C. Conings LLM & mr. J.J. Oerlemans[1]

Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend?

5

De netwerkzoeking maakt het mogelijk onderzoek te plegen in de computers van verdachten. Het is echter onduidelijk wat de reikwijdte van de opsporingsmethode is. In dit artikel wordt onder andere nagegaan in hoeverre de opsporingsmethode op afstand via internet kan worden uitgevoerd. Daarbij wordt een rechtsvergelijking gemaakt met Nederland en België, omdat er interessante verschillen tussen beide regelingen zijn.

1. Inleiding

De netwerkzoeking is een bijzondere opsporingsbevoegdheid die het mogelijk maakt tijdens een zoeking vanaf een aangetroffen computersysteem via een netwerkverbinding een zoeking uit te voeren in een ander computersysteem. De relatief onbekende opsporingsmethode is in Nederland en België op cruciale punten verschillend geregeld. Het belangrijkste verschil is wellicht dat de netwerkzoeking in België in bepaalde gevallen via internet over de landsgrenzen heen kan worden uitgevoerd, terwijl de Nederlandse netwerkzoeking beperkt blijft tot het Nederlandse territorium.

Met behulp van internet is bovendien een andere methode van opsporing denkbaar: de online doorzoeking. Meer bepaald is dit een doorzoeking op afstand – via internet – van een computersysteem, die wordt uitgevoerd vanaf eigen computers van de overheid. Die doorzoekingsmogelijkheid zou politie en justitie in staat stellen heimelijk toegang te verschaffen tot gegevens die elders in computers liggen opgeslagen.

In dit artikel staan de vragen centraal in hoeverre de netwerkzoeking grensoverschrijdend kan worden toegepast en zij de basis kan vormen van een (heimelijke) online doorzoeking. Die vragen zijn actueel, omdat zowel nationaal als internationaal druk wordt bediscussieerd in hoeverre het grensoverschrijdend doorzoeken van computersystemen wenselijk is.[2]

Het artikel is als volgt opgebouwd. Ten eerste gaan we dieper in op de reikwijdte en voorwaarden van de Nederlandse en Belgische opsporingsbevoegdheid van de netwerkzoeking en bespreken we de belangrijkste verschillen tussen beide regelingen. Vervolgens gaan we na hoe het grensoverschrijdende aspect van de opsporingsmethode zich verhoudt tot het internationaal recht. Ten slotte zoeken we een antwoord op de vraag of de netwerkzoeking een op zichzelf staande, heimelijke online doorzoeking kan legitimeren.

2. De netwerkzoeking in Nederland en België

De netwerkzoeking is een opsporingsmethode die zowel in Nederland als in België afzonderlijk is geregeld, naast de reeds bestaande zoekingen op locatie zoals de huiszoeking.[3] Zowel de Nederlandse als Belgische wetgever vonden het noodzakelijk om in een aparte regeling te voorzien. Het ontstaan van netwerken zorgde immers voor de mogelijkheid om toegang te nemen tot computers op afstand. De bestaande locatie gebonden zoekingsmogelijkheden schoten daardoor te kort. Bovendien houden de verplaatsing naar de gezochte gegevens en de vereiste van een nieuw bevel een groot risico op verlies van bewijs in, gelet op het vluchtige karakter van gegevens.[4]

2.1 *Netwerkzoeking in Nederland*

In Nederland onderkende de wetgever al in 1989 het belang van een regeling voor de netwerkzoeking.[5] De nieuwe opsporingsbevoegdheid in art. 125j Sv (Nederlandse Wetboek van Strafvordering, hierna: N-Sv) werd destijds de 'meest vergaande bevoegdheid tot onderzoek in geautomatiseerde werken' genoemd en kon slechts tijdens een huiszoeking worden toegepast.[6] De netwerkzoeking maakte het mogelijk vanuit de computer die tijdens een huiszoeking werd aangetroffen gegevens te doorzoeken op aangesloten an-

1 Charlotte Conings is doctoranda bij het instituut voor strafrecht aan de KU Leuven en medewerker van het *Belgian Cybercrime Centre of excellence for training, research & education*.
Jan-Jaap Oerlemans is promovendus bij *eLaw@Leiden, het Centrum voor Recht in de Informatiemaatschappij* van de Universiteit Leiden en juridisch adviseur bij Fox-IT.
Met dank aan L.J.A. van Zwieten (landelijk coördinerend officier van justitie high tech crime & telecom van het Landelijk Parket te Rotterdam) voor zijn commentaar bij een eerdere versie van dit artikel.

