De vordering tot uitlevering van gegevens: onbegrensd?

*mr. F. Mattheijer**

1. Inleiding

Door mondialisering en digitalisering van het bedrijfsleven, hebben Nederlandse ondernemingen steeds vaker toegang tot bedrijfsinformatie die uitsluitend in het buitenland is opgeslagen. Hierbij kan bijvoorbeeld worden gedacht aan een e-mail of een scan van een factuur die digitaal kan worden geraadpleegd, maar die geen deel uitmaakt van de fysieke administratie in Nederland en uitsluitend is opgeslagen op een server in het buitenland. Ik zal dit soort gegevens hierna aanduiden als 'buitenlandse gegevens'.

Buitenlandse gegevens kunnen relevant zijn voor opsporingsonderzoeken. Een doorgaans efficiënte bevoegdheid die kan worden ingezet om gegevens te verkrijgen, is de vordering tot uitlevering van gegevens. De vraag is echter of de uitleveringsvordering kan worden gebruikt om buitenlandse gegevens op te eisen. Het is immers niet vanzelfsprekend dat bewijs dat zich in het buitenland bevindt kan worden vergaard middels nationale opsporingsbevoegdheden. Doorgaans is daar een rechtshulpverzoek voor nodig. De vraag of een rechtshulpverzoek nodig is voor het vorderen van buitenlandse gegevens wordt steeds relevanter, omdat opslag van gegevens in het buitenland toeneemt. De noodzakelijkheid van een rechtshulpverzoek zou meebrengen dat bewijs in toenemende mate moeilijk of zelfs niet beschikbaar is voor justitie. Daarbij speelt ook een rol dat voor de inzet van alternatieve bevoegdheden, zoals een doorzoeking, hoe dan ook buitenlandse rechtshulp nodig is als verlangde gegevens buiten Nederland zijn opgeslagen.

In dit artikel staat de vraag centraal of buitenlandse gegevens kunnen worden opgeëist middels de vordering tot uitlevering. Ik ga eerst in op twee verschijningsvormen van buitenlandse gegevens (par. 2). Daarna bespreek ik in hoofdlijnen de belangrijkste commune bevoegdheid tot het vorderen van gegevens (par. 3) en ga ik in op de vordering van buitenlandse gegevens naar Nederlands en internationaal recht (par. 4-5). Vervolgens behandel ik de opvattingen in de literatuur en de rechtvaardiging voor het huidige territoriale toepassingsbereik van de uitleveringsvordering (par. 6-7). Tot slot schets ik de praktische positie van de aangezochte onderneming en enkele verweren die de verdachte kan voeren tegen het gebruik van buitenlandse gegevens in een strafzaak (par. 8). Dit artikel gaat niet in op bevoegdheden op grond van bijzondere wetten, zoals de WED.

2. Twee verschijningsvormen van buitenlandse gegevens

Ondernemingen van uiteenlopende aard en omvang kunnen toegang hebben tot buitenlandse gegevens. Een eerste verschijningsvorm van buitenlandse gegevens doet zich voor, als een Nederlandse 'alleenstaande' onderneming gebruik maakt van gegevensopslag in het buitenland. Hier kan bewust voor zijn gekozen, bijvoorbeeld uit financiële overwegingen. Bewuste opslag buiten Nederland is echter niet noodzakelijk. Voor het opslaan en beheren van data wordt steeds vaker gebruik gemaakt van 'the cloud'. Hierbij worden gegevens, zoals e-mailbestanden, door een derde beheerd op één of meer externe servers die zich overal ter wereld kunnen bevinden. De gebruiker zal veelal niet weten waar gegevens op een specifiek moment zijn opgeslagen, mede omdat de beheerder van de gegevens deze snel kan overdragen naar een server op een andere locatie.[1] Als de opslaglocatie buiten Nederland ligt, is sprake van buitenlandse gegevens.

Een tweede verschijningsvorm van buitenlandse gegevens kan zich voordoen in de context van internationale concerns. Voor de Nederlandse onderdelen van internationale concerns is het vaak zinvol om toegang te hebben tot de informatiesystemen van buitenlandse concernonderdelen. Denk bijvoorbeeld aan een fabriek in Nederland die toegang heeft tot de e-mailcorrespondentie en digitale administratie van buitenlandse zusterfabrieken. Deze extern toegankelijke gegevens kunnen per vestiging zijn opgeslagen op een lokale server. Ook kunnen gegevens zijn opgeslagen op een centrale server, bijvoorbeeld op het hoofdkantoor van het concern. Voor zover deze lokale of centrale opslag buiten Nederland plaatsvindt, is vanuit het perspectief van Nederlands concernonderdelen sprake van buitenlandse gegevens.

3. Hoofdlijnen commune bevoegdheden vorderen gegevens

Sinds 2006 kent het Wetboek van Strafvordering ruime bevoegdheden tot het vorderen van gegevens (art. 126nc e.v. Sv).[2] Het voornaamste verschil tussen deze bevoegdheden ziet op het soort gegevens waarop de vordering betrekking kan hebben (identificerende, gevoelige, toekomstige of overige gegevens), de bevoegde autoriteit (iedere opsporingsambtenaar, de officier van justitie of de rechter-commissaris) en het type strafrechtelijk onderzoek in het kader waarvan de vordering kan worden gedaan (klassieke opsporing of 'vroegsporing' naar georganiseerde criminaliteit of een terroristisch misdrijf).

---

* Frank Mattheijer is advocaat bij Houthoff Buruma.

1. M. van der Linden en Chr. A. Baardman, 'Cybercrime: ontwikkelingen en invloed daarvan op de strafrechtketen', *Strafblad* 2011, p. 70.
2. Overzicht: G.J.M. Corstens, *Het Nederlands strafprocesrecht*, Deventer: Kluwer 2011, p. 294-299 en J.T.C. Leliveld, 'Bevoegdheden tot het vorderen van gegevens in het kader van een strafrechtelijk onderzoek', *FR* 2005, p. 320-329.

