrechtenbescherming door de artikelen 7 en 8 van het Handvest

Artikel 7 (Eerbiediging van het privéleven en het familie- en gezinsleven) van het Handvest bepaalt dat "eenieder recht [heeft] op eerbiediging van zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn communicatie". In een situatie waarin verkeersgegevens worden bewaard of opgevraagd gaat het met name om de eerbiediging van privéleven en communicatie. De precieze betekenis van de vier begrippen privéleven, familie- en gezinsleven, woning en communicatie is lastig vast te stellen en lijkt ook vaak niet van belang, omdat in de praktijk het HvJ het gehele artikel 7 (of 8) van het Handvest als toepasselijk beschouwt.[46]

In het eerste lid van artikel 8 (Bescherming van persoonsgegevens) wordt bepaald dat "eenieder recht [heeft] op bescherming van de hem betreffende persoonsgegevens". In het

[44] Dit op grond van artikel 15, eerste lid van de in hoofdstuk 1 besproken e-privacyrichtlijn.
[45] Mol, de, Pahladsingh & Heijningen, van, SEW 2012, p. 223.
[46] Peers e.a. 2014, p. 156.

tweede en derde lid wordt daarnaast gesteld dat de gegevens eerlijk moeten worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Ook heeft elke EU-burger recht op toegang tot de verzamelde gegevens die hem aangaan en op rectificatie daarvan en dient een onafhankelijke autoriteit toe te zien op de naleving van de regels van artikel 8. Met artikel 8 Handvest werd een grondrecht in het leven geroepen dat bescherming biedt tegen het "onbeschermd" gebruik van persoonsgegevens. Artikel 8 maakt het via het tweede lid namelijk wél mogelijk dat persoonsgegevens verwerkt worden na toestemming van de betrokkene of als er een gerechtvaardigde grondslag in de wet is voor "dataverwerking zonder toestemming".

De artikelen 7 en 8 van het Handvest zijn op vele vlakken aan elkaar gerelateerd.[47] Aan de ene kant zou men kunnen denken dat het recht van artikel 8 Handvest op bescherming van persoonsgegevens enigszins overbodig is, nu er al een grondrecht bestaat dat zaken als privéleven en communicatie beschermt. Aan de andere kant lijkt het apart opnemen van een recht op bescherming van persoonsgegevens in het Handvest toch ook logisch. Dit gezien de specifieke geschiedenis en inhoud van dit recht: de voorwaarden en vereisten van artikel 8 Handvest maakten al vóór de inwerkingtreding van het Handvest in 2009 deel uit van het EU-recht, omdat de bescherming van persoonsgegevens toen al werd erkend als een algemeen beginsel van EU-recht.[48] Toch lijkt uit de rechtspraak van het HvJ naar voren te komen dat er in zaken die het privéleven en gegevensbescherming betreffen weinig tot geen aandacht is voor die specifieke status.[49] In de rechtspraak wordt geen onderscheid gemaakt tussen de artikelen; zij werden in het verleden steeds beide in een adem genoemd (of beide helemaal niet vermeld).[50]

3.2 De vereisten aan beperkingen op de grondrechten van de artikelen 7 en 8

Een inbreuk op grondrechten, in dit geval dus die uit de artikelen 7 en 8 van het Handvest, kan alleen legitiem zijn als aan de vereisten van artikel 52, eerste lid van het Handvest wordt voldaan. Deze bepaling geeft een algemene beperkingsregeling voor de grondrechten uit het Handvest, waaruit drie vereisten kunnen worden onderscheiden waaraan een beperking van

[47] Zij moeten geïnterpreteerd te worden in het licht van hun gezamenlijke "basis": artikel 8 van het EVRM. Dit valt op te maken uit de Toelichtingen bij de artikelen 7 en 8 bij het Handvest van de Grondrechten: *PbEU* 2007, C303/20. Bij toetsing van het gegevensbeschermingsrecht door het HvJ raakt het EVRM tegenwoordig wel steeds meer op de achtergrond, zie Koning 2015, p. 359.

[48] Koning 2015, p. 353.

[49] Aan artikel 8 liggen onder meer het Gegevensbeschermingsverdrag van de Raad van Europa uit 1981, artikel 16 van het VWEU en de gegevensbeschermingsrichtlijn uit 1995 ten grondslag, waardoor het artikel van een andere aard lijkt te zijn dan artikel 7, zie Wissels & Pahladsingh 2020.

[50] Molder, te, *DD* 2021/66, p. 856; Koning 2015, p. 362, 364. Koning spreekt van "een tandemaanpak waarbij artikel 7 en 8 Hv worden gecombineerd tot 'het recht op bescherming van de persoonlijke levenssfeer bij de verwerking van persoonsgegevens'", een recht dat ook gezamenlijk wordt getoetst.

een recht (of vrijheid) getoetst dient te worden. Ten eerste is dit het vereiste van het "gesteld zijn bij wet", ten tweede het vereiste dat de beperking in een bepaalde rechtvaardigings-categorie valt en ten derde het vereiste dat de beperking inhoudelijk gezien evenredig en noodzakelijk is en de essentie van het recht eerbiedigt. Deze vereisten zullen hieronder worden toegelicht.

3.2.1 Bij wet gesteld

Sinds het Handvest bij de inwerkingtreding van het Verdrag van Lissabon bindend werd is er in de praktijk door het HvJ niet vaak specifiek naar dit eerste vereiste, dat van de wettelijke grondslag, verwezen. De opvatting van wat er onder wettelijke regelingen verstaan kan worden lijkt in de context van het Handvest volgens Peers net zo breed te mogen worden opgevat als het begrip "bij de wet voorzien" in het EVRM.[51] Belangrijk hierbij, zo blijkt uit rechtspraak van het EHRM, is dat de wettelijke regeling in ieder geval passend (voldoende precies) en voorzienbaar is.[52] Koning signaleert dat voor het HvJ ook eenvoudigweg het bestaan van een verordening al voldoende is en dat het niet aan kwalitatieve vereisten toetst.[53]

3.2.2 Een "doelstelling van algemeen belang" of "bescherming van de rechten en vrijheden van anderen"

Uit het tweede vereiste volgt dat er getoetst dient te worden of een beperking wel in een door de Europese Unie erkende "doelstelling van algemeen belang" of de categorie "bescherming van de rechten en vrijheden van anderen" valt.[54] Met betrekking tot de eerste categorie wordt in de Toelichting bij het Handvest uiteengezet wat er onder meer onder verstaan kan worden: "… de in artikel 3 van het Verdrag betreffende de Europese Unie genoemde doelen … [en] specifieke bepalingen van de Verdragen, zoals artikel 4, lid 1, van het Verdrag betreffende de Europese Unie, artikel 35, lid 3, van het Verdrag betreffende de werking van de Europese Unie en de artikelen 36 en 346 van dat Verdrag".[55] Uit de keuze van het woord "zoals"

[51] Peers e.a. 2014, p. 1470-1471.
[52] Peers 2014, p. 235. Uit jurisprudentie van het EHRM blijkt dat er wat betreft dit vereiste concreet op drie punten wordt getoetst: was er sprake van bekendmaking van de inmenging, is voldoende aandacht besteed aan het beperkt houden van de gevolgen van de maatregel en was de voorzienbaarheid van de maatregel voldoende als die wordt afgezet tegen de zwaarte van de inmenging? (Koning 2015, p. 365).
[53] Koning 2015, p. 365.
[54] In de Toelichting bij artikel 52 Handvest wordt opgemerkt dat rechten aan beperkingen kunnen worden onderworpen "voor zover die beperkingen werkelijk beantwoorden aan de doeleinden van algemeen belang die de Gemeenschap nastreeft en, het nagestreefde doel in aanmerking genomen, niet zijn te beschouwen als een onevenredige en onduldbare ingreep, waardoor de gewaarborgde rechten in hun kern worden aangetast", *PbEU* 2007, C303/17.
[55] In lid 1 van artikel 3 van het VEU wordt als doel genoemd: de vrede, de waarden van de Unie en het welzijn van de volkeren van de EU bevorderen. In de volgende leden volgen meer concreet onder andere de

valt op de maken dat dit geen restrictieve opsomming is.[56] In de tweede categorie "bescherming van de rechten en vrijheden van anderen" gaat het om de rechten uit het Handvest en de vrijheden uit de EU-wetgeving die de vrije markt betreffen.[57] Deze tweede rechtvaardigingsgrond, "bescherming van de rechten en vrijheden van anderen," lijkt hier niet van toepassing te zijn, omdat de voorkoming en bestrijding van misdrijven niet onder de "vrije markt-rechten" valt.

3.2.3 Evenredigheid, noodzakelijkheid en het respecteren van de essentie van het recht: de proportionaliteitstest

Als aan de twee hierboven vermelde vereisten voldaan is, leidt het derde vereiste van artikel 52, eerste lid - dat van evenredigheid, noodzakelijkheid en het respecteren van de essentie van het grondrecht - ertoe dat de vaak zo genoemde "proportionaliteitstest" uitgevoerd moet worden, waarbij de afweging plaatsvindt van de grondrechten tegen de belangen die een eventuele inbreuk daarop rechtvaardigen. Dit wordt gezien als het belangrijkste toetsingsmechanisme.[58] In de praktijk komen de begrippen evenredigheid en noodzakelijkheid vaak in combinaties voor en gebruikt ook het HvJ ze in uitspraken niet los van elkaar.[59] "Passend zijn om het doel te bereiken" en "noodzakelijk" kunnen gezien worden als de twee onderdelen van een bredere evenredigheidstest, aldus rechter bij het HvJ Von Danwitz.[60] En: evenredigheid is "wat noodzakelijk is om de doelstellingen van de Verdragen te realiseren".[61] De ook in artikel 52 genoemde "essentie van een grondrecht" wordt geschaad wanneer afbreuk wordt gedaan aan het grondrecht door het bijvoorbeeld af te schaffen of het uitoefenen ervan

totstandbrenging van een interne markt, de bescherming van het milieu en de rechten van het kind, het bieden van een ruimte van vrijheid, veiligheid en recht en het waarborgen van het vrije verkeer van personen in combinatie met passende maatregelen met betrekking tot (onder meer) voorkoming en bestrijding van criminaliteit.

[56] Overigens heeft het VWEU geen artikel 35, derde lid en zou in de plaats van artikel 4, eerste lid VEU heel goed artikel 4, tweede lid bedoeld kunnen zijn, zie Peers e.a. 2014, p. 1475.

[57] Het EVRM kent deze twee rechtvaardigingsgronden voor een beperking ook. Een bekend voorbeeld van een door het EHRM legitiem geachte beperking "ter bescherming van de rechten en vrijheden van anderen" betrof een beperking op de vrijheid van meningsuiting. In 2012 oordeelde het EHRM dat een inbreuk op de vrijheid van meningsuiting toelaatbaar was ter bescherming van het recht op eerbiediging van het privéleven. Zie EHRM 7 februari 2012, ECLI:CE:ECHR:2012:0207JUD004066008 (*Von Hannover/Duitsland II*).

[58] Peers e.a. 2014, p. 1476.

[59] Peers e.a. 2014, p. 1581; Kumm, *International Journal of Constitutional Law* 2004, p. 579.

[60] Von Danwitz 2012, p. 371.

[61] Von Danwitz 2012, p. 370. Diverse auteurs signaleren daarnaast dat het HvJ niet alleen de hierboven beschreven proportionaliteitstests, maar ook een evenredigheidstest "stricto sensu" uitvoert, een belangenafweging waarbij onderzocht wordt of een door een beperking veroorzaakte inbreuk in verhouding is met het gewicht en de urgentie van het te bereiken doel. Zie Gerards, European Law Journal 2011, p. 89; Von Danwitz 2012, p. 372; Brkan & Imamović 2020.

onmogelijk te maken. Een oordeel van het HvJ dat hiervan sprake was is nog zeer weinig voorgekomen.[62]

3.3 Een nadere invulling van het proportionaliteitsvereiste

In het afgelopen decennium is in een aantal arresten die de grondrechten uit de artikelen 7 en 8 Handvest betroffen een nadere invulling gegeven aan het proportionaliteitsvereiste in relatie tot het gebruik van verkeersgegevens voor strafvorderlijke doeleinden. Zoals al aan het begin van dit hoofdstuk werd aangegeven zal daarom vóórdat de toelaatbaarheid van het gebruik van verkeersgegevens getoetst wordt aan het Handvest nader worden geanalyseerd hoe dit vereiste door het HvJ, en in de nationale rechtspraak, is uitgelegd.

Opvallend in de arresten over verkeersgegevens is ten eerste dat het HvJ het gebruik ervan als het ware opdeelt in enerzijds het bewaren en anderzijds het verkrijgen van toegang: deze handelingen vormen twee verschillende inbreuken op het privéleven.[63] Het HvJ lijkt het bewaren van verkeersgegevens als een even grote inbreuk als het vorderen ervan te beschouwen vanwege het zogenaamde "chilling effect" dat er van het eerste uitgaat: als gebruikers van telecommunicatiediensten weten dat hun gegevens bewaard worden om later eventueel voor opsporingsdoeleinden gebruikt te worden kunnen zij zich beknot voelen in hun privacy en hun handelen erdoor laten beïnvloeden. Reden voor het HvJ om het bewaren van verkeersgegevens als een op zichzelf staande (ernstige) inbreuk op het privéleven te beschouwen.[64] Ten tweede valt in de jurisprudentie die het gebruik van verkeersgegevens betreft een drietal belangrijke punten op, waaraan het HvJ toetst of aan het proportionaliteitsvereiste voldaan is.[65] Deze houden in dat de beperking op de grondrechten van artikel 7 en 8 Handvest noodzakelijk moet zijn voor het te realiseren doel, dat er sprake moet zijn van een ernstig misdrijf, en dat een onafhankelijk autoriteit voorafgaand toestemming moet geven voor het gebruik. Deze vereisten zullen hieronder worden besproken aan de hand van de relevante uitspraken.