2 Zie bijv. *Kamerstukken II* 2012/13, 28 684, nr. 363 (brief van 15 oktober 2012), waarin wordt aangegeven dat de Minister van Veiligheid en Justitie aangeeft dat hij o.a. de bevoegdheid tot 'het op afstand doorzoeken van gegevens (…) ongeacht de locatie van het geautomatiseerde werk en met inachtneming van de afspraken en regels over de internationale rechtshulp' wenselijk vindt en deze opsporingsmethode wil uitwerken in een conceptwetsvoorstel. Dit artikel beperkt zich tot de regelingen in Nederland en België. Zie over de ontwikkelingen op Europees niveau o.a. M. Hildebrandt & M.E. Koning, 'Universele handhavingsjurisdictie in cyberspace?', *Strafblad* 2012, p. 199-201 (hierna: Hildebrandt & Koning 2012).

3 Andere voorbeelden van zoekingen op locatie zijn de doorzoeking van een bedrijfsruimte of de doorzoeking van een voertuig.

4 Zie verder voor de Nederlandse toelichting van de wetgever over de noodzaak van de opsporingsbevoegdheid: *Kamerstukken II* 1989/90, 21 551, nr. 3 (MvT Wet Computercriminaliteit I), p. 11 en voor de Belgische toelichting over de noodzaak van de opsporingsmethode: *Parl. St.*, Kamer 1999/00, 213/1 (MvT), p. 22.

5 *Kamerstukken II* 1998/99, 26 671, nr. 2 (Voorstel van de Wet computercriminaliteit I), p. 8.

6 *Kamerstukken II* 1989/90, 21 551, nr. 3 (MvT Wet Computercriminaliteit I), p. 27.

dere computers binnen een netwerk. Met de Wet vorderen gegevens in 2005 is de regeling van de netwerkzoeking aangepast, zodat de opsporingsmethode tevens tijdens doorzoekingen op andere locaties kan worden toegepast.[7] Aangezien de netwerkzoeking in feite *een doorzoeking in geautomatiseerde werken ter vastlegging van gegevens* betreft, zal in Nederland in de praktijk eerst art. 125i N-Sv worden toegepast alvorens de netwerkzoeking van art. 125j N-Sv kan worden ingezet. De netwerkzoeking staat los van de inbeslagnemingsbevoegdheden en kan niet na een inbeslagname van een geautomatiseerd werk alsnog worden toegepast.

Tekstueel bekeken is art. 125j N-Sv echter een op zichzelf staande bevoegdheid die kan worden toegepast tijdens één van de doorzoekingsmogelijkheden uit art. 96b N-Sv (doorzoeking van een voertuig), art. 96c N-Sv (doorzoeking van plaatsen, niet zijnde een woning), art. 97 N-Sv en art. 110 N-Sv (doorzoeking van een woning of kantoor van een persoon met de bevoegdheid tot verschoning). Dat betekent dat de toepassing van de netwerkzoeking telkens aan andere voorwaarden is verbonden. De doorzoeking van een voertuig kan door een opsporingsambtenaar worden uitgevoerd in geval van ontdekking op heterdaad van een strafbaar feit of in geval van een misdrijf waarvoor voorlopige hechtenis mogelijk is (art. 67 lid 1 N-Sv). De doorzoeking in plaatsen niet zijnde een woning of kantoor van een verschoningsgerechtigde kan tevens slechts worden uitgevoerd in geval van ontdekking op heterdaad van een strafbaar feit of in geval van een misdrijf waarvoor voorlopige hechtenis mogelijk is. Echter, voor dit type doorzoeking moet een officier van justitie het bevel afgeven.[8] De doorzoeking van een woning of kantoor van een verschoningsgerechtigde kan op bevel van een officier van justitie in geval van ontdekking op heterdaad van een strafbaar feit of in geval van een misdrijf waarvoor voorlopige hechtenis mogelijk is worden uitgevoerd, voor zover daartoe een dringende noodzakelijkheid bestaat en het optreden van de rechter-commissaris niet kan worden afgewacht.[9] Indien die noodzaak er niet is moet de rechter-commissaris voor de doorzoeking een machtiging afgeven. Ten slotte kan een rechter-commissaris op grond van art. 110 N-Sv ambtshalve een doorzoeking in een woning of in een kantoor van een verschoningsgerechtigde uitvoeren.