In het vervolg zal ik mij richten op het breed inzetbare art. 126nd Sv.[3] Op grond van dit artikel kan de officier van justitie, bij verdenking van een misdrijf waarvoor voorlopige hechtenis is toegelaten,[4] in het belang van het onderzoek vorderen dat gegevens worden verstrekt. Alleen een beperkte categorie van 'gevoelige' gegevens, bijvoorbeeld betreffende iemands godsdienst, is uitgezonderd.[5] De vordering kan worden gericht tot degene die redelijkerwijs kan worden vermoed toegang te hebben tot de gegevens, met uitzondering van verdachten en verschoningsgerechtigden.[6]
Art. 126nd Sv is, net als de overige bevoegdheden tot het vorderen van gegevens, in zijn oorspronkelijke vorm ingevoerd per 1 juni 2004 in het kader van de Wet vorderen gegevens financiële sector.[7] Met deze wet werd onder meer uitvoering gegeven aan het eerste protocol bij het EU-rechtshulpverdrag van 16 oktober 2001.[8] Lidstaten moeten op grond van het protocol, op verzoek van een andere lidstaat, in staat zijn om gegevens met betrekking tot rekeningen en transacties te vorderen van financiële instellingen. Ter uitvoering van deze verplichting kwam art. 126nd Sv tot stand, dat echter een veel ruimer toepassingsbereik heeft gekregen dan alleen financiële gegevens. Art. 126nd Sv heeft betrekking op 'gegevens', gedefinieerd als 'informatie die is opgeslagen of vastgelegd op een gegevensdrager, hetzij op schrift, hetzij in elektronische vorm'.[9] Gegevens kunnen uiteenlopende vormen aannemen, zoals fysieke of digitale administratie, e-mailbestanden en videobeelden.
De Wet vorderen gegevens financiële sector hing niet alleen samen met het Eerste Protocol bij het EU-rechtshulpverdrag. Met de wet volgde de wetgever ook een groot deel van de adviezen van de Commissie Mevis op.[10] De Commissie signaleerde in 2001 een toenemende strafvorderlijke behoefte aan gegevensvergaring van burgers, maar concludeerde dat daartoe geen adequate bevoegdheden bestonden.[11] Alleen art. 125i Sv [oud] voorzag in een bevoegdheid van de rechter-commissaris om beperkte categorieën van gegevens te vorderen.[12] In de praktijk werden ook door opsporingsambtenaren gegevens gevorderd, terwijl een specifieke bevoegdheid daartoe ontbrak. Bij gebreke van een wettelijke medewerkingsplicht was voor aangezochte ondernemingen vaak onduidelijk of zij gehouden waren om verlangde gegevens te verstrekken. Opsporingsinstanties waren uiteindelijk afhankelijk van 'vrijwillige' verstrekking.[13] De geadresseerde onderneming diende op grond van de Wet bescherming persoonsgegevens zelf het strafvorderlijk belang af te wegen tegen de betrokken privacybelangen.[14] De Commissie Mevis deed om deze redenen een voorstel voor een wetswijziging, dat de wetgever met de Wet vorderen gegevens financiële sector grotendeels opvolgde.
Een advies van de Commissie dat de wetgever aanvankelijk negeerde, was om de bevoegdheden tot het vorderen van gegevens niet te beperken tot de financiële sector.[15] Daarin kwam verandering met de Wet bevoegdheden vorderen gegevens.[16] Sinds haar inwerkingtreding in 2006, kunnen vorderingen worden gericht tot iedere (rechts)persoon, met uitzondering van verdachten en verschoningsgerechtigden. Inhoudelijk veranderde er verder weinig aan de oorspronkelijke regeling uit 2004. Wel is de huidige regeling nog sterker gebaseerd op de voorstellen van de Commissie Mevis. De MvT is grotendeels 'gekopieerd' uit het Rapport-Mevis en de formulering van het huidige art. 126nd lid 1 Sv is zelfs identiek aan de formulering die de Commissie in 2001 voorstelde.

De bevoegdheden tot het vorderen van gegevens maken deel uit van de bijzondere opsporingsbevoegdheden. In de praktijk is hun verhouding tot enkele 'gewone' opsporingsbevoegdheden echter interessanter. Gegevens die middels een vordering tot uitlevering kunnen worden verkregen, kunnen veelal ook beschikbaar komen door inbeslagneming van de gegevensdrager waarop de gegevens zijn opgeslagen, zoals een computer of een server. Om tot deze inbeslagneming over te gaan kan een vordering tot uitlevering van de gegevensdrager worden gedaan.[17] Inbeslagneming van gegevensdragers en het vastleggen van gegevens is ook mogelijk in het kader van een doorzoeking.[18] Een specifie-

3. Lid 1 luidt: 'In geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, kan de officier van justitie in het belang van het onderzoek van degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot bepaalde opgeslagen of vastgelegde gegevens, vorderen deze gegevens te verstrekken'.
4. Lid 6 voorziet in een uitzondering op deze eis, maar verlangt wel een machtiging van de rechter-commissaris.
5. Gevoelige gegevens kunnen wel worden gevorderd op grond van art. 126nf Sv, met machtiging van de rechter-commissaris.
6. Art. 126nd lid 1 en 2 jo. art. 96a lid 3 Sv.
7. *Stb.* 2004, 109 en *Kamerstukken II* 2001/02, 28 353, nr. 3.
8. Zie *Trb.* 2000, 96 voor het EU-rechtshulpverdrag en *Stb.* 2004, 108 voor het Eerste Protocol.
9. *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 7.
10. Formeel: 'De Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij'. Ik trof het Rapport-Mevis niet (meer) aan in 'officiële' databanken; zie wel www.recht.nl/nieuws/privacyrecht/archief/index.html?nid=1833.
11. Rapport-Mevis, p. 19-22.
12. Rapport-Mevis, p. 35-38 en E.C. Mac Gillavry, *Met wil en dank. Een rechtsvergelijkend onderzoek naar de medewerking aan strafvordering door bedrijven* (diss. Groningen), Groningen: Wolf Legal Publishers 2004, p. 95-99.
13. Rapport-Mevis, p. 25.
14. Rapport-Mevis, p. 23-27 en 39-40. Zie voor een uitgebreide analyse van de voormalige praktijk inzake de medewerking van strafvordering aan bedrijven E.C. Mac Gillavry, *Met wil en dank. Een rechtsvergelijkend onderzoek naar de medewerking aan strafvordering door bedrijven* (diss. Groningen), Groningen: Wolf Legal Publishers 2004 en E.C. Mac Gillavry, *Meewerken aan strafvordering door banken en Internet Service Providers*, Deventer: Gouda Quint 2000.
15. Rapport-Mevis, p. 9, 25-26.
16. Zie *Stb.* 2005, 390 en *Kamerstukken II* 2003/04, 29 441, nr. 3.
17. Art. 96a Sv. Dit artikel heeft alleen betrekking op voorwerpen die vatbaar zijn voor inbeslagneming: art. 94 Sv jo. art. 134 Sv. Gegevens zijn, anders dan voorwerpen, niet vatbaar voor inbeslagneming omdat de houder daarover blijft beschikken; *Kamerstukken II* 2001/02, 28 353, nr. 3, p. 6-7 en *Kamerstukken II* 1989/90, 21 551, nr. 3, p. 5.
18. De doorzoeking kan niet alleen strekken tot inbeslagneming van voorwerpen (zoals gegevensdragers), maar sinds een wetswijziging op voorstel van de Commissie Mevis ook tot de vastlegging van gegevens. Zie art. 125i Sv en *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 11-12.