---

[62] Brkan noemt de zaak Schrems als voorbeeld: HvJ 6 oktober 2015, C-362/14, ECLI:EU:C:2015:650 (*Schrems*). Zie Brkan, *German Law Journal* 2019, p. 868 en 882-883. Voor een verdere beschouwing over het begrip "essentie van het recht" als middel voor een zelfstandige toets bij een vermeende inbreuk op de grondrechten van het Handvest zie Brkan, *German Law Journal* 2019, p. 864-883. In het arrest Digital Rights voerde het HvJ deze toets overigens uit en concludeerde dat de dataretentierichtlijn de essentie van de grondrechten van artikel 7 en 8 niet teniet deed, omdat deze richtlijn de opslag van gegevens over telefoonverkeer betrof en niet de inhoud (zie HvJ 8 april 2014, gev. zaken C-293/12 en C-594/12, ECLI:EU:C:2014:238 (*Digital Rights Ireland en Seitlinger e.a.*), r.o. 39, 40.

[63] Zie onder meer HvJ 8 april 2014, gev. zaken C-293/12 en C-594/12, ECLI:EU:C:2014:238 (*Digital Rights Ireland en Seitlinger e.a.*), r.o. 34,35.

[64] Molder, te, *DD* 2021/66, p. 864; HvJ 8 april 2014, gev. zaken C-293/12 en C-594/12, ECLI:EU:C:2014:238 *(Digital Rights Ireland en Seitlinger e.a.*), r.o. 37.

[65] Zie ook hierop lijkende onderverdelingen in Oerlemans, Hagens & Royer, *Computerrecht* 2021 (in de paragrafen 3 en 4) en Toor, van, ehrcupdates 2021(in de paragrafen 3,4 en 5).

3.3.1 Niet verdergaand dan het strikt noodzakelijke om het gestelde doel te realiseren: de arresten Digital Rights Ireland en Seitlinger e.a. en Tele2 Sverige

Het arrest Digital Rights Ireland en Seitlinger e.a., dat het HvJ in 2014 wees, was de eerste verregaande uitspraak met betrekking tot het *bewaren* van verkeersgegevens. Het HvJ oordeelt in dit arrest dat het bewaren van gegevens ten behoeve van de bestrijding van criminaliteit op zichzelf aanvaardbaar is, omdat de openbare veiligheid erdoor beschermd wordt. Ook is het bewaren van gegevens - gelet op het steeds groter wordende belang van elektronische communicatiemiddelen - in beginsel een geschikt middel voor het realiseren van dat doel en raakt een algemene bewaarplicht niet aan de wezenlijke inhoud van het recht op eerbiediging van het privéleven.[66] De gegevensbewaring die plaatsvond op grond van de dataretentierichtlijn wordt echter beschouwd als een ernstige inbreuk op de grondrechten, omdat uit de gegevens "zeer precieze conclusies kunnen worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard".[67] Door het ongelimiteerde aspect van de bewaring wordt er volgens het HvJ zo'n zware inmenging op de grondrechten gemaakt dat dit de inbreuk ongeoorloofd maakt. Bewaring in deze vorm, waarbij ook de toegang tot de gegevens niet wordt ingeperkt, is niet noodzakelijk om het nagestreefde doel van "onderzoek, opsporing en vervolging van ernstige misdrijven" te bereiken.[68] Daarop volgde de ongeldigverklaring van de richtlijn.

De ongeldigverklaring was daarmee dus het gevolg van het feit dat de richtlijn niet precies en zorgvuldig genoeg was om het onbeperkte bewaren te verhinderen, maar ook van het feit dat de toegang tot de gegevens niet geregeld was. Onder welke voorwaarden het bewaren (en vorderen) van gegevens in nationale wetgeving dan wél toegestaan was werd in dit arrest nog niet verduidelijkt.[69] Zes jaar later echter, in het arrest La Quadrature du Net, kwam het HvJ met nadere vereisten waaraan regelingen voor het bewaren van verkeersgegevens moeten voldoen: een dergelijke regeling zou beperkingen moeten bevatten ten aanzien van de kring personen waarvan gegevens bewaard worden, van de periode en/of van het gebied.[70]

---

[66] HvJ 8 april 2014, gev. zaken C-293/12 en C-594/12, ECLI:EU:C:2014:238 (*Digital Rights Ireland en Seitlinger e.a.*), r.o. 39, 41-44.

[67] HvJ 8 april 2014, gev. zaken C-293/12 en C-594/12, ECLI:EU:C:2014:238 *(Digital Rights Ireland en Seitlinger e.a.*), r.o. 27

[68] HvJ 8 april 2014, gev. zaken C-293/12 en C-594/12, ECLI:EU:C:2014:238 *(Digital Rights Ireland en Seitlinger e.a.*), r.o. 56-71.

[69] Zie ook Molder, te, *DD* 2021/66, p. 857.

[70] HvJ 6 oktober 2020, gev. zaken C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net*), r.o. 147-151. Uit dit arrest blijkt overigens ook dat het HvJ van mening is dat indien er in een lidstaat sprake is van een ernstige en reële of voorzienbare bedreiging van de nationale veiligheid het in (uitzonderlijke) situaties legitiem kan zijn een bevel aan een telecomprovider te geven persoonsgegevens in zijn algemeenheid te bewaren, én door te geven. De doelstelling van de bescherming van de nationale veiligheid rechtvaardigt dit, die

In het Tele2 Sverige-arrest sprak het HvJ zich in 2016 uit over de betekenis van het Digital Rights-arrest voor de nationale wetgeving in de EU-landen. Het HvJ stelt eerst dat nationale regelingen die de algemene en ongedifferentieerde bewaring van verkeersgegevens mogelijk maken in strijd met de grondrechten kunnen worden geacht.[71] Vervolgens wordt overwogen dat *bewaring* van gegevens uitsluitend gebeurt om de nationale autoriteiten in bepaalde gevallen *toegang* tot die gegevens te geven. Daarom moet een nationale regeling voor de bewaring van verkeersgegevens óók noodzakelijkerwijs de toegang tot die gegevens door de bevoegde autoriteiten regelen.[72] Iedere nationale regeling die (ook) ziet op de toegang tot die bewaarde verkeers- en locatiegegevens moet daarom aan een aantal criteria voldoen, aldus het HvJ. Deze kunnen worden samengevat in de volgende "regels":

1. Gelet op de ernst van de ingreep in de betrokken grondrechten mag de nationale regeling voor de bewaring van verkeersgegevens niet verder gaan dan strikt noodzakelijk is om zware criminaliteit aan te kunnen pakken.
2. Een nationale wettelijke maatregel moet regels voor de bewaartermijn, de informatieplicht en de bescherming van de verwerkte gegevens hebben en aangeven hoe er adequate waarborgen voor het verkrijgen van toegang door de autoriteiten geregeld zijn.[73]

Uit de criteria blijkt wel dat het vereiste van de zware criminaliteit in dit arrest al speelt. Dit is echter voornamelijk in de context van de eisen aan nationale wetgeving die op de bescherming van bewaarde verkeersgegevens ziet.[74] Een nadere uitwerking door het HvJ van het zware criminaliteits-vereiste volgde later (zie paragraaf 2.3.2 hieronder).

Naar aanleiding van het arrest Digital Rights Ireland en het daarmee samenhangende vonnis van de rechtbank Den Haag waarin de Wet bewaarplicht buitenwerking wordt gesteld voert men in 2014 en 2015 in enige Nederlandse strafzaken het verweer dat telecommunicatiegegevens die in een strafzaak gebruikt worden niet bewaard hadden mogen worden. Het tóch gebruiken van de gegevens die nog in het kader van de Wet bewaarplicht verzameld waren zou een vormverzuim opleveren. Dit verweer wordt echter verworpen met het argument dat van een vormverzuim in de zin van artikel 359a Sv alleen sprake kan zijn indien

van de bestrijding van criminaliteit en van bescherming van de openbare veiligheid niet (r.o. 136-137). Zie ook Oerlemans & Hagens, *JBP* 2021/1, p. 31-33; Careel & Royer, *P&I* 2020, p. 270.

[71] HvJ 21 december 2016, gev. zaken C-203/15 en C-698/15, ECLI:EU:C:2016:970 (*Tele2 Sverige*), resp. r.o. 76 en r.o. 125.

[72] HvJ 21 december 2016, gev. zaken C-203/15 en C-698/15, ECLI:EU:C:2016:970 (*Tele2 Sverige*), r.o. 79.

[73] HvJ 21 december 2016, gev. zaken C-203/15 en C-698/15, ECLI:EU:C:2016:970 (*Tele2 Sverige*), resp. de r.o. 102-112 en 117-125.

[74] HvJ 21 december 2016, gev. zaken C-203/15 en C-698/15, ECLI:EU:C:2016:970 (*Tele2 Sverige*), r.o. 118.

het verzuim heeft plaatsgevonden in het voorbereidend onderzoek. Omdat de telecommunicatiegegevens van de verdachte niet bewaard waren in het kader van een opsporingsonderzoek, maar "gewoon" door de telecomaanbieder op grond van de Wet bewaarplicht, hadden de opsporingsambtenaren niet met de bewaring te maken gehad.[75] Het oordeel is dus steeds dat de inbreuk op de privacy geen vormverzuim in de zin van artikel 359a Sv oplevert, en dat er daarom ook geen reden is om eventueel tot bewijsuitsluiting over te gaan.

Een categorie apart vormt de rechtspraak over de zogenaamde stille sms'jes en IMSI-catchers. Door middel van een stille sms, verzonden door de politie, kan grofweg de plaats van een mobiele telefoon worden bepaald; de inzet van een IMSI-catcher kan vervolgens tot een verfijndere locatie-aanduiding leiden.[76] Sinds de invoering van de Wet bob is in een flink aantal zaken door de verdediging betoogd dat gegevens verkregen door middel van de stille sms'jes en de IMSI-catchers niet verzameld hadden mogen worden. De strekking van de gevoerde verweren was steeds dat door het (vaak meerdere malen) gebruiken van deze middelen om tot een plaatsbepaling te komen een stelselmatig inbreuk op de privacy gemaakt was. De Politiewet zou samen met de artikelen 141 en 142 Sv onvoldoende grondslag vormen voor het gebruiken van deze middelen om locatiegegevens te verkrijgen.

Uit de uitspraken volgt echter vrijwel steeds dat, na een afweging van proportionaliteit en subsidiariteit, wordt geoordeeld dat slechts sprake is van een geringe inbreuk op de privacy.[77] Daarnaast laten de uitspraken zien dat men het gebruik van de stille sms en de IMSI-catcher niet ziet als een dwangmiddel zoals beschreven in het Wetboek van Strafrecht, bijvoorbeeld zoals onder 126n.[78] Het verzamelen van locatiegegevens op deze manier hoeft daarom niet te voldoen aan de voorwaarden zoals gesteld in de bepalingen die de dwangmiddelen betreffen. Vormverzuimen die te maken hebben met het inzetten van de stille sms of de IMSI-catcher worden dus niet geconstateerd. Wél wordt op een gegeven moment opgemerkt dat "enige nadere regeling, ten behoeve van de transparantie van het strafproces, wel aanbevelenswaardig is".[79] Deze komt er niet, maar wel een conclusie van de advocaat-generaal bij de Hoge Raad, die gevolgd wordt door de Hoge Raad. De advocaat-generaal stelt dat "voor elke

[75] HvJ Amsterdam 9 mei 2014, ECLI:NL:GHAMS:2014:1835, r.o. 5.1.1; Rb. Limburg 9 december 2015, ECLI:NL:RBLIM:2015:10222, r.o. 3.3.
[76] De grondslag voor deze opsporingsmethode is te vinden in Politiewet 1993, artikel 2 en later in Politiewet 2012, artikel 3 (resp. *Stb.* 1993, 724 *en Stb*. 2012, 315).
[77] Rb. 's Hertogenbosch 15 oktober 2007, ECLI:NL:RBSHE:2007:BB6088; Rb. Amsterdam 8 maart 2011, ECLI:NL:RBAMS:2011:BP7233; Hof Arnhem-Leeuwarden 24 januari 2012, ECLI:NL:GHARN:2012:BV3076; Hof Arnhem-Leeuwarden 12 juni 2015, ECLI:NL:GHARL:2015:4335. Anders: Hof 's Hertogenbosch 20 juni 2013 ECLI:NL:GHSHE:2013:2579.
[78] Hof 's Hertogenbosch 15 augustus 2013, ECLI:NL:GHSHE:2013:4046.
[79] Hof 's Hertogenbosch 15 augustus 2013, ECLI:NL:GHSHE:2013:4046.

opsporingsmethode, of deze nu een specifieke wettelijke grondslag heeft of niet, geldt dat deze op een meer of minder indringende wijze kan worden toegepast". Daarom moet er, wanneer beoordeeld wordt of een methode toelaatbaar is, een weging van de omstandigheden van het geval plaatsvinden: er moet daarbij bekeken worden in welke mate de methode daadwerkelijk inbreuk heeft gemaakt op de persoonlijke levenssfeer.[80] Ondanks alle vereisten aan het verzamelen en vorderen van verkeersgegevens die volgen uit de in de hiervoor genoemde arresten van het HvJ mocht de dataverzameling via sms en IMSI-catcher - mits er een afweging plaatsvond - dus doorgaan buiten het Wetboek van Strafvordering om, wegens de geringe inbreuk die het middel maakt en de specifieke aard (de verzameling door de politie, niet door telecomaanbieders) ervan.