Meer concreet kan een netwerkzoeking in Nederland plaatsvinden tijdens een doorzoeking in een woning op geautomatiseerde werken die via een netwerk met elkaar in verbinding staan, zoals een thuiscomputer die in verbinding staat met een mediaserver of spelcomputer waarop muziek en films kunnen worden opgeslagen en afgespeeld. Niet zelden zijn bijvoorbeeld ook gegevens op een externe harde schijf via een computernetwerk toegankelijk. Gegevens op de computersystemen die kunnen dienen om de waarheid aan de dag te brengen, kunnen door de zoekende autoriteit vervolgens worden gekopieerd en gedocumenteerd. Een andere situatie waarbij de bevoegdheid tot een netwerkzoeking kan worden toegepast is tijdens een doorzoeking bij een bedrijf, waarbij blijkt dat relevante gegevens op een andere – via het bedrijfsnetwerk toegankelijke – locatie in een datacentrum zijn opgeslagen.[10]

Een belangrijke beperking van de netwerkzoeking is dat de bijzondere opsporingsbevoegdheid uitdrukkelijk slechts mag worden toegepast voor zover dat noodzakelijk is. Het vermoeden moet bestaan dat voor het onderzoek relevante gegevens in de aanliggende computersystemen zijn te vinden. Bovendien mag een netwerkzoeking in aanliggende systemen slechts ten uitvoer worden gelegd voor zover de personen die op de plek van de doorzoeking wonen, werken of verblijven daartoe toegangsrechten hebben.[11] Denkbaar is dat een systeembeheerder of andere medewerker van een bedrijf met toegangsrechten de netwerkzoeking zou kunnen faciliteren. Een bevel tot toegangverlening tot een beveiligde computer en tot ontsleuteling van de relevante gegevens kan overeenkomstig art. 125k N-Sv in het verlengde van een doorzoeking ter vastlegging van gegevens en netwerkzoeking worden afgegeven. Op grond van art. 125k lid 3 N-Sv kan dit bevel echter niet aan de verdachte worden gericht.[12] Wel kan de verdachte (vrijwillig) medewerking verlenen. In Nederland mogen opsporingsambtenaren in het kader van een netwerkzoeking aanliggende systemen niet hacken teneinde toegang tot de gegevens te verkrijgen.[13] Ten slotte moeten de verdachte en rechthebbende van een plaats waar de doorzoeking heeft plaatsgevonden op grond art. 125m N-Sv zo spoedig mogelijk schriftelijk op de hoogte worden gesteld van de doorzoeking.

2.2 *De netwerkzoeking in België*

De Belgische netwerkzoeking werd op 28 november 2000 door de wet inzake informaticacriminaliteit in het leven geroepen.[14] Art. 88 ter B-Sv (Belgische Wetboek van Strafvordering, hierna: B-Sv) vormt de wettelijke basis voor de net-

7 *Stb.* 2005, 390.

8 Ingevolge lid 2 van art. 96c N-Sv kan het bevel bij dringende noodzakelijkheid door een hulpofficier van justitie worden afgegeven, indien de hulpofficier daarvoor gemachtigd is.

9 Indien ook het optreden van de officier van justitie niet kan worden afgewacht, dan komt de bevoegdheid toe aan de hulpofficier van justitie.

10 Zie voor dit voorbeeld J. Verbeek, C. van der Net & J. Tempelman, 'Netwerkzoeking in theorie en praktijk', *ITeR* 13, 1998, p. 255.

11 *Kamerstukken II* 1989/90, 21 551, nr. 3 (MvT Wet Computercriminaliteit I), p. 27.