ker alternatief is de netwerkzoeking.[19] Daarbij wordt tijdens een doorzoeking onderzoek verricht in een elders gelegen computer(netwerk) dat vanaf de plaats van de doorzoeking rechtmatig toegankelijk is. Tijdens de netwerkzoeking kunnen zonodig gegevens worden vastgelegd.
De wet sluit een vrije keuze tussen de zojuist besproken bevoegdheden niet uit. De wetsgeschiedenis maakt echter duidelijk dat de vordering tot uitlevering van gegevens het uitgangspunt is. Alternatieve bevoegdheden, zoals inbeslagneming, hebben veelal disproportionele gevolgen en dienen achterwege te blijven als een vordering tot uitlevering van gegevens volstaat.[20]
Sinds de invoering van de huidige bevoegdheden tot het vorderen van gegevens, mogen opsporingsinstanties geen beroep meer doen op vrijwillige gegevensverstrekking door burgers. Het staat opsporingsinstanties 'niet vrij om daarbuiten van derden te vragen op vrijwillige basis mee te werken aan het verstrekken van gegevens.'[21] De Hoge Raad heeft deze benadering bevestigd in 2010.[22] Een vordering is echter niet verplicht als een burger op eigen initiatief gegevens verstrekt.[23] Als ten onrechte wordt verzuimd een vordering te doen, mag dit overigens niet zonder meer leiden tot bewijsuitsluiting. Normaal gesproken komt alleen strafvermindering in aanmerking als eventuele sanctie.[24]

4. Vorderen van buitenlandse gegevens – wetsgeschiedenis

Op basis van de wettekst en wetsgeschiedenis geldt als hoofdregel dat aan een vordering ex art. 126nd Sv dient te worden voldaan, als de geadresseerde rechtmatig toegang heeft tot gevorderde gegevens.[25] Buitenlandse gegevens zijn niet wettelijk uitgezonderd, maar dat zegt weinig omdat het territoriale toepassingsbereik van opsporingsbevoegdheden niet volgt uit hun formulering.[26] In de wetsgeschiedenis is niet specifiek ingegaan op de vraag of buitenlandse gegevens kunnen vallen onder de uitleveringsvordering. Wel zijn er sterke aanwijzingen voor een bevestigende beantwoording.
Een eerste aanwijzing volgt uit de MvT behorend bij de voorloper van art. 126nd Sv,[27] dat de rechter-commissaris een beperkte bevoegdheid gaf om gegevens te vorderen. De MvT bevat de volgende passage: 'De vraag kan rijzen of het bevel ook betrekking kan hebben op gegevens die buiten Nederland zijn opgeslagen. Het komt mij voor dat indien de betrokkene beschikkingsmacht over de gegevens heeft en daartoe zonder een ander toestemming te hoeven vragen, toegang heeft, hij kan worden aangesproken ingevolge deze bepaling. Indien daarmee geheimhoudingsbepalingen die in het buitenland ten aanzien van deze gegevens gelden, zouden worden overtreden, is er sprake van een conflict van jurisdictie. Internationaal overleg zal ertoe moeten leiden dergelijke situaties zoveel mogelijk te beperken'.[28] Aangezien het huidige art. 126nd Sv veel ruimer is dan zijn voorloper, ligt het voor de hand dat bovenstaande interpretatie nog steeds opgaat.[29]
Een tweede aanwijzing dat buitenlandse gegevens kunnen vallen onder de uitleveringsvordering volgt uit het Rapport-Mevis, de uitdrukkelijke inspiratiebron voor de huidige regeling. De Commissie Mevis betoogde dat opsporingsautoriteiten twee mogelijkheden hebben om buitenlandse gegevens te verkrijgen van een internationale onderneming met een vestiging in Nederland. Ten eerste is een rechtshulpverzoek aan het opslagland mogelijk. Ten tweede zouden de gegevens direct kunnen worden gevorderd van de Nederlandse vestiging als deze toegankelijk zijn via haar computernetwerk. Een dergelijke vordering moet echter achterwege blijven, als verstrekking een schending oplevert van wettelijke geheimhoudingsbepalingen in het opslagland. In dat geval zou wel een rechtshulpverzoek vereist zijn.[30]
De wetgever is niet expliciet ingegaan op deze visie van de Commissie Mevis. Omdat de huidige regeling zo sterk is geinspireerd op haar voorstellen, is het echter waarschijnlijk dat de wetgever eenzelfde benadering voorstond.
In het licht van het voorgaande, is mijn conclusie dat buitenlandse gegevens naar huidig recht kunnen worden gevorderd van een in Nederland gevestigde onderneming, mits 1) die onderneming rechtmatig toegang heeft tot de gegevens, 2) de verstrekking daarvan geen schending oplevert van wettelijke geheimhoudingsbepalingen in het opslagland en 3) de onderneming geen verdachte of verschoningsgerechtigde is.
Voor de helderheid merk ik alvast op, dat een andere benadering geldt voor de eerder besproken netwerkzoeking. De netwerkzoeking mag niet zonder rechtshulpverzoek worden ingezet voor onderzoek in geautomatiseerde werken die zich kennelijk in het buitenland *bevinden:* 'De Nederlandse wet kan immers geen grondslag bieden voor een onderzoek in een geautomatiseerd werk dat onder de jurisdictie van een ander land valt'.[31]