3.3.2 Het vereiste van de verdenking van een ernstig misdrijf: La Quadrature du Net en de conclusie bij het arrest Ministerio Fiscal

Uit het hierboven besproken arrest Tele2 Sverige blijkt dat het HvJ van mening is dat een nationale regeling die het bewaren van verkeersgegevens regelt er óók voor zorgt dat er toegang tot die gegevens bestaat. De brug tussen het bewaren van verkeersgegevens en de toegang ertoe wordt vier jaar later definitief geslagen in het arrest La Quadrature du Net. Het HvJ overweegt in dit arrest eerst dat toegang tot op grond van artikel 15 van de e-privacyrichtlijn bewaarde verkeersgegevens alleen kan worden gerechtvaardigd door een doelstelling van algemeen belang. Dit belang mag echter niet de "vervolging en bestraffing van een gewoon strafbaar feit" zijn, omdat dat strijdig zou zijn met het evenredigheidsbeginsel.[81] Na het aanhalen van dit beginsel oordeelt het HvJ dat alléén de doelstelling "bestrijding van zware criminaliteit" de toegang tot de verkeersgegevens kan rechtvaardigen. Daarbovenop oordeelt het HvJ dat zelfs in die gevallen van zware criminaliteit alléén toegang mag worden verleend tot de verkeersgegevens die in overeenstemming met artikel 15 eerste lid bewaard zijn.[82] Hieruit valt af te leiden dat wanneer de bewaring van verkeersgegevens onrechtmatig is geweest, het gebruik ervan dat per definitie ook is.[83]

[80] Concl. A-G F.W. Bleichrodt 8 april 2014, ECLI:NL:PHR:2014:633, r.o. 34.
[81] HvJ 6 oktober 2020, gev. zaken C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net*), r.o. 166.
[82] HvJ 6 oktober 2020, gev. zaken C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net*), r.o. 167.
[83] Dit gezien het feit dat het HvJ het bewaren van en de toegang tot de verkeersgegevens als twee op zichzelf staande privacy-inbreuken beschouwt, die "dientengevolge afzonderlijk moeten worden gerechtvaardigd", zie paragraaf 2.3 en Molder, te, *DD* 2021/66, p. 859.

Het begrip, "zware (of ernstige) criminaliteit" wordt overigens niet verder ingevuld in dit arrest, of in andere arresten die verkeersgegevens betreffen. Behalve voor de bijzonder zware criminaliteit met een grensoverschrijdende dimensie (artikel 83, eerste lid VWEU) geeft de Europese wetgeving ook geen indicatie van wat eronder verstaan moet worden.[84] In een andere context is in de conclusie bij het arrest Ministerio Fiscal echter een aantal factoren opgesomd die in aanmerking kunnen worden genomen bij het beoordelen van de zwaarte van delicten.[85] Het gaat hier onder andere om de context van het feit (in hoeverre speelt opzet mee, zijn er verzwarende omstandigheden zijn, is er sprake van recidive), de omvang van het geschade maatschappelijke belang, de aard en omvang van de schade en de hoogte van de straffen die doorgaans voor dergelijke feiten worden opgelegd. Op basis van deze factoren zou een strafbaar feit al dan niet vallen onder "ernstige criminaliteit". [86]

Gebruikersgegevens, een subcategorie van verkeersgegevens die onder andere naam- en adresgegevens inhoudt (zie paragraaf 1.1), worden in het arrest La Quadrature du Net besproken als in beginsel minder privacygevoelig, omdat zij slechts bestaan uit de gegevens die het mogelijk maken vast te stellen wie op een bepaald tijdstip gebruik heeft gemaakt van bijvoorbeeld een specifiek IP-adres of telefoonnummer. Het bewaren van gebruikersgegevens zou in beginsel algemeen en ongedifferentieerd mogen plaatsvinden, omdat de inmenging op het privéleven die het opvragen van gebruikersgegevens veroorzaakt niet als ernstig wordt beschouwd.[87] Het HvJ stelt wel dat IP-adressen meer over een gebruiker kunnen prijsgeven dan andere gebruikersgegevens, omdat zij "onder meer kunnen worden gebruikt om de volledige zoekgeschiedenis van een internetgebruiker te traceren" en zo een gedetailleerd profiel van iemand kunnen geven.[88] De algemene bewaring ervan wordt onder omstandigheden toch toelaatbaar geacht. Er moet dan nog steeds wél sprake zijn van zware criminaliteit en de bewaartermijn mag niet langer zijn dan strikt noodzakelijk is.[89]

---

[84] Genoemd worden onder andere seksuele uitbuiting, illegale drugshandel en het witwassen van geld.
[85] Concl. A-G H. Saugmandsgaard Øe, HvJ 3 mei 2018, C-207/16, ECLI:EU:C:2018:300 (*Ministerio Fiscal*), r.o. 105.
[86] Ook in de conclusie bij het hierna te bespreken arrest Prokuratuur wordt nader beschreven wat meeweegt bij het bepalen of een feit een ernstig strafbaar feit is. De AG merkt hier op dat er "rekening [moet] worden gehouden met de aard van de strafbare feiten, de aan de maatschappij toegebrachte schade, de aantasting van de rechtsbelangen, en de algemene gevolgen ervan voor de nationale rechtsorde en voor de waarden van een democratische samenleving. De specifieke historische, economische en sociale context van elke lidstaat speelt in dit verband eveneens een rol". (Concl. A-G G. Pitruzzella, HvJ 21 januari 2020, C-746/18, ECLI:EU:C:2020:18 (*Prokuratuur*), r.o. 93).
[87] HvJ 6 oktober 2020, gev. zaken C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net*), r.o. 155-159.
[88] HvJ 6 oktober 2020, gev. zaken C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net*), r.o. 153.
[89] HvJ 6 oktober 2020, gev. zaken C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net*), r.o. 154-156.

Bij het bestuderen van de Nederlandse jurisprudentie die verkeersgegevens betreft valt op dat er regelmatig sprake is van verweren die zien op de afwezigheid van een verdenking van een strafbaar feit ten tijde van het vorderen van die gegevens. Daarom zou de vordering onrechtmatig zijn geweest.[90] De hoeveelheid verweren waarin de rechtmatigheid van de vordering van verkeersgegevens werd betwist omdat er geen sprake zou zijn geweest van een *ernstig* strafbaar feit lijkt echter niet groot.[91] In één gevonden zaak werd aangevoerd dat het in de onderhavige zaak niet draaide om de bestrijding van zware criminaliteit omdat het slechts om winkeldiefstal ging. Het gerechtshof Den Haag oordeelde in dit geval echter dat er sprake was van een serie diefstallen, heling én deelneming aan een criminele organisatie, waardoor ruim aan het vereiste van artikel 126n werd voldaan.[92] In de andere zaken werd gesteld dat er bij de start van de onderzoeken vormverzuimen waren ontstaan, omdat de verdenking die er op dát moment was van een ernstig misdrijf of van een misdrijf in georganiseerd verband dat een ernstige inbreuk maakt op de rechtsorde achteraf onterecht bleek: er hadden dus geen verkeersgegevens gevorderd mogen worden. In beide gevallen oordeelde de rechtbank dat de verdenking bij de start voldoende grondslag gaf voor de vordering van de gegevens, omdat de op dat moment beschikbare informatie daar genoeg aanleiding voor gaf.[93]

3.3.3 Voorafgaande controle door een rechterlijke autoriteit bij het vorderen van verkeersgegevens: het arrest Prokuratuur

Na de reeks uitspraken die het bewaren in combinatie met het vorderen van verkeersgegevens betroffen gaf het HvJ in maart 2021 in het arrest Prokuratuur meer invulling aan de voorwaarden voor het vorderen van verkeersgegevens. In dit arrest doet het HvJ een duidelijke uitspraak over de voorafgaande toetsing die gedaan moet worden om na te gaan of een vordering voor het verkrijgen van toegang tot verkeersgegevens wel een geoorloofde inbreuk is op de privacy van de betrokkene. Eerder al oordeelde het dat toegang tot verkeersgegevens alleen maar kan worden verleend na voorafgaande toestemming door een rechterlijke instantie of een onafhankelijke bestuurlijke entiteit.[94] In het arrest Prokuratuur

[90] Zie bijvoorbeeld Rb. Roermond 2 november 2011, ECLI:NL:RBROE:2009:BK199; Rb. Noord-Holland 20 juli 2017, ECLI:NL:RBNHO:2017:6175; Rb. Midden-Nederland 6 maart 2020, ECLI:NL:RBMNE:2020:853.
[91] Zie ook Buiten, van, *DD* 2016, p. 138. Andere gevonden zaken betreffen onderzoeken die de inhoud van de communicatie betreffen. Hierin komt een afweging "zwaarte van het feit" (vereist is dat het feit een ernstige inbreuk op de rechtsorde oplevert) versus "mate van de inbreuk" voor. Zie bijvoorbeeld Rb. Noord-Holland 16 mei 2019, ECLI:NL:RBNHO:2019:4280.
[92] HvJ Den Haag 20 juli 2021, ECLI:NL:GHDHA:2021:1588.
[93] Rb. Arnhem 22 april 2011, ECLI:NL:RBARN:2011:BQ2163; Rb. Amsterdam 20 juli 2017, ECLI:NL:RBAMS:2017:5130.
[94] In bijvoorbeeld HvJ 6 oktober 2020, C-623/17, ECLI:EU:C:2020:790 (*Privacy International*), r.o. 68 en HvJ 21 december 2016, gev. zaken C-203/15 en C-698/15, ECLI:EU:C:2016:970 (*Tele2 Sverige*), r.o. 117-118.

wordt nu bepaald dat een vordering door een officier van justitie, met daaropvolgend een latere toetsing door een rechter, niet afdoende waren om hieraan te voldoen.

Het HvJ overweegt dat wetgevers de voorwaarden vaststellen waaronder telecomaanbieders aan bepaalde autoriteiten toegang moeten verlenen tot de persoonsgegevens waarover zij beschikken. De nationale wetgever bepaalt daarbij dan ook de materiële en procedurele voorwaarden voor het gebruik van de regeling. Daarom moet er een onafhankelijke instantie zijn die controleert of aan deze voorwaarden voldaan wordt bij het verkrijgen van toegang, aldus het HvJ. Deze instantie dient namelijk over alle bevoegdheden te beschikken en alle noodzakelijke waarborgen te bieden om ervoor te zorgen dat de verschillende betrokken belangen en rechten met elkaar in overeenstemming worden gebracht.[95] In de zaak Prokuratuur stelt het HvJ voor het eerst expliciet dat een openbaar ministerie, dat betrokken is bij de uitvoering van het strafrechtelijk onderzoek en als procespartij de strafvordering instelt, niet als een dergelijke onafhankelijke autoriteit kan worden beschouwd.[96] Hiermee lijkt het HvJ - in ieder geval voor met Estland te vergelijken rechtssystemen - de officier van justitie definitief van zijn statuut als onafhankelijk opererend rechterlijk ambtenaar te ontdoen.[97]

Sinds het Prokuratuurarrest is er in enkele tientallen Nederlandse uitspraken aandacht geschonken aan de - al dan niet - onrechtmatigheid van het gebruik van verkeersgegevens omdat een rechterlijke toetsing bij het vorderen van de gegevens van een telecomaanbieder ontbroken zou hebben.[98] De oordelen van de diverse rechtbanken en gerechtshoven over het gebruik van de gegevens houden steeds een drietal “stappen” in. Als eerste wordt overwogen dat het voor strafrechtelijke doeleinden verlenen van toegang tot verkeersgegevens slechts is toegestaan in het kader van procedures ter bestrijding van zware criminaliteit en procedures ter voorkoming van ernstige bedreigingen van de openbare veiligheid. Vervolgens wordt gesteld dat uit Europese rechtspraak volgt dat nationale wetgevers de voorwaarden moeten vaststellen waaronder telecomaanbieders aan de bevoegde instanties toegang moeten verlenen tot hun

[95] HvJ 2 maart 2021, C-746/18, ECLI:EU:C:2021:152 (*Prokuratuur*), r.o. 48-52.
[96] HvJ 2 maart 2021, C-746/18, ECLI:EU:C:2021:152 (*Prokuratuur*), r.o. 54-57. De rechter wordt nu aangewezen als enige onafhankelijke instantie, zoals ook al gebeurde in eerdere uitspraken die het uitvaardigen van Europese arrestatiebevelen door de officier van justitie betroffen, namelijk in HvJ 27 mei 2019, gev. zaken C-508/18 en C-82/19 PPU, ECLI:EU:C:2019:456 (*OG en PI*) en HvJ 24 november 2020, C-510/19), ECLI:EU:C:2020:953 (*AZ*).
[97] Vgl. paragraaf 2.3.1.
[98] Er wordt hierbij in meerdere gevallen verwezen naar het vonnis van de rechtbank Rotterdam van 30 april 2021, één van de eerste uitspraken waarin het Prokuratuurarrest aan de orde kwam. Overigens wordt door diverse raadslieden gepoogd om onderzoek aan een mobiele telefoons en het gebruik van een IMSI-catcher onder het bereik van het arrest te laten vallen, zie bijvoorbeeld Rb. Midden-Nederland 20 augustus 2021, ECLI:NL:RBMNE:2021:3965.

bewaarde persoonsgegevens. Als laatste wordt dan overwogen dat die gereglementeerde toegang onderworpen dient te zijn aan een voorafgaande toetsing door een rechterlijke instantie of een onafhankelijke bestuurlijke entiteit, waarbij gesteld wordt dat de instantie die die toetsing verricht niet betrokken mag zijn bij de uitvoering van het betrokken strafrechtelijk onderzoek. De instantie moet neutraal zijn ten opzichte van de partijen in de strafprocedure, om aan het vereiste van onafhankelijkheid te voldoen. Dat is niet het geval bij een Openbaar Ministerie dat de onderzoeksprocedure van een strafrechtelijk onderzoek leidt en ook optreedt als openbaar aanklager tijdens de strafprocedure, zo wordt steeds geoordeeld.[99] Er wordt dan ook in alle gevallen geoordeeld dat het recht op bescherming van de persoonlijke levenssfeer geschonden is en dat er sprake is van vormverzuimen.[100] Opvallend is dat het gerechtshof Amsterdam in een zaak overweegt dat de inbreuk op de persoonlijke levenssfeer van de verdachte relatief kort duurde en dat er door de (beperkte hoeveelheid) verzamelde gegevens geen "zeer compleet beeld van het privéleven van verdachte is verkregen".[101] Hiermee lijkt het te bedoelen dat de inmenging niet ernstig was: in dit geval een reden om het bij het constateren van een vormverzuim te houden.