12 Zie ook *Kamerstukken II* 1989/90, 21 551, nr. 3 (MvT Wet computercriminaliteit I), p. 27-28. Zie over het toegangs- of decryptiebevel aan een verdachte ook *Kamerstukken II* 2003/04, 29 441, nr. 3 (MvT Wet bevoegdheden vorderen gegevens), p. 26. Nederland overweegt echter art. 125k N-Sv te amenderen zodat ook de verdachte een toegangs- of decryptiebevel kan worden opgelegd bij verdenking van kinderpornografie of terrorisme. Zie de brief van 27 november over het onderzoek naar een wettelijk decryptiebevel en B.J. Koops, *Het decryptiebevel en het nemo-teneturbeginsel*, Den Haag: WODC 2012 (*Kamerstukken II* 2012/13, 33 400VI, nr. 68 (bijlage)). De auteur komt tot de conclusie dat – afhankelijk hoe het decryptiebevel wordt ingericht – het bevel verenigbaar is met art. 6 EVRM.

13 Zie ook C.P.M. Cleiren (red.), *Tekst en Commentaar Strafvordering*, art. 125j N-Sv aant. 3.

14 Wet van 28 november 2000 inzake informaticacriminaliteit, *B.S.* 3 februari 2001.

werkzoeking. Naar Belgisch recht wordt de netwerkzoeking eveneens voorafgegaan door een andere zoeking, namelijk de zoeking in een informaticasysteem (hierna: informaticazoeking). Art. 88 ter § 1 B-Sv definieert de netwerkzoeking immers als de *uitbreiding van de zoeking in een informaticasysteem of een deel daarvan* naar een informaticasysteem of een deel daarvan dat zich op een andere plaats bevindt. Uit de parlementaire voorbereidingen blijkt dat een dergelijke informaticazoeking niet noodzakelijk in het verlengde ligt van een huiszoeking.[15] De netwerkzoeking kan dus, net zoals in Nederland, worden toegepast in het kader van andere zoekingen, zoals de doorzoeking van vervoermiddelen (art. 29 Wet op het politieambt[16]) of de fouillering (art. 28 WPA). De informaticazoeking is op het eerste gezicht vergelijkbaar met de Nederlandse doorzoeking ter vastlegging van gegevens (art. 125i N-Sv). In België valt echter geen expliciete rechtsgrond voor een informaticazoeking te bespeuren, wat de nodige problemen met zich meebrengt (zie *infra*).

Art. 88 ter B-Sv stelt twee cumulatieve voorwaarden voorop voor de toepassing van de netwerkzoeking.[17] Enerzijds dient de uitbreiding noodzakelijk te zijn om de waarheid aan het licht te brengen ten aanzien van het misdrijf dat het voorwerp uitmaakt van de zoeking. Anderzijds moeten andere maatregelen disproportioneel zijn of moet er een risico bestaan dat zonder de uitbreiding bewijselementen verloren gaan.[18] Onzes inziens zal echter al snel sprake zijn van een risico op verlies van bewijsmateriaal. Kenmerkend voor informaticagegevens is immers dat ze erg vluchtig zijn en (op afstand) in een mum van tijd kunnen worden verwijderd. Bovendien zullen andere maatregelen vaak disproportioneel zijn. Een opeenstapeling van huiszoekingen zou immers bijzonder tijd- en werkkrachtrovend zijn en bovendien wellicht ingrijpender zijn voor de betrokkenen. In de praktijk vormen de voorwaarden geen effectieve rem op de netwerkzoeking, waardoor de netwerkzoeking telkens tot de mogelijkheden behoort wanneer de opsporingsautoriteiten het noodzakelijk achten voor de waarheidsvinding.[19]
Net zoals in Nederland kan de Belgische netwerkzoeking enkel betrekking hebben op informaticasystemen of delen daarvan waartoe de personen die gerechtigd zijn het onderzochte systeem te gebruiken *in het bijzonder toegang hebben* (art. 88 ter § 2 B-Sv). Het gaat hierbij om een *rechtmatige* toegang van de betrokken persoon tot systemen die niet voor iedereen toegankelijk zijn.[20] De wet bepaalt niet op welke manier opsporingsinstanties zich toegang kunnen verschaffen tot deze systemen. Wanneer het wachtwoord van de betrokkene niet bekend is, lijkt het gebruik van (hacker)tools daarom in België tot de mogelijkheden te behoren (cf. digitale slotenmaker). Aangezien opsporingsinstanties op grond van de netwerkzoeking gerechtigd zijn toegang te nemen tot het informaticasysteem, zijn wij van mening dat de betrokken opsporingsambtenaren zich niet schuldig maken aan het misdrijf hacking, zoals omschreven in art. 550 bis B-Sw (Belgische Strafwetboek, hierna: B-Sw).[21] Op basis van art. 88 quater § 1 B-Sv kan de onderzoeksrechter de verdachte bovendien verplichten zijn of haar wachtwoord af te geven.[22]
Mogelijke concrete toepassingen van de Belgische netwerkzoeking zijn vergelijkbaar met de Nederlandse situaties zoals hierboven omschreven. De Belgische rechtsleer geeft tevens aan dat rechthandhavingsinstanties via de netwerkzoeking onder andere toegang kunnen nemen tot systemen die via internet toegankelijk zijn, zoals de (online)bankrekening van de verdachte of diens webmail.[23] Art. 39 bis B-Sv creëert ten slotte de mogelijkheid om de aangetroffen gegevens onder bepaalde voorwaarden te kopiëren, ontoegankelijk te maken en te verwijderen.