5. Vorderen van buitenlandse gegevens – internationaal recht

Voor de bevoegdheden inzake buitenlandse gegevens, kan ook internationaal recht relevant zijn. In de eerste plaats kan internationaal recht blijk geven van een gedeelde opvatting over de bevoegdheid om gegevens te vorderen die buiten de landsgrenzen zijn opgeslagen. Ten tweede zou een verdrag

19. Art. 125j Sv; B.J. Koops en Y. Buruma, 'Formeel strafrecht en ICT', in: B.J. Koops (red.), *Strafrecht en ICT*, Den Haag: Sdu Uitgevers 2007, p. 95-95.
20. *Kamerstukken II* 2001/02, 28 353, nr. 3, p. 6-7; *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 12 en Aanwijzing opsporingsbevoegdheden, § 2.10.
21. *Kamerstukken II* 2003/04, 29 441, nr. 6, p. 2.
22. HR 21 december 2010, *NJ* 2012/24. Anders nog: HR 5 september 2006, *LJN* AX7473.
23. *Kamerstukken II* 2003/04, 29 441, nr. 6, p. 3.
24. HR 21 december 2010, *NJ* 2012/24 (specifiek § 14 van de noot van Borgers) en HR 20 september 2011, *NJ* 2011. Dat soms in het geheel geen sanctie volgt, blijkt uit Rb. Utrecht 26 augustus 2011, *NJFS* 2011/278; Rb. Utrecht 26 mei 2011, *LJN* BQ9073 en Rb. Haarlem 5 maart 2012, *LJN* BV7836.
25. *Kamerstukken II* 2001/02, 28 353, nr. 3, p. 12 en *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 8.
26. Zie wel art. 539a Sv en hierna.
27. Art. 125i Sv [oud], reeds besproken in de vorige paragraaf.
28. *Kamerstukken II* 1989/90, 21 551, nr. 3, p. 26-27.
29. Mac Gillavry, art. 126nd Sv, aant. 9.2 (*Melai/Groenhuisen*).
30. Rapport-Mevis, p. 79.
31. *Kamerstukken II* 1989/90, 21 551, nr. 3, p. 11-12 en, recenter, *Kamerstukken II* 2004/05, 26 671, nr. 10, p. 13 en 23. Zie ook uitgebreid F.P.E. Wiemans, *Onderzoek van gegevens in geautomatiseerde werken* (diss. Tilburg), Nijmegen: WLP 2004, p. 152-163.

Nederland ertoe kunnen verplichten (of juist beperken) om die bevoegdheid in te zetten. Ten derde kan internationaal recht invulling geven aan art. 539a Sv. Die bepaling brengt mee dat nationale strafvorderlijke bevoegdheden in beginsel buiten Nederland inzetbaar zijn, mits dit verenigbaar is met internationaal recht.[32]

Een beginsel dat in deze context relevant is, is dat van (territoriale) soevereiniteit. Dit beginsel lag bijvoorbeeld ten grondslag aan de klassieke *Lotus*-zaak[33] en is neergelegd in het VN-Handvest. In de context van het formele strafrecht, brengt het beginsel van soevereiniteit mee dat opsporingshandelingen op het grondgebied van een ander land slechts zijn toegestaan, als dat land daarmee per verdrag of ad hoc heeft ingestemd.[34] Als opsporingsambtenaren zich bij de inzet van bevoegdheden fysiek begeven in het buitenland, zoals voor een aanhouding of doorzoeking, is het meestal eenvoudig om vast te stellen dat sprake is van grensoverschrijdende opsporing waarvoor toestemming nodig is. Een bijzonder kenmerk van digitale bewijsgaring is echter, dat opsporingsautoriteiten zich daarvoor niet per definitie begeven naar de plaats waar bewijs zich bevindt. Hiermee rijst de vraag of digitale bewijsgaring in het buitenland een soevereiniteitsschending oplevert.

Een rechtsbron die op deze vraag ingaat, is het Cybercrime Verdrag van 23 november 2001 van de Raad van Europa, dat voor Nederland in werking trad op 1 maart 2007 ('CCV').[35] Het CCV is inmiddels door 37 landen geratificeerd, waaronder twee landen die geen lid zijn van de Raad van Europa (de VS en Japan). Het CCV beoogt om harmonisatie van materieel en formeel strafrecht te bewerkstelligen en rechtshulpverlening tussen de verdragsstaten te bevorderen.[36] Op het terrein van het formele strafrecht verplicht het CCV de lidstaten om een aantal opsporingsbevoegdheden te kunnen inzetten, onder meer ter vergaring van digitaal bewijs voor strafbare feiten (wel of geen cybercrime). Interessant is dat het CCV, net als het Wetboek van Strafvordering, de vordering tot uitlevering ruimer benadert dan de netwerkzoeking.

Art. 18 van het CCV regelt de vordering tot uitlevering van computergegevens ('production order'). De opsporingsautoriteiten van een lidstaat moeten bevoegd zijn om gegevens te vorderen van een persoon die zich tijdelijk of permanent bevindt op het grondgebied van deze lidstaat. Deze gegevens moeten '*in that person's possession or control*' zijn. Zo lang de adressant van de vordering bevoegd is om de gegevens op het territoir van de lidstaat te produceren, is de opslaglocatie irrelevant. Op grond van het CCV moet dus ook een bevoegdheid bestaan om buitenlandse gegevens te vorderen.[37]

Het CCV hanteert, net als de Nederlandse regeling, een striktere benadering als het gaat om grensoverschrijdend onderzoek aan computersystemen. Art. 19 van het CCV bepaalt dat de autoriteiten van de lidstaten bevoegd moeten zijn om geautomatiseerde werken te doorzoeken die zich bevinden '*in its territory*'. Volgens de toelichting zijn deze laatste woorden bewust gekozen, om te benadrukken dat voor '*transborder search and seizure*' een rechtshulpverzoek nodig is.[38] Een rechtshulpverzoek kan alleen achterwege blijven, als de onderzochte gegevens publiekelijk beschikbaar zijn of als de rechthebbende instemt met het onderzoek.[39]

Naast het CCV, bestaan er geen volkenrechtelijke bronnen die de bevoegdheid tot het vorderen van buitenlandse gegevens specifiek voorschrijven of begrenzen. Wel is de verwachting dat er in de nabije toekomst op EU-niveau regelgeving wordt afgevaardigd met betrekking tot grensoverschrijdende digitale bewijsgaring.[40] Uiteraard bestaan er al vele rechtshulpregelingen, waaronder het CCV zelf. Verder werken nationale opsporingsdiensten in toenemende mate samen om rechtshulpverzoeken met betrekking tot digitaal bewijs doelmatiger af te handelen.[41] Rechtshulpverzoeken worden echter pas noodzakelijk, als nationale bevoegdheden ontoereikend zijn. Omdat art. 126nd Sv in beginsel kan worden ingezet voor de verkrijging van buitenlandse gegevens, is het 'terugvallen' op rechtshulp normaliter dus niet nodig.