In meerdere uitspraken wordt bij de hierboven beschreven drie stappen ook nog expliciet de bescherming door de e-privacyrichtlijn genoemd. In de voorkomende gevallen lijkt dit steeds het gevolg te zijn van een door het openbaar ministerie ingenomen standpunt dat het Prokuratuurarrest alleen ziet op verkeersgegevens die in het kader van een (in Nederland niet meer bestaande) wettelijke algemene bewaarplicht bewaard zijn. De rechtbanken en hoven overwegen daarop echter steeds dat, gelet op de doorwerking van de e-privacyrichtlijn in de Nederlandse rechtsorde, het feit dat de gegevens ten behoeve van de bedrijfsvoering van telecomaanbieders zijn bewaard niet afdoet aan de verplichting om te voldoen aan de eisen die de richtlijn stelt aan de toegang tot gegevens van gebruikers. Het Prokuratuurarrest ziet dus ook op de in de kader van de bedrijfsvoering van de telecomproviders bewaarde gegevens.[102] Door onder meer de rechtbank Rotterdam en het gerechtshof Den Haag wordt daartoe ook het arrest van het HvJ in de zaak Ministerio Fiscal aangehaald, waarin werd geoordeeld dat een in het

[99] Zie onder andere: Rb. Rotterdam 30 april 2021, ECLI:NL:RBROT:2021:3906; HvJ Den Haag 20 juli 2021, ECLI:NL:GHDHA:2021:1588; HvJ Arnhem-Leeuwarden 28 juni 2021, ECLI:NL:GHARL:2021:6245; HvJ Amsterdam 8 oktober 2021, ECLI:NL:GHAMS:2021:2863.
[100] Meestal wordt volstaan met de enkele constatering hiervan en worden er geen verdere rechtsgevolgen aan verbonden. Uitzondering hierop was bijvoorbeeld in juni 2021 het HvJ Arnhem-Leeuwarden, dat het door vormverzuim ontstane nadeel compenseerde door in plaats van 34 maanden 33 maanden en 2 weken gevangenisstraf op te leggen (HvJ Arnhem-Leeuwarden 28 juni 2021, ECLI:NL:GHARL:2021:6245).
[101] HvJ Amsterdam 8 oktober 2021, ECLI:NL:GHAMS:2021:2863.
[102] Bijvoorbeeld in Rb. Rotterdam 30 april 2021, ECLI:NL:RBROT:2021:3906; HvJ Den Haag 20 juli 2021, ECLI:NL:GHDHA:2021:1588; HvJ Arnhem-Leeuwarden 28 juni 2021, ECLI:NL:GHARL:2021:6245.

kader van een opsporingsonderzoek geformuleerd verzoek om toegang tot verkeersgegevens binnen de werkingssfeer van de e-privacyrichtlijn valt.[103]

In het voorgaande werden de vereisten voor een legitieme beperking van de grondrechten van de artikelen 7 en 8 besproken, zoals die aan de orde zijn wanneer er gebruik wordt gemaakt van verkeersgegevens voor strafrechtelijk onderzoek. De gronden en mogelijkheden voor zo'n legitieme beperking werden geanalyseerd aan de hand van artikel 52, eerste lid van het Handvest en aan de hand van de nadere invulling die er wat betreft het gebruik van verkeersgegevens aan de bescherming van de grondrechten wordt gegeven in Europese en nationale rechtspraak. Een legitieme beperking dient op grond van artikel 52, eerste lid aan drie vereisten te voldoen: het gesteld zijn bij wet, het beantwoorden aan een Europeesrechtelijke doelstelling van algemeen belang en het proportionaliteitsvereiste. In het kader van de proportionaliteitstoets zijn in het geval van het gebruik van verkeersgegevens met name de criteria van de strikte noodzakelijkheid van de maatregel, de verdenking van een ernstig misdrijf en de voorafgaande controle op de vordering van de verkeersgegevens door een rechterlijke autoriteit van belang. In het volgende hoofdstuk zal het gebruik van verkeersgegevens zoals dat in Nederland geregeld is dan ook getoetst worden aan deze combinatie van criteria.

[103] Rb. Rotterdam 30 april 2021, ECLI:NL:RBROT:2021:3906; HvJ Den Haag 20 juli 2021, ECLI:NL:GHDHA:2021:1588. Waarschijnlijk wordt hier verwezen naar r.o. 35-36 van het arrest, zie: HvJ 2 oktober 2018, C-207/16, ECLI:EU:C:2018:788 (*Ministerio Fiscal*), r.o. 35-36. Overigens werd in zaken die de Encrochatdata betreffen ook veelvuldig een beroep op de beschermende werking van de e-privacyrichtlijn en het Handvest gedaan. In dit verband werd echter opgemerkt dat uit de richtlijn blijkt dat deze "in geen geval" werking heeft wanneer de staat op strafrechtelijk gebied handelt. De gegevens werden immers verkregen door het "hacken" van de servers van EncroChat, waarbij het opsporingsonderzoek gericht was op provider EncroChat (en dus niet op de gebruikers van telecomdiensten) omdat die zware criminaliteit gefaciliteerd zou hebben. Zie onder meer Rb. Oost-Brabant 15 september 2021, ECLI:NL:RBOBR:2021:4986, r.o. 2.2.

HOOFDSTUK 4: HET GEBRUIK VAN VERKEERSGEGEVENS GETOETST

Zoals bleek uit de voorgaande hoofdstukken zijn voor het gebruik van verkeersgegevens ten behoeve van strafrechtelijk onderzoek niet alleen de relevante bepalingen uit het Wetboek van Strafvordering van belang, maar ook die uit de Telecommunicatiewet. Artikel 11.13, eerste lid van de Telecommunicatiewet bepaalt dat telecomaanbieders bevoegd zijn het vertrouwelijkheidsbeginsel te doorbreken, indien dit noodzakelijk is ter voorkoming, opsporing en vervolging van strafbare feiten. In de artikelen 126n, 126u en 126zh Sv wordt bepaald dat verkeersgegevens slechts gevorderd mogen worden als dit in het belang van het onderzoek is. Ook moet er sprake zijn van een "verdenking van een misdrijf als omschreven in artikel 67, eerste lid", respectievelijk van een redelijk vermoeden van een dergelijk misdrijf als dat wordt "beraamd of gepleegd in georganiseerd verband" en een ernstige inbreuk op de rechtsorde oplevert, of van "aanwijzingen van een terroristisch misdrijf". Een vordering van verkeersgegevens bij een telecomaanbieder op grond van de voornoemde artikelen mag echter slechts betrekking hebben op bepaalde, in het Besluit vorderen gegevens telecommunicatie genoemde, gegevens en mag, sinds de buitenwerkingstelling van de Wet bewaarplicht telecommunicatiegegevens en bij gebrek aan een nieuwe wet, niet méér inhouden dan de categorie gegevens die voor de communicatie zelf en voor factu rerings- en marketingdoeleinden bewaard wordt, zo blijkt uit het Wetboek van Strafvordering en de Telecommunicatiewet. In zowel de Telecommunicatiewet als het Wetboek van Strafvordering worden termijnen gesteld aan het bewaren van en de toegang tot de gegevens. De artikelen 11.2a derde lid, 11.3 en 11.3a Telecommunicatiewet regelen de informatie aan gebruikers over het onderscheppen van communicatie en over de beveiliging van de bewaarde gegevens. Artikel 15.1, eerste lid sub g regelt het toezicht op de naleving van de wet in het geval van het gebruik van verkeersgegevens en locatiegegevens. Het Wetboek van Strafvordering bepaalt vervolgens weer de vereisten die gelden voor de toegang tot de gegevens door justitie.[104]

De inhoud van de hierboven genoemde bepalingen zal in het navolgende langs de lat van de artikelen 7 en 8 van het Handvest worden gelegd. Zoals hiervoor al aangegeven komt het vorderen van verkeersgegevens in alle gevallen neer op een - lichte dan wel ernstige - inbreuk op de grondrechten van de artikelen 7 en 8: daarom zal deze toetsing plaatsvinden aan de hand van de vereisten die op grond van artikel 52, eerste lid gesteld worden aan beperkingen

[104] Het laatste lid van de artikelen 126n, 126u en 126zh Sv bepaalt steeds dat er daaraan ook middels een algemene maatregel van bestuur regels kunnen worden gesteld, in casu is dit het Besluit vorderen gegevens telecommunicatie (zie paragraaf 2.1).

op de grondrechten. Eerst zal kort aandacht worden besteed aan de vereisten "Bij wet gesteld' en "Met een doelstelling van algemeen belang". Vervolgens komt de proportionaliteitstoets aan de orde, waarbij (met name de Europese) jurisprudentie op dit gebied betrokken zal worden.

4.1 Deel uitmakend van een formele wet

De regelingen die van toepassing zijn voor toetsing aan het vereiste "bij wet gesteld" zijn de gedeelten van de Telecommunicatiewet die de omgezette e-privacyrichtlijn betreffen en de bepalingen uit het Wetboek van Strafvordering die zien op het vorderen van verkeersgegevens. Omdat deze regelingen deel uitmaken van formele wetten kan genoegzaam worden aangenomen dat zij - geredeneerd vanuit het Handvest - voldoende precies en voorzienbaar zijn (zie paragraaf 3.2.1). Aan het eerste vereiste dat de beperking "bij wet gesteld" moet zijn is daarmee voldaan.[105]

4.2 Met een doelstelling van algemeen belang

Door het brede bereik van door de EU erkende doelstellingen en beschermingsgronden zijn er zeer veel mogelijkheden om de rechten uit het Handvest te beperken. Bulterman stelt zelfs: "Van de belangen die in dat kader voor bescherming in aanmerking komen valt geen uitputtende opsomming te geven, omdat in beginsel elke dwingende reden van algemeen belang als legitiem doel naar voren kan worden gebracht".[106] Uit de Toelichting bij artikel 52 van het

Handvest valt op te maken dat de opstellers ervan in ieder geval artikel 3 VEU relevant vinden als bron voor de doelstellingen van algemeen belang. In artikel 3 worden onder meer genoemd dat de Unie als doelen heeft" "het welzijn van haar volkeren bevorderen", "een ruimte van […] recht" te bieden en bescherming te bevorderen. In artikel 67, derde lid VWEU wordt daarnaast het streven van de Unie naar een hoog niveau van veiligheid genoemd, door middel van maatregelen ter voorkoming en bestrijding van criminaliteit.[107]

Gezien het bovenstaande kan worden aangenomen dat voor de beperking op de bescherming van persoonsgegevens zeker een rechtvaardigingsgrond aanwezig is als het om het inzetten van vertrouwelijke gegevens voor strafvorderlijk onderzoek gaat. Ook geeft

[105] Zie ook de uitgebreide toelichting op dit vereiste door de minister in de *Kamerstukken II* 2001/02, 28059, nr. 5, p. 11. Hier wordt bijvoorbeeld vermeld dat het "met het oog op de waarborgen tegen willekeur […] van belang is dat een vordering tot het verstrekken van gegevens schriftelijk dient te zijn en dat van de verstrekking van gegevens een proces-verbaal dient te worden opgemaakt, waarin de feiten of omstandigheden waaruit blijkt dat is voldaan aan het vereiste van een verdenking van een strafbaar feit van een bepaalde ernst en waarin de reden waarom de gegevens in het belang van het onderzoek worden gevorderd dienen te worden vermeld".
[106] Bulterman 2015, p. 74.
[107] Uit de redactie van de Toelichting bij artikel 52 van het Handvest volgt dat de daar genoemde artikelen met Unie-doelstellingen geen uitputtende lijst vormen, zie paragraaf 3.2.2.

bijvoorbeeld het arrest Digital Rights Ireland en Seitlinger e.a. hier een aanwijzing voor: in dit arrest oordeelde het HvJ dat dataretentie gerechtvaardigd kon zijn omdat het bestrijden van ernstige criminaliteit een doel van algemeen belang van de Unie is. Daarnaast wordt in dit verband in dit arrest opgemerkt dat in het Handvest wordt bepaald dat eenieder niet alleen recht heeft op vrijheid, maar ook op veiligheid.[108] Wat betreft de aanwezigheid van een door de EU erkende doelstelling kan de beperking daarom mijns inziens als legitiem worden beschouwd. Hiermee is ook aan de tweede voorwaarde voldaan.

4.3 De proportionaliteitstest doorstaan

Nu aan de eerste twee voorwaarden voldaan is dient op grond van artikel 52, eerste lid Handvest getoetst te worden of de Nederlandse wetgeving inzake het gebruik van verkeersgegevens in strafrechtelijk onderzoek voldoet aan het proportionaliteitsvereiste in al zijn aspecten. Dit wordt hieronder besproken aan de hand van drie toetsingscategorieën: de categorie van de strikte noodzakelijkheid, die van de verdenking van en zwaar misdrijf en die van de voorafgaande controle door een rechterlijke autoriteit.

4.3.1 Wat betreft de strikte noodzakelijkheid van de inbreuk

In overeenstemming met de arresten Digital Rights Ireland en Seitlinger e.a. en Tele2 Sverige vindt de *bewaring* van gegevens sinds de buitenwerkingstelling van de Wet bewaarplicht nog maar in zeer beperkte mate plaats. Wát er aan verkeersgegevens bewaard mag worden is uitgewerkt in artikel 11.5 van de Telecommunicatiewet. Dit betreft niét de inhoud van de communicatie, waarmee de essentie van de grondrechten van de artikelen 7 en 8 veilig lijkt te zijn (zie paragraaf 3.2.3). Daarnaast zorgt de Telecommunicatiewet voor een wettelijke regeling van bewaartermijn, informatieplicht, beveiliging en bescherming van de bewaarde verkeersgegevens. Hiermee wordt ook gedeeltelijk voldaan aan de in paragraaf 3.3.1 genoemde "regel 2" van het Tele2 Sverige-arrest, namelijk aan het vereiste dat een wettelijke maatregel materiële en procedurele regels voor die onderwerpen bevat. Het bovenstaande in ogenschouw nemende kan worden geconcludeerd dat wat de bewaring betreft voldaan wordt aan de vereisten van de artikelen 7 en 8 Handvest voor noodzakelijkheid en afbakening. Mijns inziens geeft de Nederlandse regeling voor de bewaring dan ook geen aanleiding om te veronderstellen dat er bij een vordering verkeersgegevens gegevens worden verkregen die in strijd met de

[108] HvJ 8 april 2014, gev. zaken C-293/12 en C-594/12, ECLI:EU:C:2014:238 (*Digital Rights Ireland en Seitlinger e.a.*), r.o. 41-44.

grondrechten bewaard zijn, wat een schending van het Handvest zou opleveren (zie paragraaf 3.3.2).