2.3 *Tussenconclusie*

De Nederlandse en Belgische netwerkzoeking maken het mogelijk tijdens een zoeking een doorzoeking in aanliggende computersystemen uit te voeren. Toegang tot de aanliggende systemen kan echter enkel worden verkregen indien de betrokkene, ten aanzien van wie de zoeking wordt uitgevoerd, op rechtmatige wijze toegang tot de gezochte gegevens heeft.

15 *Parl. St.*, Kamer 1999/00, 213/11 (Verslag namens de commissie voor de justitie), p. 3-4.

16 Wet van 5 augustus 1992 op het politieambt, *B.S.* 22 december 1992 (hierna: WPA).

17 Zie voor een gedetailleerde beschrijving van de toepassingsvoorwaarden en uitvoering van de netwerkzoeking: D. Dewandeleer, 'Computermisdrijven en strafonderzoek in een ICT-context', in: R. Verstraeten & F. Verbruggen, *Straf- en strafprocesrecht*, Brugge: Die Keure 2009-2010, p. 142 e.v. (hierna: Dewandeleer 2009-2010); P. Van Linthout & J. Kerkhofs, 'Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel', *T. Strafr.* 2008, nr. 2, p. 79-95 (hierna: Van Linthout & Kerkhofs 2008).

18 Deze voorwaarde ligt in Nederland besloten in het subsidiariteitsbeginsel.

19 *Parl. St.*, Kamer, 213/4 (Verslag namens de commissie voor de justitie), p. 62; P. Van Linthout, 'Technische en juridische aspecten van ICT criminaliteit', in: X., *Recht in beweging*, Antwerpen: Maklu 2010, p. 440.

20 *Parl. St.*, Kamer 1999/00, 213/1 (MvT), p. 23; T. Laureys, *Informaticacriminaliteit: actuele wetgeving, tekst, analyse en bronnen*, Gent: Mys & Breesch 2001 (hierna: Laureys 2001), p. 65; *Parl. St.*, Kamer 1999/00, 213/4 (Verslag namens de commissie voor de justitie), p. 91.

21 Art. 550 bis B-Sw omschrijft het misdrijf hacking immers als volgt: 'Hij die, terwijl hij weet dat hij daar toe *niet gerechtigd is*, zich toegang verschaft tot een informaticasysteem of zich daarin handhaaft (…)'.