6. Vorderen van buitenlandse gegevens – opvattingen literatuur

De hiervoor besproken, ruime opvatting van de wetgever omtrent het vorderen van buitenlandse gegevens, is in de gepubliceerde rechtspraak nog niet uitdrukkelijk aan de orde

32. *Kamerstukken II* 1964/65, 7979, nr. 3, p. 10, Y.G.M. Baaijens-Van Geloven, 'Bespiegelingen over de internationale samenwerking en het nationale straf(proces)recht', in: G.J.M. Corstens en M.S. Groenhuijsen (red.), *Rede en recht*, Deventer: Gouda Quint 2000, p. 355 en J. Koers, *Nederland als verzoekende staat bij de wederzijdse rechtshulp in strafzaken* (diss. Tilburg), Nijmegen: Wolf Legal Publishers 2001, p. 397, 412-413.
33. PCIJ 7 september 1927, *Lotus S.S. (France v. Turkey)*.
34. Uitgebreider: A.H. Klip, 'Soevereiniteit in het strafrecht', in: G.J.M. Corstens en M.S. Groenhuijsen (red.), *Rede en recht*, Deventer: Gouda Quint 2000, p. 139-152, J. Koers, *Nederland als verzoekende staat bij de wederzijdse rechtshulp in strafzaken* (diss. Tilburg), Nijmegen: Wolf Legal Publishers 2001, p. 396-433, J.M. Sjöcrona, *De kleine rechtshulp* (diss. Leiden), Arnhem: Gouda Quint 1990, p. 11-14, 97-100.
35. *Trb.* 2002, 18 en *Trb.* 2004, 290. Zie over dit verdrag uitgebreid: R. Kaspersen, 'Het Cybercrime-verdrag van de Raad van Europa', in: B.J. Koops (red.), *Strafrecht en ICT*, Den Haag: Sdu Uitgevers 2007, p. 137-180 en P.J. van der Flier, 'De Wet Computercriminaliteit-II en het Cybercrime Verdrag', *AA* 2006, p. 914-922.
36. Zie ook *Kamerstukken II* 2004/05, 26 671, nr. 10, p. 2-3.
37. Zie Explanatory Report § 173, te raadplegen via de site van de Raad van Europa; *Kamerstukken II* 2004/05, 30 036, nr. 3, p. 27; Rapport-Mevis, p. 79 en R. Kaspersen, 'Het Cybercrime-verdrag van de Raad van Europa', in: B.J. Koops (red.), *Strafrecht en ICT*, Den Haag: Sdu Uitgevers 2007, p. 161.
38. Explanatory Report § 192, 193 en 195; *Kamerstukken II* 2004/05, 30 036, nr. 3, p. 28-29 en 39 en R. Kaspersen, 'Het Cybercrime-verdrag van de Raad van Europa', in: B.J. Koops (red.), *Strafrecht en ICT*, Den Haag: Sdu Uitgevers 2007, p. 160.
39. Explanatory Report § 293-294.
40. M. Hildebrandt en M.E. Koning, 'Universele handhavingsjurisdictie in cyberspace?', *Strafblad* 2012, p. 200-201.
41. M. van der Linden en Chr. A. Baardman, 'Cybercrime: ontwikkelingen en invloed daarvan op de strafrechtketen', *Strafblad* 2011, p. 70.