De jurisprudentie van het HvJ maakt ook duidelijk dat er voor *toegang* tot bewaarde verkeersgegevens sprake moet zijn van een strikte noodzaak. In het Tele2 Sverige-arrest werd al gesteld dat een nationale wettelijke maatregel diende aan te geven hoe er adequate waarborgen voor het verkrijgen van toegang door de autoriteiten geregeld waren. Men kan zich afvragen of de bepalingen in de artikelen 126n, 126u en 126zh Sv wel specifiek genoeg aangeven wanneer een gemaakte inbreuk (strikt) noodzakelijk is. Bij het vorderen van verkeersgegevens wordt gebruik gemaakt van een opsporingsmiddel dat ten tijde van de invoering van de Wet bob nog een relatief lichte inbreuk op de persoonlijke levenssfeer maakte. Het vorderen van verkeersgegevens werd toen nog algemeen beschouwd als significant minder ingrijpend dan methoden als het opnemen van communicatie of het binnendringen van een geautomatiseerd werk. Inmiddels is aan dit inzicht wel een en ander gewijzigd, nu het gebruik van mobiele telefoons en internet een enorme vlucht heeft genomen. Het bestaan van een verschil tussen de twee opsporingsmethoden lijkt dan ook steeds meer betwijfeld te worden.[109] Het informatiegehalte van verkeersgegevens wordt door verschillende auteurs als veel groter dan vroeger beschouwd, eenvoudigweg door de enorme toename van de hoeveelheid gegevens die er van een betrokkene bestaat. Ook het HvJ is van mening dat de hoeveelheid van de gegevens het mogelijk maakt precieze conclusies te trekken over het privéleven van de betrokken personen (zie ook paragraaf 3.3.1).

Uit de verschillende criteria voor vorderingen in titel IV A, zevende en achtste afdeling Sv schemert echter nog het "oude" verschil in opvatting over de impact van de inbreuken door. Wanneer namelijk een vordering tot het opnemen van telecommunicatie of tot het binnendringen in een geautomatiseerd werk wordt gedaan, bijvoorbeeld op grond van respectievelijk de artikelen 126m en 126nba Sv, is vereist dat het onderzoek dit "dringend vordert". Dit houdt in dat de bevoegdheid alleen dan mag worden gebruikt wanneer men niet kan verwachten dat hetzelfde resultaat kan worden bereikt door middel van een lichtere opsporingsbevoegdheid.[110] In de artikelen die de verkeersgegevens betreffen wordt daarentegen slechts de voorwaarde van het "belang van het onderzoek" genoemd waaraan voldaan moet worden wanneer door de officier van justitie een vordering tot het verstrekken van verkeersgegevens wordt gedaan.[111] Er valt mijns inziens echter te betwijfelen of in de huidige

[109] Zie Koops & Smits 2014, p 111; Brkan *German Law Journal* 2019, p. 872.
[110] *Kamerstukken II* 1996/97, 25403, nr. 3 , p. 30.
[111] Zie voor de omschrijving van dit begrip paragraaf 2.3.3.

tijd het opnemen van de - lichtere - eis dat de vordering gerechtvaardigd wordt door het "belang van het onderzoek" wel voldoende adequaat is en niet teveel aan de discretie van de officier van justitie overlaat: doet het nog wel voldoende recht aan de ingrijpendheid van dit dwangmiddel en wordt het noodzakelijkheidsvereiste er voldoende mee gediend?

4.3.2 Wat betreft de verdenking van een (zwaar) misdrijf

Uit de arresten Tele2 Sverige en la Quadrature du Net volgt niet alleen dat nationale regelingen die het vorderen van verkeersgegevens regelen zich moeten beperken tot personen die worden verdacht van een misdrijf, maar óók dat deze personen minstens moeten worden verdacht van betrokkenheid bij of het plannen of plegen van een *ernstig* misdrijf.[112]

Lidstaten hebben in beginsel de vrijheid om het begrip ernstige criminaliteit zelf in te vullen. Bij het toepassen van dwangmiddelen is een algemeen uitgangspunt van de Nederlandse wetgever dat het "naarmate de bevoegdheid ingrijpender is, dient […] te gaan om een verdenking van een ernstiger misdrijf".[113] Dit aldus de memorie van toelichting bij de Wetswijziging bevoegdheden vorderen gegevens in 2004. De voorlopige hechtenis-feiten van artikel 67, eerste lid Sv vormen de ondergrens bij de bevoegdheid verkeersgegevens te vorderen. De vraag is of alle strafbare feiten die onder de voorlopige hechtenis-feiten vallen in lijn met de hiervoor genoemde memorie van toelichting beschouwd kunnen worden als ernstig genoeg voor een ingrijpende bevoegdheid als het vorderen van verkeersgegevens en ook of zij in alle gevallen kunnen worden beschouwd als de zware criminaliteit waar het HvJ op doelt.

In 2015 oordeelde de rechtbank Den Haag dat het vereiste van het voorlopige hechtenis-feit niet kon waarborgen dat de toegang tot de verkeersgegevens daadwerkelijk beperkt werd tot hetgeen strikt noodzakelijk was voor de bestrijding van (enkel) ernstige criminaliteit. Er werd daarbij overwogen dat de categorie voorlopige hechtenis-feiten eveneens strafbare feiten inhield die niet voldoende ernstig waren om de inmenging in de grondrechten te rechtvaardigen: een diefstal van een fiets kan hier ook al onder vallen.[114] Ook misdrijven als het verspreiden van een opruiend geschrift (artikel 132 Sr) en het "zonder vergunning exploiteren van speelautomaten" (artikel 30h Wet op de kansspelen) vallen op grond van artikel 67, eerste lid onder b en c Sv onder de strafbare feiten waarvoor verkeersgegevens gevorderd kunnen worden.

[112] Overigens lijkt het HvJ ook akkoord te gaan met het vorderen van verkeersgegevens van slachtoffers of personen uit de sociale of professionele omgeving van de verdachte indien "op basis van objectieve en niet-discriminatoire factoren kan worden geoordeeld dat die gegevens kunnen helpen bij het ophelderen van een […] misdrijf". Zie HvJ 6 oktober 2020, gev. zaken C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net*), r.o. 165.
[113] *Kamerstukken II* 2003/04, 29441, nr. 3, p. 5.
[114] Rb. Den Haag (vzr.) 11 maart 2015, ECLI:NL:RBDHA:2015:2498, r.o. 3.10.

Het criterium van het voorlopige hechtenis-feit lijkt daarnaast ook niet altijd afdoende te zijn wanneer de context van het misdrijf, de omvang van het geschade maatschappelijke belang, de aard en omvang van de schade en de hoogte van de doorgaans opgelegde straffen meegewogen worden.[115] Afweging van deze factoren kan er mijns inziens heel goed toe leiden dat een feit uit de lijst van artikel 67, eerste lid Sv niet als een ernstig misdrijf kan worden beschouwd. Wanneer de omstandigheden per geval worden meegewogen zal dit bijvoorbeeld kunnen gelden in gevallen als de hierboven al genoemde fietsendiefstal of een winkeldiefstal, verduistering of eenvoudige bedreiging.

Het moge duidelijk zijn dat wanneer in een geval van een "te licht misdrijf" het gewicht en de urgentie van het misdrijf tegen de inbreuk op de grondrechten wordt afgewogen niet voldaan wordt aan de uitleg van de beperkingsvereisten zoals die door het HvJ gegeven wordt.[116] Dit wordt mijns inziens niet anders als wordt meegewogen dat lidstaten zelf mogen definiëren wat zij onder ernstige criminaliteit verstaan. Uiteraard blijft het aan de officier van justitie om te beslissen of er een vordering voor het verstrekken van verkeersgegevens wordt gedaan, maar feit blijft dat de bepalingen in het Wetboek van Strafvordering op dit moment niet volledig genoeg lijken te zijn om opsporingshandelingen die een grote inbreuk maken op het privéleven in het geval van minder zware misdrijven te voorkomen. Daarmee lijkt mijns inziens de inhoud van de huidige artikelen die het vorderen van verkeersgegevens regelen ook op dit punt niet voldoende specifiek om te voldoen aan het bepaalde in de artikelen 7 en 8 van het Handvest.

4.3.3 Wat betreft de onafhankelijke rechterlijke instantie

In het Tele2 Sverige-arrest werd al geoordeeld dat een vordering van verkeersgegevens door een onafhankelijke autoriteit moet worden gedaan. In het Prokuratuurarrest werd bepaald dat een vordering door een officier van justitie, met daaropvolgend een latere toetsing door een rechter, niet aan dit vereiste voldoet. Hoewel de uitspraak in het Prokuratuurarrest een specifieke zaak betreft, spelende in Estland, kan wel aangenomen worden dat het arrest gevolgen heeft voor de eisen die in zijn algemeenheid gelden wat betreft de autoriteit die toestemming moet verlenen voor de toegang tot de gegevens.

[115] Voor de factoren die het HvJ eerder in aanmerking nam bij het beoordelen van de zwaarte van delicten: zie paragraaf 2.3.2.
[116] Voor ditzelfde uitgangspunt dat verkeersgegevens alleen bij zwaardere misdrijven mogen worden opgevraagd pleiten onder meer Koops 2003, p. 70; Odinot e.a. 2013, p. 145; Koops & Smits 2014, p. 50; Brkan *German Law Journal* 2019, p. 872.

De toegang tot verkeersgegevens verloopt in Nederland volgens de huidige bepalingen via de officier van justitie. Dat in 1971 de officier van justitie werd aangewezen om tijdens het onderzoek inlichtingen te vorderen is niet vreemd in het licht van de toen geldende opvattingen omtrent de rol van de officier als onafhankelijk opererende rechterlijk ambtenaar.[117] De IRT-affaire en de Wet tot wijziging van de Wet op de rechterlijke organisatie[118] brachten echter met zich mee dat de rol van de officier meer en meer in de richting van én leider van het opsporingsonderzoek én "crime fighter" ging opschuiven.[119] Aan het onafhankelijk statuut van de officier van justitie lijkt dus intussen één en ander veranderd te zijn. Daarom is het mijns inziens tegenwoordig niet meer zo dat de officier van justitie de meest aangewezen persoon is voor het doen van een vordering verkeersgegevens: er dient immers een onafhankelijke afweging van het geoorloofd zijn van de privacy-inbreuk gemaakt te worden.[120] De Rechtbank Den Haag stelde overigens al in 2015 vast dat het openbaar ministerie niet als een rechterlijke instantie of onafhankelijke administratieve instantie beschouwd kon worden.[121] Dat achteraf door de rechter getoetst kan worden of de opsporingsbevoegdheid terecht is gebruikt doet daar ook niet aan af.[122]

Sinds de uitspraak in het Prokuratuurarrest worden de betreffende vorderingen in Nederland voorgelegd aan de rechter-commissaris: de artikelen uit het Wetboek van Strafvordering worden daarmee richtlijnconform geïnterpreteerd.[123] De bevoegdheid van de rechter-commissaris om de vorderingen te beoordelen wordt hierbij dus gebaseerd op de e-privacyrichtlijn en de rechtspraak van het Hof van Justitie, maar is nog niet wettelijk geregeld. Totdat het Wetboek van Strafvordering zó is aangepast dat voor het vorderen van

[117] Zie bijvoorbeeld Lindeman 2017, p. 10.
[118] Voluit: Wet tot wijziging van de Wet op de rechterlijke organisatie, het Wetboek van Strafvordering, de Politiewet 1993 en andere wetten, *Stb.* 1999, 194.
[119] Gerding 2011, p. 127. Sinds de IRT-affaire transformeerde het Openbaar Ministerie tot een organisatie met een duidelijk aanwezige centrale leiding: hoe de vervolging dient te verlopen wordt nu landelijk bepaald en de officier van justitie is de gezagsdrager van de opsporing geworden (Lindeman 2017, p. 97; *Kamerstukken II* 1997/98, 25403, nr. 7, p.23).
[120] Zie ook: Toor, van, ehrcupdates 2021, par. 11 "Hoe dan ook, de zelfstandige bevoegdheid van de officier van justitie om bepaalde data van telecommunicatieaanbieders te vorderen, is in strijd de Unierechtelijke privacybescherming".
[121] Rb. Den Haag (vzr.) 11 maart 2015, ECLI:NL:RBDHA:2015:2498, r.o. 3.9 en 3.11.
[122] Concl. A-G G. Pitruzzella, HvJ 21 januari 2020, C-746/18, ECLI:EU:C:2020:18 (*Prokuratuur*), r.o. 128. En dichter bij huis: Van 't Hullenaar stelt dat een toetsing achteraf een onrechtmatige toegang tot de gegevens niet verhindert (Hullenaar, van 't, vcasblog 2021, par. 1); Van Buiten signaleert dat bevoegdheden meestal niet aan bod komen ter terechtzitting als ze geen verbazing wekken of disproportioneel lijken (Van Buiten *DD* 2016, p. 142).
[123] Dit met ingang van 19 augustus 2021, zie Lassche 2021, versie 3.5, p. 35. Te Molder (Molder, te, *DD* 2021/66, p. 866) merkt in dit verband op dat uit de recente rechtspraak ook blijkt dat er in het geval van een relatief kleine privacy-inbreuk wellicht geaccepteerd kan worden dat een officier van justitie zelfstandig toegang verleent tot verkeersgegevens. Dit zou volgen uit de Beslissing van de rechter-commissaris van de Rb. Den Haag 14 september 2021, ECLI:NL:RBDHA:2021:10868.

verkeersgegevens een machtiging van de rechter-commissaris is vereist lijkt mij daarom dat de artikelen 126n, 126u en 126zh Sv strikt gezien niet in overeenstemming zijn met de grondrechten van het Handvest.