gekomen. In de literatuur is overwegend kritisch gereageerd.[42]
Kaspersen huldigde in 2000, dus voor de totstandkoming van art. 126nd Sv en het CCV, een opvatting die vergelijkbaar is met die van de wetgever.[43] Hij betoogde dat staten het niet zonder meer hoeven te aanvaarden als vanuit een ander land gegevens worden gevorderd die op basis van lokale wetgeving bescherming genieten. Kaspersen voegde hier aan toe dat het internationale recht op dit punt (anno 2000) onduidelijk was.
Wiemans is in zijn dissertatie uit 2004 kritisch op het feit dat de voorloper van art. 126nd Sv kon worden aangewend om buitenlandse gegevens te vorderen.[44] Zoals besproken, biedt ook het huidige art. 126nd Sv deze mogelijkheid. Wiemans acht deze situatie precair en betoogt: 'Dat geldt niet zozeer voorzover het gaat om in publieke databanken aanwezige gegevens maar wel indien het gaat om gegevens waarvoor justitie, indien zij deze gegevens zelf uit het buitenland had willen betrekken, aldaar een verzoek om rechtshulp had moeten indienen. Door het geven van een bevel tot uitlevering aan een persoon, die zelfstandig toegang heeft tot zulke gegevens in het buitenland, worden in feite bepalingen van internationaal recht omzeild. Dat klemt temeer indien de betreffende gegevens in het buitenland bescherming genieten'.[45] Ook Wiemans meent dat het internationale recht op dit punt onduidelijk is en geeft aan dat het CVV dat niet heeft veranderd.
Tot slot kan ook Mac Gillavry zich niet vinden in de ruime territoriale reikwijdte van art. 126nd Sv. Mac Gillavry betoogt dat de bevoegdheden tot het vorderen van gegevens niet mogen worden toegepast als dit leidt tot 'het omzeilen van rechtshulpverzoeken'.[46] Mac Gillavry betoogt ook dat de reikwijdte van de uitleveringsvordering onverenigbaar is met de reikwijdte van de netwerkzoeking. Zoals besproken, kan alleen eerstgenoemde bevoegdheid leiden tot het vergaren van buitenlandse gegevens. Mac Gillavry merkt over dat verschil op: 'De steunbevoegdheid is daarmee verstrekkender dan de grondbevoegdheid'.[47]
Ik zelf deel de visie van Wiemans en Mac Gillavry niet. Op het eerste gezicht is het inderdaad merkwaardig dat er een verschil bestaat tussen de vordering tot uitlevering van buitenlandse gegevens en het vergaren van die gegevens middels een netwerkzoeking. Identieke gegevens zouden op basis van de ene bevoegdheid wel en op basis van de andere bevoegdheid niet kunnen worden vergaard zonder een rechtshulpverzoek. De rechtvaardiging voor dit verschil blijkt niet uit de wetsgeschiedenis van art. 126nd Sv of de toelichting op het CCV, maar kan wel worden beredeneerd. Als een computer wordt doorzocht die in het buitenland staat, vindt er opsporing plaats buiten de landsgrenzen. Dit gebeurt weliswaar zonder het fysiek betreden van het grondgebied van een andere staat, maar in virtuele zin 'begeven' opsporingsambtenaren zich wel in een computer op het territorium van het opslagland en verzamelen zij daaruit informatie zonder tussenkomst van een andere partij.
Bij de uitleveringsvordering ligt dit anders, omdat opsporingsautoriteiten zich daarvoor fysiek noch virtueel begeven op vreemd grondgebied. De essentie van de uitleveringsvordering is niet zozeer het eigenhandig 'ophalen' van bewijs dat zich elders bevindt, maar het toepassen van dwang ten opzichte van een burger die in staat is om dat bewijs zelf aan te leveren. Deze dwang wordt niet uitgeoefend in het buitenland, maar in het land waar de adressant van de vordering zich bevindt en vanwaar hij de gegevens direct kan verstrekken.
In het licht van dat verschil, levert het vorderen van buitenlandse gegevens als zodanig geen omzeiling op van rechtshulpverzoeken, zoals Wiemans en Mac Gillavry betogen. Integendeel, op basis van het CCV moet er juist een bevoegdheid bestaan om buitenlandse gegevens te vorderen van partijen die daartoe toegang hebben vanaf het territorium van een lidstaat. De gedeelde opvatting van de verdragspartijen was kennelijk dat daar in beginsel geen rechtshulpverzoek voor nodig is. Dat een andere benadering geldt voor de netwerkzoeking, kan op basis van het voorgaande worden verklaard. Het benaderingsverschil van de wetgever is daarmee niet in strijd met internationaal recht, maar vloeit daar juist uit voort. Hiernaast is het de vraag of Mac Gillavry de vordering tot uitlevering terecht bestempelt als een steunbevoegdheid ten opzichte van de netwerkzoeking. De vordering tot uitlevering beoogt niet om de netwerkzoeking te faciliteren, maar is een zelfstandig instrument. Verder kennen beide bevoegdheden belangrijke verschillen, bijvoorbeeld als het gaat om hun inzetbaarheid ten opzichte van verdachten.

7. Vorderen van buitenlandse gegevens – waarom onbegrensd?

Uit de voorgaande paragrafen volgt, dat voor de vordering tot uitlevering van gegevens in beginsel alleen relevant is of de aangezochte partij daartoe vanuit Nederland rechtmatig toegang heeft. De kritiek op dat uitgangspunt is in mijn ogen niet overtuigend, maar daarmee is het ruime territoriale toepassingsbereik van art. 126nd Sv nog niet gerechtvaardigd. Een argument voor dat toepassingsbereik is dat Nederlandse ondernemingen bewust of onbewust steeds vaker toegang hebben tot buitenlandse gegevens, ook als het gaat om informatie die alleen verband houdt met Nederlandse bedrijfsactiviteiten. De vorderingsbevoegdheid zou in effectiviteit afnemen, als gegevensopslag in het buitenland verder toeneemt en deze gegevens niet kunnen worden gevorderd op grond van art. 126nd Sv.[48] Ter verkrijging van gegevens zijn dan steeds vaker rechtshulpverzoeken nodig, ook als het gaat om reguliere bedrijfsgegevens van Nederlandse onder-

42. Algemene kritiek op de huidige regeling laat ik onbesproken. Zie bijvoorbeeld L. Stevens, B.J. Koops en P. Wiemans, 'Een strafvorderlijke gegevensvergaring nieuwe stijl', *NJB* 2004, 1680-1686.
43. H.W.K. Kaspersen, 'Grensoverschrijdend onderzoek in computernetwerken', in: G.J.M. Corstens en M.S. Groenhuijsen (red.), *Rede en recht*, Deventer: Gouda Quint 2000, p. 298-299.
44. Art. 125i [oud] Sv.
45. F.P.E. Wiemans, *Onderzoek van gegevens in geautomatiseerde werken* (diss. Tilburg), Nijmegen: WLP 2004, p. 140.
46. Mac Gillavry, art. 126nd Sv, aant. 9.2 (*Melai/Groenhuisen*).
47. Mac Gillavry, art. 126nd Sv, aant. 9.2 (*Melai/Groenhuisen*).
48. Vgl. M. van der Linden en Chr.A. Baardman, 'Cybercrime: ontwikkelingen en invloed daarvan op de strafrechtketen', *Strafblad* 2011, p. 69 en Mac Gillavry, art. 126nd Sv, aant. 9.2 (*Melai/Groenhuisen*).

nemingen die 'toevallig' in het buitenland zijn opgeslagen. Daar komt bij dat het rechtshulptraject veelal zinloos zal zijn, als de opslaglocatie van gegevens onbekend is of snel kan veranderen, bijvoorbeeld omdat de gegevens zijn opgeslagen in de steeds vaker gebruikte cloud.[49] Tot slot zouden ondernemingen bewust kunnen anticiperen op een beperkte internationale reikwijdte van de vorderingsbevoegdheid, door te kiezen voor gegevensopslag in een land dat naar verwachting geen gehoor geeft aan een Nederlands rechtshulpverzoek.

Achter elk van deze argumenten schuilt de vrees dat opsporingsbevoegdheden te veel achter gaan lopen op technische ontwikkelingen. Als bevoegdheden moeten meegaan met technische vooruitgang, leidt dit echter onvermijdelijk tot een aantasting van klassieke strafrechtelijke uitgangspunten. Zo hebben de bevoegdheden tot het vorderen van gegevens geleid tot een vergaande plicht van burgers om medewerking te verlenen aan strafvordering, terwijl vrijwillige medewerking aan het opsporingsonderzoek voorheen het uitgangspunt was.[50] Hiernaast wordt steeds vaker gepleit voor een gewijzigde benadering van het territorialiteitsbeginsel in de context van digitale opsporing. Een conservatieve toepassing van dat beginsel zou niet aansluiten bij het internationale karakter van cyberspace en digitaal onderzoek onnodig belemmeren.[51]

Exemplarisch voor deze laatste ontwikkeling is de brief die (toenmalig demissionair) minister Opstelten op 15 oktober 2012 stuurde aan de Tweede Kamer.[52] In de brief onderstreept de minister dat een verdere uitbreiding van digitale onderzoeksbevoegdheden moet worden gerealiseerd middels een nog te ontwikkelen concept wetsvoorstel, 'zodat de gewenste en afgesproken opsporings- en vervolgingsprestaties kunnen worden geleverd.'[53] Opstelten gaat onder meer in op de netwerkzoeking en acht het problematisch dat deze niet kan worden ingezet voor het onderzoeken in computersystemen buiten Nederland. De minister heeft een regeling voor ogen die alleen een rechtshulpverzoek verlangt bij concrete wetenschap van de locatie van het op afstand te onderzoeken systeem. Zoveel mogelijk onwetend blijven van die locatie wordt daarmee gestimuleerd. Bovendien is het sterk de vraag of de beoogde regeling verenigbaar is met het CCV. De minister acht het in ieder geval 'van groot belang dat enigerlei bevoegdheid tot grensoverschrijvende opsporing internationaal geborgd wordt'[54] en 'kiest ervoor' deze verbetering voor Nederland al in gang te zetten middels het aangekondigde wetsvoorstel.

De brief van Opstelten gaat niet in op een voorgenomen uitbreiding van art. 126nd Sv of de andere bevoegdheden tot het vorderen van gegevens. De verklaring daarvoor kan zijn dat het huidige art. 126nd Sv letterlijk vrijwel onbegrensde mogelijkheden biedt om gegevens te vorderen van niet-verdachte burgers. Een uitbreiding van de uitleveringsvordering is niet nodig, omdat deze al kan worden ingezet om gegevens te vorderen die buiten Nederland zijn opgeslagen.

8. Praktische positie geadresseerde en verweren verdachte

In deze laatste paragraaf ga ik allereerst in op de praktische positie van de onderneming die wordt gedwongen om buitenlandse gegevens te verstrekken. Ten tweede bespreek ik de slagingskans van enkele verweren die de verdachte kan voeren tegen het gebruik van buitenlandse gegevens als bewijs in een strafzaak. Zowel de aangezochte onderneming als de verdachte kunnen zich verzetten tegen de vordering en het gebruik van buitenlandse gegevens. In de praktijk lopen hun belangen en informatiepositie echter sterk uiteen.

Aangezochte onderneming

De aangezochte onderneming zal zich vaak niet de (juridische) vraag stellen of zij verplicht is om gegevens te verstrekken die in het buitenland zijn opgeslagen. Als deze vraag al opkomt, is het voor de onderneming vaak de veiligste optie om toch geen bezwaar te maken en de gegevens te verstrekken. Vooral grotere ondernemingen kunnen vrezen dat protest tegen de vordering wordt uitgelegd als een weigering om medewerking te verlenen aan een strafrechtelijk onderzoek, een 'ongepaste' houding voor organisaties waarbinnen compliance hoog in het vaandel staat.

Een directer risico dat de aangezochte onderneming kan bewegen tot medewerking, is vervolging voor het niet opvolgen van een ambtelijk bevel.[55] Een weigering tot verstrekking kan er ook toe leiden dat opsporingsinstanties (alsnog) ingrijpendere bevoegdheden inzetten, zoals een doorzoeking of een netwerkzoeking. Als gegevens uitsluitend buiten Nederland zijn opgeslagen, zal de inzet van deze bevoegdheden zinloos blijken. In dit kader moet echter worden bedacht, dat de betrokken opsporingsambtenaren vaak onbekend zullen zijn met de automatiseringsstructuren van de aangezochte onderneming. Dat de verlangde gegevens buiten Nederland zijn opgeslagen, kan daarom pas blijken als de onderneming dit zelf ter sprake brengt en alternatieve bevoegdheden al zijn ingezet.

Een volgend argument voor de aangezochte onderneming om geen bezwaar te maken tegen de vordering van buitenlandse gegevens, is dat zij (als het goed is) zelf geen verdachte is en in die zin geen eigen belang heeft bij weigering. Een weigering tot verstrekking is normaliter alleen opportuun als zelfincriminatie toch op de loer ligt, als de belangen van de klant(en) waarop de gegevens betrekking hebben zwaarder wegen dan de risico's van weigering of als verstrekking mag worden geweigerd vanwege wettelijke geheimhoudingsbepalingen in het opslagland.

Verdachte

De verdachte heeft een veel directer belang bij verweer tegen de rechtmatigheid van de vordering tot uitlevering van buitenlandse gegevens, vooral als deze belastend bewijs heeft opgeleverd. Dergelijk verweer kan worden gevoerd in

49. M. Hildebrandt en M.E. Koning, 'Universele handhavingsjurisdictie in cyberspace?', *Strafblad* 2012, p. 198.
50. E.C. Mac Gillavry, 'De voorstellen van de Commissie-Mevis: dwangmiddelen voor de informatiemaatschappij', *NJB* 2001.
51. Bijvoorbeeld M. Hildebrandt en M.E. Koning, 'Universele handhavingsjurisdictie in cyberspace?', *Strafblad* 2012 en A. Lodder, 'Soevereiniteit op het web bestaat niet', *Het Financieele Dagblad* 19 april 2012. Vgl. ook J. Koers, *Nederland als verzoekende staat bij de wederzijdse rechtshulp in strafzaken* (diss. Tilburg), Nijmegen: Wolf Legal Publishers 2001, p. 397, 401-402.
52. *Kamerstukken II* 2012/13, 28 684, nr. 363.
53. *Kamerstukken II* 2012/13, 28 684, nr. 363, p. 2.
54. *Kamerstukken II* 2012/13, 28 684, nr. 363, p. 2.
55. Art. 184 Sr.