4.4 Het vorderen van verkeersgegevens in overeenstemming met het Handvest

Waar dit nodig was voor een bespreking van de mogelijkheid tot het vorderen van verkeersgegevens, of voor een beter begrip van de uitspraken van het HvJ, werden in het voorgaande de vereisten aan het bewaren van verkeersgegevens besproken. Hieruit bleek dat wat de *bewaring* van verkeersgegevens betreft in Nederland voldaan wordt aan de vereisten aan noodzakelijkheid en afbakening. Daarentegen lijken enige aanpassingen van de artikelen 126n, 126u en 126zh noodzakelijk te zijn om recht te doen aan Europeesrechtelijke en nationale jurisprudentie over het *vorderen* van verkeersgegevens. Daarom zal hieronder nader worden ingegaan op de mogelijkheden tot het nader specificeren van deze artikelen. Hierbij zal ook kort aandacht besteed worden aan de manier waarop verkeersgegevens aan de orde komen in de plannen voor het gemoderniseerde Wetboek van Strafvordering.

4.4.1 Opvragen van verkeersgegevens voor het onderzoek “dringend vereist”

Ten eerste zou mijn voorstel zijn het vereiste dat de vordering “in het belang van het onderzoek” gedaan moet worden te vervangen door het vereiste dat het onderzoek “dringend vordert” dat de vordering wordt gedaan. De artikelen sluiten dan wat dit gedeelte betreft meer aan bij de verwante artikelen over het opnemen van telecommunicatie, het onderzoek in geautomatiseerde werken en de vordering tot bewaring gegevens.[124] De regeling zou hiermee eveneens beter dan nu uitdrukken dat het opvragen van verkeersgegevens net zoveel overdenking verdient als het opvragen van de gegevens uit de verwante artikelen.[125]

In de artikelen 2.7.48 en 2.7.50 van het gemoderniseerde Wetboek van Strafvordering wordt het belang van het onderzoek niet meer als voorwaarde voor een vordering van verkeersgegevens genoemd. De memorie van toelichting bij artikel 2.7.48 vermeldt echter wel dat het om “nummers” moet gaan “waarvan het in het belang van het onderzoek is dat de historische gegevens met betrekking tot die nummers worden verkregen.[126] Hiermee lijkt er op het eerste gezicht niets te veranderen ten opzichte van de huidige artikelen 126n en 126u en 126zh. Toch is er in het wetsvoorstel voor het nieuwe wetboek wel een verandering te vinden

[124] Deze zijn geregeld in de artikelen 126l, 126m, 126nba, 126ni, 126s, 126t, 126uba, 126ui, 126zf, 126zg, 126zja en 126zpa Sv.
[125] Vgl. Buiten, van, *DD* 2016, p. 139, die stelt dat dit voorgestelde criterium “een extra (strenge) toets oplevert”.
[126] MvT Wetsvoorstel nieuwe Wetboek van Strafvordering (ambtelijke versie), 2020, p. 437.

die aansluit bij het hiervoor door mij geschetste voorstel: in artikel 2.7.50, tweede lid wordt namelijk bepaald dat het belang van het onderzoek dringend moet vereisen dat gegevens direct na de verwerking (het gaat hier dus om toekomstige gegevens) worden verstrekt. Deze bepaling lijkt wat dit betreft dus meer dan nu aan te sluiten bij de huidige bepalingen over bijvoorbeeld het vorderen van de inhoud van communicatie en ook bij bijvoorbeeld het in het wetsvoorstel genoemde artikel 2.8.13, dat een bevel tot vastlegging van communicatie regelt.

4.4.2 Een ernstige inbreuk op de rechtsorde

Een tweede naar mijn mening aanbevelenswaardige aanpassing zou moeten inhouden dat aan het vereiste van de toegestane voorlopige hechtenis van artikel 126n wordt toegevoegd dat er sprake moet zijn van een misdrijf "dat gezien de aard of de samenhang met andere door verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert". Zoals hierboven in paragraaf 3.2.3 beschreven lijkt het vereiste dat voor een misdrijf voorlopige hechtenis toegelaten moet zijn niet altijd te voldoen wanneer dit wordt afgezet tegen het vereiste van het "ernstige strafbare feit" dat voortkomt uit het Handvest. Door het vereiste van de ernstige inbreuk op de rechtsorde in artikel 126n te verwerken valt mijns inziens duidelijker dan nu het geval is vast te stellen of de toegang tot verkeersgegevens nodig is voor de bestrijding van ernstige criminaliteit.[127]

In de memorie van toelichting bij de Wet bob valt te lezen dat het bij misdrijven die gezien hun aard of hun samenhang een ernstige inbreuk op de rechtsorde opleveren (een voorwaarde voor infiltratie, een telefoontap en het opnemen van communicatie) kan gaan om "handel in drugs, mensenhandel, omvangrijke milieudelicten, wapenhandel en omvangrijke ernstige fraude". Ook van bijvoorbeeld een 's nachts gepleegde woninginbraak of een kleinere fraudezaak waarvan vermoed wordt dat deze deel uitmaakt van een grotere kan gezegd worden dat zij een ernstige inbreuk op de rechtsorde vormen, doordat ze door hun omvang en gevolgen de samenleving schokken. Een misdrijf dat in combinatie met een ander misdrijf gepleegd is kan dit ook bewerkstelligen, aldus de memorie van toelichting.[128] De concrete feiten en omstandigheden bij het gepleegde of beraamde het misdrijf zijn dus ook van belang.

[127] In artikel 126u is dit vereiste al wel opgenomen, via artikel 126o, in artikel 126zh zijn "aanwijzingen van een terroristisch misdrijf" vereist. Advocaat-generaal Keulen signaleert overigens dat de Rechtbank Rotterdam in een vonnis van april 2021 zelf uit het Prokuratuurarrest afleidt dat een vordering van verkeersgegevens alleen toegestaan is als er sprake is van een voorlopige hechtenis-feit dat "gezien zijn aard of de samenhang met andere door verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert". Zie Concl. A-G B.F. Keulen 14 december 2021, ECLI:NL:PHR:2021:1179, r.o. 6.
[128] Kamerstukken II 1996/97, nr. 3, p. 24-25.

In een conclusie uit 2013 legt de advocaat-generaal nader de inhoud van het vereiste van de ernstige inbreuk op de rechtsorde uit: bij het beoordelen of daaraan voldaan wordt gaat het om de vraag "of het, in het licht van de omstandigheden van het geval, een zwaar genoeg feit betreft bezien naar de klaarblijkelijk heersende rechtsovertuiging in de samenleving". Er wordt hierbij aangegeven dat de heersende rechtsovertuiging in de samenleving ervoor kan zorgen - sneller dan wellicht gedacht - dat een feit zwaar genoeg is om onder het "ernstige inbreuk"-criterium te vallen.[129] Een invoering van dit vereiste zou er daarom mijns inziens niet toe hoeven te leiden dat er voor minder misdrijven een vordering verkeersgegevens is toegestaan. Wél wordt het nader beschouwen van de concrete feiten en omstandigheden van een misdrijf er waarschijnlijk belangrijker door, wat van invloed kan zijn op de afweging om al dan niet over te gaan tot de vordering. Een artikel 126n met daarin opgenomen het vereiste van de ernstige inbreuk op de rechtsorde zou naar mijn mening dan ook tot gevolg hebben dat deze bepaling meer in lijn komt met de rechtspraak van het HvJ over de privacy-grondrechten uit het Handvest.[130]

Overigens lijkt het erop dat er in het gemoderniseerde Wetboek van Strafvordering wat betreft de zwaarte van het misdrijf geen nieuwe eisen gesteld zullen gaan worden.[131] Uit de memorie van toelichting bij de artikelen 2.7.48 en 2.7.50, die het opvragen van respectievelijk de historische en de toekomstige verkeersgegevens regelen, blijkt dat het voorlopige hechtenis-criterium zal worden losgelaten en dat daarvoor in de plaats het criterium komt van een verdenking van een misdrijf waarop een gevangenisstraf van vier jaar of meer is gesteld.[132] Omdat het nieuwe wetboek ook een lijst van lichtere misdrijven gaat bevatten die worden gelijkgesteld aan de "4-jaar-of-meer-misdrijven" zal de materiële uitwerking van deze wijziging in feite niet voor een verandering zorgen, aldus de memorie.[133]

[129] Concl. A-G A.E. Harteveld 17 december 2013, ECLI:NL:PHR:2013:2696, r.o. 4.6 en 4.7.
[130] Anders: Concl. A-G B.F. Keulen 14 december 2021, ECLI:NL:PHR:2021:1179, r.o. 87. De A-G stelt dat indien de Hoge Raad oordeelt dat het volgens het HvJ aan de nationale rechter is om te bepalen wat er onder het begrip "ernstige strafbare feiten" valt, de huidige wettelijke bepalingen voldoende verzekeren dat verkeers- en locatiegegevens alleen in het geval van ernstige strafbare feiten gevorderd mogen worden.
[131] In het gemoderniseerde wetboek geldt ook weer het uitgangspunt dat hoe meer het opvragen van een bepaalde soort gegevens als ingrijpend wordt gezien, hoe zwaarder de eisen en hoe "hoger" de autoriteit die toestemming geeft moeten zijn. Het HvJ neemt echter bij het bepalen van de ingrijpendheid van een inbreuk niet alleen de soort gegevens in ogenschouw, en het gaat niet uit van het idee dat bepaalde soorten gegevens per definitie een ernstiger inbreuk maken op het recht op privacy dan andere. En vraag die hierbij gesteld kan worden is of de Nederlandse wetgever dan wel moet vasthouden aan de huidige wijze van normering, waarbij de mate van rechtsbescherming afhangt van louter het soort gegevens. Zie Molder, te, *DD* 2021/66, p. 868; *Rapport Commissie-Koops* 2018, p. 128-129.
[132] MvT Wetsvoorstel nieuwe Wetboek van Strafvordering (ambtelijke versie), 2020, p. 432.
[133] MvT Wetsvoorstel nieuwe Wetboek van Strafvordering (ambtelijke versie), 2020, p. 253.

4.4.3 Machtiging van de rechter-commissaris vereist

Ten derde en laatste zou de wetgever mijns inziens de artikelen 126n, 126u en 126zh zó moeten aanpassen dat er een machtiging van de rechter-commissaris vereist is voordat verkeersgegevens gevorderd mogen worden. Dit zou inhouden dat de werkwijze zoals die sinds de augustus 2021 feitelijk wordt toegepast in een wettelijke regel wordt opgenomen en dat wordt beantwoord aan het Europeesrechtelijke vereiste van de onafhankelijk instantie die toeziet op de toegang tot verkeersgegevens.[134]

In de memorie van toelichting bij het wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering wordt in de artikelen 2.7.48 en 2.7.50 de officier van justitie nog genoemd als degene die de bevoegdheid heeft om te bevelen gegevens te verstrekken; wellicht niet verwonderlijk omdat de ambtelijke versie van het wetsvoorstel dateert van vóór het Prokuratuurarrest.[135] Ook in de memorie van toelichting bij het gemoderniseerde wetboek wordt weer opgemerkt dat de officier van justitie leiding geeft aan het opsporingsonderzoek en dat het gevolg daarvan moet zijn dat de rechter-commissaris daaruit terugtreedt.[136]

Te Molder merkt op dat er ook iets te zeggen zou zijn voor het in het leven roepen van een nieuwe onafhankelijke autoriteit die de machtiging voor het opvragen van verkeersgegevens verleent. Op die manier zouden enerzijds de kabinetten rechter-commissaris ontlast worden en anderzijds zou deze autoriteit ook toezicht kunnen houden op de andere bevoegdheden die spelen als er digitale gegevens worden verzameld. Zij signaleert dat dit er ook toe zou kunnen bijdragen dat voldaan wordt aan het derde lid van artikel 8 van het Handvest, dat bepaalt dat er een onafhankelijk toezicht op het verwerken van gegevens moet zijn.[137] Ook Revolidis en Van Toor zien wel de voordelen van een dergelijke onafhankelijke autoriteit.[138]

---

[134] A-G Keulen stelt dat er vooruitlopend op een eventuele wetswijziging al een rechtsbasis bestaat die de inschakeling van de rechter-commissaris mogelijk maakt. Indien dit voor de evenwichtigheid en rechtmatigheid van het vooronderzoek geboden is, mag een officier van justitie ook nu al een machtiging van de rechter-commissaris vorderen. Kort gezegd ziet hij daarmee al in de wet besloten liggen dat de rechter-commissaris de bevoegdheid heeft "ook buiten de expliciet in de wet geregelde gevallen toepassing van een bijzondere opsporingsbevoegdheid te bewerkstelligen" (Concl. A-G B.F. Keulen 14 december 2021, ECLI:NL:PHR:2021:1179, r.o. 117-127).

[135] MvT Wetsvoorstel nieuwe Wetboek van Strafvordering (ambtelijke versie), 2020, resp. p. 437 en 239. Anderzijds luidde de conclusie van de advocaat generaal in de zaak Prokuratuur al in 21 januari 2020 "dat niet is voldaan aan de eis dat de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens wordt onderworpen aan een voorafgaand toezicht door een rechterlijke instantie of een onafhankelijke bestuurlijke autoriteit wanneer een nationale regeling bepaalt dat een dergelijk toezicht wordt uitgeoefend door het openbaar ministerie dat als taak heeft het opsporingsonderzoek te leiden, maar ook in rechte kan optreden als openbaar aanklager" (Concl. A-G G. Pitruzzella, HvJ 21 januari 2020, C-746/18, ECLI:EU:C:2020:18 (*Prokuratuur*), r.o. 130).

[136] MvT Wetsvoorstel nieuwe Wetboek van Strafvordering (ambtelijke versie), 2020, p. 15.

[137] Molder, te, *DD* 2021/66, p. 867.

[138] Revolidis, *European Data Protection Law Review* 2020, p. 324; Van Toor, van, ehrcupdates 2021, par. 6.