het kader van een beklagprocedure,[56] dan wel later tijdens een eventuele strafzitting. De verdachte en zijn advocaat hebben echter een informatieachterstand die meebrengt dat de praktische mogelijkheden tot verweer worden beperkt. Ten eerste zal de verdachte veelal pas op de hoogte raken van de vordering als de buitenlandse gegevens al (lang) zijn verstrekt, namelijk op het moment dat hij het strafdossier ontvangt.[57] Ten tweede zal op basis van het strafdossier (en de daarin opgenomen uitleveringsvordering) zelden kenbaar zijn dat de vordering betrekking had op buitenlandse gegevens, zeker als de aangezochte onderneming deze zonder protest heeft verstrekt. Alleen in bijzondere gevallen kan toch worden 'geraden' dat de verstrekte gegevens buiten Nederland moesten zijn opgeslagen, bijvoorbeeld als de vordering was gericht aan de Nederlandse vestiging van een internationaal concern, terwijl de vordering betrekking had op aangelegenheden die alleen een buitenlands concernonderdeel raken.

Zelfs als de verdachte aanleiding ziet om verweer te voeren, zijn kansrijke opties schaars. In het licht van het voorgaande is moeilijk te bepleiten dat de vordering als zodanig onrechtmatig was omdat deze betrekking had op buitenlandse gegevens. Hier komt bij dat de verdachte kan stuiten op de Schutznorm. In de rechtspraak wordt standaard aangenomen dat ontoelaatbare opsporing in het buitenland niet de persoonlijke belangen van de verdachte raakt, maar de (soevereiniteits)belangen van het betreffende land.[58] Als de verstrekking in strijd was met wettelijke geheimhoudingsbepalingen in het opslagland, heeft de verdachte meer kans. De vordering is dan in beginsel onrechtmatig en de verdachte zou kunnen bepleiten dat de geschonden geheimhoudingsbepalingen wel zijn belangen beogen te beschermen.[59] Deze bepalingen zullen echter niet altijd bekend zijn voor de verdediging.

De Schutznorm kan ook een obstakel opleveren als de verdachte aanvoert dat de vordering van gegevens een onevenredige inspanning opleverde voor de geadresseerde,[60] omdat gegevens 'uit het buitenland moesten komen'. Die stelling is echter hoe dan ook zwak, als de gegevens gemakkelijk vanuit Nederland konden worden gereproduceerd. De slagingskans is mogelijk iets groter als kan worden bepleit dat de privacybelangen van de verdachte onevenredig zijn geraakt door de hoeveelheid gevorderde gegevens.

Tot slot zou, in de zojuist beschreven situatie waarin van een Nederlands concernonderdeel gegevens worden gevorderd die feitelijk betrekking hebben op een buitenlandse zustervennootschap, mogelijk onzuiverheid van oogmerk kunnen worden bepleit. Als gevorderde gegevens geen verband houden met de activiteiten van het Nederlandse concernonderdeel, kan worden gesteld dat de gegevens daar niet mogen worden gevorderd. Op zichzelf is verdedigbaar dat buitenlandse gegevens kunnen worden gevorderd, omdat de effectiviteit van de uitleveringsvordering anders te zeer afhankelijk is van de IT-structuren van Nederlandse ondernemingen. Het is echter het andere uiterste om een Nederlandse vennootschap aan te zoeken in de hoop dat zij 'toevallig' toegang heeft tot het netwerk van zustervennootschappen buiten Nederland. In dat geval wordt niet zozeer de soevereiniteit van het opslagland geschonden, maar simpelweg de verkeerde partij aangezocht.

9. Conclusie

Sinds 2006 bestaan er ruim inzetbare bevoegdheden om gegevens te vorderen van burgers, waaronder de uitleveringsvordering op grond van art. 126nd Sv. Uit de wetsgeschiedenis volgen sterke indicaties dat dit artikel ook de bevoegdheid geeft om gegevens te vorderen die uitsluitend zijn opgeslagen in het buitenland, tenzij de verstrekking daarvan in strijd zou komen met wettelijke geheimhoudingsbepalingen in het opslagland. Dit territoriale toepassingsbereik lijkt op het eerste gezicht in strijd met het beginsel van territoriale soevereiniteit en maakt dat de uitleveringsvordering ruimer inzetbaar kan zijn dan de bevoegdheid om op afstand een computer(netwerk) te onderzoeken. Bij nader inzien levert het vorderen van buitenlandse gegevens echter geen schending op van internationaal recht of een omzeiling van rechtshulpverzoeken. Uit het CCV volgt dat Nederlandse opsporingsinstanties bevoegd moeten zijn om buitenlandse gegevens te vorderen; volgens de lidstaten is daar geen rechtshulpverzoek voor nodig. Het belangrijkste argument voor de huidige reikwijdte van art. 126nd Sv, is dat Nederlandse ondernemingen steeds vaker gebruik maken van buitenlandse gegevens en de uitleveringsvordering ineffectief wordt als deze niet kan worden ingezet ter vergaring van die gegevens. De angst dat bestaande opsporingsbevoegdheden niet zijn opgewassen tegen technische ontwikkelingen, wordt inmiddels ook gebruikt ter rechtvaardiging van aangekondigde voorstellen die beogen om andere bevoegdheden dan de uitleveringsvordering te verruimen. In de praktijk kunnen zowel de aangezochte onderneming als de verdachte verweer voeren tegen het vorderen van buitenlandse gegevens, maar hun informatiepositie en belangen verschillen sterk. Voor de verdachte zijn enkele verweren denkbaar, maar kansrijke verweren zijn normaliter schaars.

56. Ex art. 552a Sv; *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 27.
57. Mede vanwege de strafrechtelijk gesanctioneerde geheimhoudingsplicht voor de geadresseerde; art. 126bb lid 5 Sv jo. art. 272 Sr.
58. Zie bijvoorbeeld HR 17 april 2012, *NJ* 2012, 268.
59. Vgl. F.P.E. Wiemans, *Onderzoek van gegevens in geautomatiseerde werken* (diss. Tilburg), Nijmegen: WLP 2004, p. 160-161.
60. *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 23.