Of een zo'n autoriteit bestaansrecht heeft zou naar mijn mening zeker onderzocht moeten worden. Het vorderen en gebruiken van verkeersgegevens vormt al lang geen lichte inbreuk meer en nieuwe technologieën zorgen voor steeds weer nieuwe ontwikkelingen. De algemene bewaarplicht voor verkeersgegevens die tussen 2009 en 2015 gold betrof bijvoorbeeld nog geen gegevens van diensten als Skype, Google en Whatsapp. Het is echter goed voorstelbaar dat een nieuwe Wet bewaarplicht - in welke vorm dan ook - ook over deze communicatiediensten zal gaan: het toepassingsbereik in de Telecommunicatiewet van wat als een "aanbieder van een elektronische communicatiedienst" wordt beschouwd is inmiddels al verruimd, zodat dergelijke diensten er ook onder vallen.[139] Het instellen van een nieuwe autoriteit die zich zowel onafhankelijk bezighoudt met machtigingen voor het vorderen van verkeersgegevens als met andere bevoegdheden waarbij zeer uiteenlopende (elektronische) persoonsgegevens in het spel zijn zou daarom een zinvolle en toekomstbestendige optie kunnen zijn.

De hiervoor voorgestelde wijzigingen nemen overigens het probleem niet weg van de zeer beperkte mogelijkheid tot het bewaren van gegevens. Een bespreking van dit probleem valt echter buiten de scope van de onderzoeksvraag van deze scriptie. Afgaande op zijn brief over het Wetsvoorstel aanpassing bewaarplicht telecommunicatiegegevens lijkt de minister toe te willen naar een algemene bewaring van locatie- en gebruikersgegevens.[140] In verband met onder andere een nader uit te voeren onderzoek naar - kort samengevat - het privacyprobleem dat ontstaat als meerdere gebruikers één IP-adres gebruiken is het proces van de wetswijziging echter vertraagd geraakt.[141] Tot zeer recent (januari 2022) heeft het wetsvoorstel daarnaast op de lijst van controversiële onderwerpen gestaan, waarvan de behandeling aangehouden werd tot het aantreden van een nieuw kabinet.[142]

[139] Oerlemans, Hagens & Royer, *Computerrecht* 2021/59, p. 153. Het Wetsvoorstel tot Wijziging van de Telecommunicatiewet in verband met de implementatie van Richtlijn (EU) 2018/1972 is op 28 oktober 2021 aangenomen. Zie *Kamerstukken II* 2020/21, 35865, nr. 2, p. 3 en 4 voor de hierboven besproken wijziging.
[140] *Kamerstukken II*, 2017/18, 34537, nr. 7, p. 7-8.
[141] *Kamerstukken II*, 2017/18, 34537, nr. 8. Het onderzoek is intussen uitgevoerd. Zie: T. van der Vorst, e.a. 2019, p. 9.
[142] *Kamerstukken II*, 2020/21, 35718, nr. 90.

HOOFDSTUK 5: CONCLUSIE

In het voorgaande werd onderzocht of het gebruik van verkeersgegevens zoals bedoeld in de artikelen 126n, 126u en 126zh Sv nog kan worden toegestaan in strafrechtelijk onderzoek, gelet op de artikelen 7 en 8 van het Handvest.

Verkeersgegevens - digitale gegevens van telecomaanbieders die géén betrekking hebben op de inhoud van de communicatie - bleken in beperkte vorm en voor een beperkte duur bewaard te mogen worden. Een officier van justitie mag deze gegevens op grond van de artikelen 126n, 126u en 126zh Sv vorderen, mits wordt voldaan aan de in deze artikelen opgesomde vereisten. Het vorderen van de gegevens is toegestaan ondanks de "garantie van vertrouwelijkheid" die erop rust: telecomaanbieders mogen op grond van de Telecommunicatiewet de vertrouwelijkheid namelijk doorbreken als dit noodzakelijk is in het belang van de voorkoming, opsporing en vervolging van strafbare feiten.

De artikelen 7 en 8 van het Handvest beperken de ruimte voor het verwerken én voor het gebruiken van persoonlijke gegevens ten behoeve van strafrechtelijk onderzoek. Daarom werd vervolgens in hoofdstuk 3 besproken volgens welke criteria de rechten uit deze artikelen ingeperkt mogen worden als er verkeersgegevens gevorderd worden. Uit artikel 52, eerste lid Handvest werden drie vereisten onderscheiden waaraan een beperking van een recht getoetst diende te worden. Het betrof het vereiste van het "gesteld zijn bij wet", het vereiste dat de beperking in een bepaalde rechtvaardigings-categorie valt en het zogenaamde proportionaliteitsvereiste: het vereiste dat de beperking evenredig en noodzakelijk is en de essentie van het recht eerbiedigt. Met name het laatste vereiste werd nader uitgewerkt, waarbij een overzicht werd gegeven van de toepassing ervan in de Europese en nationale rechtspraak betreffende het bewaren, en vooral, het gebruiken van verkeersgegevens.

Opvallend in de Europese uitspraken over verkeersgegevens was dat het HvJ het gebruiken van die soort gegevens op lijkt te delen in enerzijds het bewaren en anderzijds het verkrijgen van toegang. Daarnaast viel in de recente jurisprudentie die het gebruik van verkeersgegevens betreft een drietal belangrijke punten op waaraan het HvJ toetst of aan het proportionaliteitsvereiste voldaan is: ten eerste moet de beperking op de grondrechten van artikel 7 en 8 Handvest noodzakelijk zijn voor het te realiseren doel, ten tweede moet er sprake zijn van een ernstig misdrijf, en ten derde moet een onafhankelijk autoriteit voorafgaand toestemming geven voor het gebruik van de gegevens. Dit laatste omdat op onafhankelijk wijze vastgesteld dient te worden of een inbreuk op de privacy wel geoorloofd is.

In hoofdstuk 4 werd de Nederlandse regeling voor het gebruik van verkeersgegevens getoetst aan een combinatie van de hierboven genoemde criteria. Eerst werd aandacht besteed aan de vereisten dat de beperking bij wet gesteld moet zijn en een doelstelling van algemeen belang dient. Vervolgens kwam de proportionaliteitstoets aan de orde, waarbij met name de Europese jurisprudentie op dit gebied betrokken werd. Geconcludeerd werd dat aan de eerste twee vereisten wordt voldaan. Meer problemen werden gesignaleerd bij het toetsen van de Nederlandse wetgeving aan het proportionaliteitsvereiste. Hoewel geconcludeerd werd dat de bewaring van verkeersgegeven in overeenstemming met het Handvest plaatsvindt werden er vraagtekens bij geplaatst of de toegang tot de gegevens in overeenstemming verloopt met de uitleg van het Handvest. De strikte noodzakelijkheid die er voor de toegang dient te bestaan lijkt immers niet te volgen uit de zinssnede in de Nederlandse regeling dat een vordering verkeersgegevens "in het belang van het onderzoek" moet zijn. Daarnaast volgde uit de proportionaliteitstoets dat niet alle strafbare feiten die onder de voorlopige hechtenis-feiten vallen beschouwd kunnen worden als ernstig genoeg - naar de maatstaven van het HvJ - voor een ingrijpende bevoegdheid als het vorderen van verkeersgegevens. Volgens de Nederlandse wet is voorlopige hechtenis immers ook voor een aantal minder zware misdrijven toegestaan. Als derde en laatste werd vastgesteld dat vorderingen tot het verstrekken van verkeersgegevens sinds het Prokuratuurarrest in Nederland worden voorgelegd aan de rechter-commissaris. Er werd geconcludeerd dat de huidige regeling daarmee strikt gezien echter niet voldoet aan het vereiste van een onafhankelijke weging van de privacy-inbreuk.

In de laatste paragraaf van hoofdstuk 4 werden enkele suggesties voor aanpassingen gedaan om de artikelen in overeenstemming met het Handvest te brengen De eerste suggestie hield in dat het vereiste dat de vordering "in het belang van het onderzoek" gedaan moet worden vervangen zou moeten worden door het vereiste dat het onderzoek "dringend vordert" dat de vordering wordt gedaan. Op deze wijze zou de regeling beter kunnen waarborgen dat niet strikt noodzakelijk privacy-inbreuken ook met betrekking tot de steeds veelzeggender wordende verkeersgegevens voorkomen worden. Een tweede voorgestelde aanpassing was dat aan het vereiste van de toegestane voorlopige hechtenis van artikel 126n wordt toegevoegd dat er sprake moet zijn van een misdrijf "dat gezien de aard of de samenhang met andere door verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert". Hierdoor valt immers duidelijker dan nu het geval is vast te stellen of om de toegang tot verkeersgegevens verzocht wordt voor de bestrijding van ernstige criminaliteit. Als laatste werd gesignaleerd dat de wetgever de artikelen 126n, 126u en 126zh zou moeten aanpassen in die zin dat er een machtiging van de rechter-commissaris vereist is voordat verkeersgegevens gevorderd mogen

worden. Ook werd als wellicht nader te onderzoeken mogelijkheid genoemd dat er een onafhankelijke instantie voor het verstrekken van deze machtigingen in het leven zou worden geroepen. Buiten het bereik van dit onderzoek viel de problematiek van de momenteel slechts zeer beperkte mogelijkheid tot het bewaren van verkeersgegevens.

Op grond van de toetsing en de voorgestelde aanpassingen in het voorgaande zou ik willen stellen dat het probleem van de weinig specifieke bewoordingen in de verkeersgegevens-artikelen als het om de strikte noodzaak van de vordering gaat eventueel ondervangen zou kunnen worden door bij de beoordeling hiervan de lijn te volgen van de vereisten zoals die volgen uit de artikelen 7 en 8 van het Handvest en de bijbehorende jurisprudentie. Het concept "belang van het onderzoek" biedt daartoe mijns inziens wel ruimte. Wat betreft de vereisten aan de zwaarte van het misdrijf en aan de autoriteit die de machtiging voor het opvragen van verkeersgegevens mag afgeven is dit anders. Het gebruik van verkeersgegevens is door het ontbreken van eenduidige vereisten aan de ernst van het misdrijf en van een onafhankelijke autoriteit die de toegang tot de gegevens regelt immers gewoonweg niet in overeenstemming met de Europeesrechtelijke vereisten.

Als antwoord op de onderzoeksvraag zou ik dan ook willen concluderen dat het gebruik van verkeersgegevens in strafrechtelijk onderzoek op de wijze als bepaald in de artikelen 126n, 126u en 126zh Sv gelet op de artikelen 7 en 8 van het Handvest niet meer kan worden toegestaan, omdat de regeling niet voldoet aan de proportionaliteitsvereisten die aan de orde zijn in het geval van wetgeving die een inbreuk maakt op de Europese grondrechten. Hoe graag wij in de Westerse maatschappij ook alles uit de kast halen om onze veiligheid te garanderen en hoezeer wij ook van nature geneigd zijn om ook op dit gebied mee te gaan in - om met de filosoof Foucault te spreken - de "verhoging van de productiviteit van de macht", onze regelgeving over het gebruik van verkeersgegevens zal moeten meebewegen met de door technologische ontwikkelingen veranderde status ervan en de Unierechtelijke eisen aan de waarborgen in nationale regelingen moeten incorporeren.[143] In het traject van de modernisering van het Wetboek van Strafvordering**,** door middel van spoedwetgeving of door een uitvoeringswet van wellicht nog te realiseren Europese verordeningen: op enigerlei wijze zullen deze ontwikkelingen en eisen in de nabije toekomst hun plaats moeten vinden in het Nederlandse Wetboek van Strafvordering.

[143] Foucault 1989, p. 287.

GERAADPLEEGDE LITERATUUR, JURISPRUDENTIE EN STUKKEN

Boeken, tijdschriften en weblogs

Blom, in: *T&C Strafvordering*

T. Blom, commentaar op art. 126n Sv, in: C.P.M. Cleiren, M.J.M. Verpalen & J.H. Crijns (red.), *Tekst & Commentaar Strafvordering*, Deventer: Wolters Kluwer.

Bokhorst, Kogel, de & Meij van der 2002

R.J. Bokhorst, C.H. de Kogel & C.F.M. van der Meij, *Evaluatie van de Wet BOB – fase 1. De eerste praktijkervaringen met de Wet Bijzondere opsporingsbevoegdheden* (rapport WODC), Meppel: Boom Juridische uitgevers 2002.

Brkan, *German Law Journal* 2019, p. 864-883

M. Brkan, 'The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning', *German Law Journal* 2019, afl. 6, p. 864-883.

Brkan & Imamović 2020

M. Brkan & Š. Imamović, 'Article 52: Twenty-Eight Shades of Interpretation?', in: M. Bobek & J. Adams-Prassl (red.), *The EU Charter of Fundamental Rights in the Member States*, Londen: Hart Publishing 2020, hfdst. 22 (digitaal geraadpleegd).

Buiten, van, *DD* 2016, p. 130-144

N. van Buiten, 'De modernisering van de Wet BOB - Herinneren we ons de IRT-affaire nog?', *DD* 2016, afl. 10, p. 130-144.

Bulterman 2015

M. Bulterman, 'Ontwikkelingen in de Luxemburgse rechtspraak', in: J. Gerards, H. de Waele & K. Zwaan (red.), *Vijf jaar bindend EU-Grondrechtenhandvest*, Deventer: Wolters Kluwer 2015, p. 55-80.

Careel & Royer, *P&I* 2020, p. 269-272

S. Careel & S. Royer, 'Bewaart Hof van Justitie evenwicht tussen veiligheid en privacy in nieuwe dataretentie-arresten?', *P&I* 2020, afl. 6, p. 269-272.

Danwitz, von, 2012

T. von Danwitz, 'Thoughts on Proportionality and Coherence in the Jurisprudence of the Court of Justice', in: P. Cardonnel, A. Rosas & N. Wahl, *Constitutionalising the EU Judicicial System: Essays in Honour of Pernilla Lindh*, Oxford and Portland OR: Hart 2012, p. 367-382.

Falot & Hijmans, *NtEr* 2017, p. 44-52

Falot, N. & Hijmans, H., 'Tele2: de afweging tussen privacy en veiligheid nader omlijnd', *NtEr* 2017, afl. 3, p. 44-52.

Ferdinandusse, Hendriks & Laheij 2015

W.N. Ferdinandusse, J.C. Hendriks & D. Laheij, *De bewaarplicht telecomgegevens en de opsporing. Het belang van historische telecommunicatiegegevens voor de opsporing*, bijlage bij *Kamerstukken II* 2014/2015, 33870, nr. 3.

Foucault 1989

M. Foucault, *Discipline, toezicht en straf: de geboorte van de gevangenis*, Groningen: Historische Uitgeverij 1989.

Gerards, *European Law Journal* 2001, p. 80-120

J. Gerards, 'Pluralism, Deference and the Margin of Appreciation Doctrine', *European Law Journal* 2011, afl. 1, p. 80-120.

Gerding 2011

R.A.F. Gerding, 'Het Openbaar Ministerie in de periode 1950-1999. Turbulentie', in: A.G. Bosch e.a. (red.), Twee eeuwen openbaar ministerie 1811-2011, Den Haag: Sdu Uitgevers/openbaar ministerie 2011, p. 115-146.

Hullenaar, van 't, vcasblog 2021

S.F.W. van 't Hullenaar, 'Onderzoek in smartphones: klare taal gewenst', vcasblog, 24 maart 2021.

Knol, *in: T&C Privacy- en gegevensbeschermingsrecht*

P.C. Knol, commentaar op art. 13.2a Telecommunicatiewet, in: G.J. Zwenne & H.R. Kranenborg (red.), *Tekst & Commentaar Privacy- en gegevensbeschermingsrecht,* Deventer: Wolters Kluwer.

Koning 2015

M. Koning, 'Het recht op bescherming van persoonsgegevens in de Europese en nationale rechtsorde na Lissabon', in: J. Gerards, H. de Waele & K. Zwaan (red.), *Vijf jaar bindend EU-Grondrechtenhandvest,* Deventer: Wolters Kluwer 2015, p. 351-385.

Koops 2003

B.J. Koops, 'Verkeersgegevens en strafrecht: een agenda voor discussie', in: L. F. Asscher & A.H. Ekker (red.), *Verkeersgegevens. Een juridische en technische inventarisatie,* Amsterdam: Otto Cramwinckel 2003, p. 59-92.

Koops & Smits 2014

B.J. Koops & J.M. Smits, *Verkeersgegevens en artikel 13 Grondwet. Een technische en juridische analyse van het onderscheid tussen verkeersgegevens en inhoud van communicatie,* Oisterwijk: WLP 2014.

Kumm, *International Journal of Constitutional Law* 2004, p. 574–596

M. Kumm, 'Constitutional Rights as Principles: On the Structure and Domain of Constitutional Justice. A Review Essay on a Theory of Constitutional Rights', *International Journal of Constitutional Law* 2004, afl. 2, p. 574–596.

Lassche 2021, versie 3.5

H. Lassche, *Digitalisering en de opsporingspraktijk Juridische aspecten,* Apeldoorn: Politieacademie 2021 (online: versie 3.5).

Lenaerts, *ECLR* 2012, p. 375-403

K. Lenaerts, 'Exploring the Limits of the EU Charter of Fundamental Rights', *ECLR* 2012, afl. 8, p. 375-403.

Lindeman 2017

J. M. W. Lindeman, *Officieren van justitie in de 21e eeuw* (diss. Universiteit Utrecht), Den Haag: Boom juridisch 2017

***Study on the retention of electronic communications non-content data* 2020**

Study on the retention of electronic communications non-content data for law enforcement purposes (rapport van september 2020 in opdracht van de Europese Commissie, departement Migratie en Binnenlandse Zaken), Luxemburg: Publications Office of the European Union, 2020 (online publiek).

Mol, de, Pahladsingh & Heijningen, van, *SEW* 2012, p. 222-236

M. de Mol, A. Pahladsingh & L.R. van Heijningen, 'Inroepbaarheid in rechte van het Handvest van de Grondrechten van de Europese Unie: Toepassingsgebied en het onderscheid tussen 'rechten' en 'beginselen'', *SEW* 2012, afl. 6, p. 222-236.

Molder, te, *DD* 2021/66

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, afl. 9, p. 844-869.

Møller Pedersen, Udsen & Sandfeld Jakobsen, *International Data Privacy Law* 2018, p. 160-174

A. Møller Pedersen, H. Udsen & S. Sandfeld Jakobsen, 'Data retention in Europe- the Tele 2 case and beyond', *International Data Privacy Law* 2018, Afl. 8, nr. 2, p. 160-174.

Odinot e.a. 2013

Odinot e.a., *De Wet bewaarplicht telecommunicatiegegevens. Over het bewaren en gebruiken van gegevens over telefoon- en internetverkeer ten behoeve van de opsporing* (rapport WODC), Den Haag: Boom Lemma Uitgevers 2013.

Oerlemans & Hagens, *JBP* 2021/1, p. 31-36

J.J. Oerlemans & M. Hagens, Annotatie bij HvJ 6 oktober 2020, C-623/17, ECLI:EU:C:2020:790 (*Privacy International*) en HvJ 6 oktober 2020, gev. zaken C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net*), Jurisprudentie

Bescherming Persoonsgegevens, Sdu OpMaat (online: opmaat.sdu.nl), 15 maart 2021, afl.1, p. 31-36.

Oerlemans, Hagens & Royer, *Computerrecht* 2021/59

J.J. Oerlemans, M. Hagens & S. Royer, 'Tijd voor een nieuwe bewaarplicht?', *Computerrecht* 2021/59, afl. 2, p. 151-159.

Peers e.a. 2014

S. Peers e.a. (red.), *The EU Charter of Fundamental Rights. A Commentary,* Portland: Hart Publishing 2014.

***Rapport Commissie-Koops* 2018**

Commissie modernisering opsporingsonderzoek in het digitale tijdperk (Commissie-Koops), *Regulering van opsporingsbevoegdheden in een digitale omgeving*, s.l. 2018 (online publiek).

Revolidis, *European Data Protection Law Review* 2020, p. 319-324

I. Revolidis, 'H.K. v Prokuratuur: On Balancing Crime Investigation and Data Protection', *European Data Protection Law Review* 2020, afl. 2, p. 319-324.

Toor, van, ehrcupdates 2021

D.A.G. van Toor, annotatie bij HvJ EU, 2 maart 2021, C-746/18, ECLI:EU:C:2021:152, ehrcupdates, 10 mei 2021.

Vorst, van der, e.a. 2019

T. van der Vorst, e.a., *Mogelijkheden voor identificatie op internet op basis van IP-adres* (rapport in opdracht van het Ministerie van Justitie en Veiligheid), Den Haag: Dialogic Innovatie en Interactie/WODC 2019.

Wissels & Pahladsingh 2020

C. Wissels & A. Pahladsingh, 'The Netherlands: The New Kid on the Block: Growing Pains or Growing Gains?', in: M. Bobek & J. Adams-Prassl (red.), *The EU Charter of Fundamental Rights in the Member States*, Londen: Hart Publishing 2020, hfdst. 12 (digitaal geraadpleegd).

Jurisprudentie

EHRM 7 februari 2012, ECLI:CE:ECHR:2012:0207JUD004066008 *(Von Hannover/Duitsland II).*

HvJ EG 13 juli 1989, C 5/88, ECLI:EU:C:1989:321 (*Wachauf*).
HvJ 8 april 2014, gev. zaken C-293/12 en C-594/12, ECLI:EU:C:2014:238 *(Digital Rights Ireland en Seitlinger e.a*).
HvJ 6 oktober 2015, C-362/14, ECLI:EU:C:2015:650 (*Schrems*).
HvJ 21 december 2016, gev. zaken C-203/15 en C-698/15, ECLI:EU:C:2016:970 (*Tele2 Sverige*).
Concl. A-G H. Saugmandsgaard Øe, HvJ 3 mei 2018, C-207/16, ECLI:EU:C:2018:300 (*Ministerio Fiscal*).
HvJ 2 oktober 2018, C-207/16, ECLI:EU:C:2018:788 (*Ministerio Fiscal*).
HvJ 27 mei 2019, gev. zaken C-508/18 en C-82/19 PPU, ECLI:EU:C:2019:456 (*OG en PI*).
Concl. A-G G. Pitruzzella, HvJ 21 januari 2020, C-746/18, ECLI:EU:C:2020:18 (*Prokuratuur*).
HvJ 6 oktober 2020, C-623/17, ECLI:EU:C:2020:790 (*Privacy International*).
HvJ 6 oktober 2020, gev. zaken C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net*).
HvJ 24 november 2020, C-510/19), ECLI:EU:C:2020:953 (*AZ*).
HvJ 2 maart 2021, C-746/18, ECLI:EU:C:2021:152 (*Prokuratuur*).

HR 7 april 1998, ECLI:NL:HR:1998:ZD1002.
Concl. A-G A.E. Harteveld 17 december 2013, ECLI:NL:PHR:2013:2696.
Concl. A-G F.W. Bleichrodt 8 april 2014, ECLI:NL:PHR:2014:633.
Concl. A-G B.F. Keulen 14 december 2021, ECLI:NL:PHR:2021:1179.

Hof Arnhem-Leeuwarden 24 januari 2012, ECLI:NL:GHARN:2012:BV3076.
Hof ’s Hertogenbosch 20 juni 2013 ECLI:NL:GHSHE:2013:2579.
Hof ’s Hertogenbosch 15 augustus 2013, ECLI:NL:GHSHE:2013:4046.
Hof Amsterdam 9 mei 2014, ECLI:NL:GHAMS:2014:1835.
Hof Arnhem-Leeuwarden 12 juni 2015, ECLI:NL:GHARL:2015:4335.
Hof Arnhem-Leeuwarden 28 juni 2021, ECLI:NL:GHARL:2021:6245.
Hof Den Haag 20 juli 2021, ECLI:NL:GHDHA:2021:1588.
Hof Amsterdam 8 oktober 2021, ECLI:NL:GHAMS:2021:2863.

Rb. ’s Hertogenbosch 15 oktober 2007, ECLI:NL:RBSHE:2007:BB6088.
Rb. Amsterdam 8 maart 2011, ECLI:NL:RBAMS:2011:BP7233.
Rb. Arnhem 22 april 2011, ECLI:NL:RBARN:2011:BQ2163.
Rb. Roermond 2 november 2011, ECLI:NL:RBROE:2009:BK199.
Rb. Den Haag (vzr.) 11 maart 2015, ECLI:NL:RBDHA:2015:2498.
Rb. Limburg 9 december 2015, ECLI:NL:RBLIM:2015:10222.
Rb. Amsterdam 20 juli 2017, ECLI:NL:RBAMS:2017:5130.
Rb. Noord-Holland 20 juli 2017, ECLI:NL:RBNHO:2017:6175.
Rb. Noord-Holland 16 mei 2019, ECLI:NL:RBNHO:2019:4280
Rb. Midden-Nederland 6 maart 2020, ECLI:NL:RBMNE:2020:853.
Rb. Rotterdam 30 april 2021, ECLI:NL:RBROT:2021:3906
Rb. Rotterdam 27 mei 2021, ECLI:NL:RBROT:2021:4427.
Rb. Midden-Nederland 20 augustus 2021, ECLI:NL:RBMNE:2021:3965.
Rb. Oost-Brabant 15 september 2021, ECLI:NL:RBOBR:2021:4986.

Parlementaire stukken

Kamerstukken II 1992/93, 23047, nr. 3.
Kamerstukken II 1996/97, 25403, nr. 3.
Kamerstukken II 1997/98, 25403, nr. 7.
Kamerstukken II 2001/02, 28059, nr. 3 en 5.
Kamerstukken II 2002/03, 28851, nr. 3.
Kamerstukken II 2003/04, 29441, nr. 3.
Kamerstukken II 2014/15, 33542, nr. 17.
Kamerstukken II, 2017/18, 34537, nr. 2, 7 en 8.
Kamerstukken II, 2020/21, 35718, nr. 90.
Kamerstukken II 2020/21, 35865, nr. 2.

Memorie van toelichting bij het Wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering (ambtelijke versie), juli 2020.

BIJLAGE BIJ HOOFDSTUK 2

In artikel 2 van het Besluit vorderen gegevens telecommunicatie worden de volgende gegevens concreet aangewezen als gegevens in de zin van artikel 126n, artikel 126u en artikel 126zh:

a. de naam, het adres en de woonplaats van de gebruiker;

b. de nummers van de gebruiker;

c. de naam, het adres, de woonplaats en het nummer van de natuurlijke persoon of rechtspersoon met wie de gebruiker verbinding heeft, heeft gehad of heeft getracht tot stand te brengen, of van de natuurlijke persoon of rechtspersoon die heeft getracht met de gebruiker verbinding tot stand te brengen;

d. de datum en het tijdstip waarop de verbinding met de gebruiker tot stand is gebracht en beëindigd en de duur van de verbinding, dan wel, ingeval er geen verbinding tot stand is gekomen, de datum en het tijdstip waarop is getracht verbinding met de gebruiker tot stand te brengen, alsmede de afwijking van dit tijdstip van de wettelijke tijd, bedoeld in artikel 1, eerste lid, van de wet van 16 juli 1958 tot nadere regeling van de wettelijke tijd (*Stb.* 352);

e. de locatiegegevens van het netwerkaansluitpunt dan wel gegevens betreffende de geografische positie van de randapparatuur van een gebruiker ingeval van een verbinding of poging daartoe;

f. de nummers van de randapparatuur waarvan de gebruiker gebruik maakt of heeft gemaakt;

g. de soorten diensten waarvan de gebruiker gebruik maakt of heeft gemaakt evenals de daarbij behorende gegevens;

h. de naam, het adres en de woonplaats van degene die de rekening betaalt voor de openbare telecommunicatiediensten en telecommunicatienetwerken die de gebruiker ter beschikking heeft of heeft gehad, indien deze een ander is dan de gebruiker.