22 De wetgever sluit het bevel aan de verdachte immers enkel uit met betrekking tot actieve medewerking (art. 88 quater § 2 B-Sv) en niet met betrekking tot het louter verschaffen van inlichtingen (art. 88 quater § 1 B-Sv). Een bevel tot ontsleuteling kan zo bijv. niet aan de verdachte worden gericht. In de rechtsleer wordt betwijfeld of een bevel tot inlichtingen gericht aan de verdachte mogelijk is in het licht van de recentere rechtspraak van het EHRM in verband met het zwijgrecht. Zie: Dewandeleer 2009-2010, p. 159-160. Anders: B.J. Koops, *Het decryptiebevel en het nemo-teneturbeginsel*, Den Haag: WODC 2012, p. 54-55. Onzes inziens verwijzen de woorden 'Het bevel bedoeld in het eerste lid' naar lid 1 van par. 2 en dus niet naar par. 1 van art. 88 quater B-Sv, zoals Koops in zijn rapport aangeeft.

23 P. De Hert & G. Lichtenstein, 'Huiszoeking en beslag in geautomatiseerde omgevingen', in: M. Bockstaele, *Huiszoeking en beslag*, Brussel: Politeia 2004, p. 66 (hierna: De Hert & Lichtenstein 2004). Voor zover dat het niet gaat om communicatie '*in overdracht*' waarop de tapwetgeving van toepassing is (art. 90 ter e.v. Sv). Zie voor een toepassing van de netwerkzoeking op een webmailaccount: Corr. Brussel 10 januari 2008, *T.Strafr.* 2008, p. 149; met uitspraak in hoger beroep: Brussel 26 juni 2008, *T. Strafr.* 2008, afl. 6, p. 467-468.

De belangrijkste verschillen tussen de Nederlandse en Belgische netwerkzoeking zijn onzes inziens dat in België wel mag worden ingebroken in de computers waartoe de betrokkene toegang heeft en de verdachte kan worden gedwongen tot afgifte van het wachtwoord of sleutel teneinde toegang te krijgen tot aanliggende systemen. Daarnaast heeft de Belgische netwerkzoeking een breder bereik, omdat tevens informatiesystemen die via internet in verbinding staan met de computer van de verdachte kunnen worden doorzocht, waaronder de servers die toegang tot webmail- of een onlinebetalingsdienst faciliteren.

De netwerkzoeking en andere zoekingen in computersystemen kunnen een ernstige inbreuk op het recht op privacy met zich meebrengen. In de volgende paragraaf gaan we daarom na of ons huidig juridisch kader voldoende bescherming biedt tegen overheidinmengingen in computersystemen.

3. Het beschermingswaardige karakter van private computersystemen

Aangezien computers een grote hoeveelheid uiteenlopende private gegevens kunnen bevatten (agenda, communicatiegegevens en -inhoud, foto's, financiële gegevens enz.) dienen zij, overeenkomstig art. 8 EVRM voldoende beschermd te worden tegen inmengingen van de overheid. Hoewel het Europees Hof van de Rechten van de Mens in zijn jurisprudentie computersystemen op zich nog niet expliciet heeft gekwalificeerd als een te respecteren dimensie van het privacyrecht, vormt een inbreuk op de integriteit en vertrouwelijkheid van de computer wel degelijk een ingrijpende inmenging in de persoonlijke levenssfeer.[24] Naar onze mening is de privacyschending bij een informatica- en netwerkzoeking in veel gevallen vergelijkbaar met de inbreuk bij andere bijzondere opsporingsbevoegdheden, zoals de telecommunicatietap of de huiszoeking. Deze bevoegdheden vormen een ernstige inbreuk op het privacyrecht van de betrokkene en nopen tot een meer gedetailleerde regeling met voldoende waarborgen tegen misbruik.[25] De vraag rijst of daarbij een onderscheid moet worden gemaakt naar de soorten computersystemen. Niet alle informaticasystemen zullen immers privacygevoelige informatie bevatten. Wij menen in ieder geval dat een gedetailleerde regeling met hoge waarborgen op zijn plaats is. De opsporingsbevoegdheid zou op zijn minst slechts mogen worden toegepast op bevel van een officier van justitie/Openbaar Ministerie of met een machtiging van een rechter-commissaris/onderzoeksrechter. De vertrouwelijkheid en integriteit van computersystemen in het algemeen wordt immers aangetast. Bovendien zorgt een zekere mate van toezicht ervoor dat de kans op misbruik verkleint.[26] Geautomatiseerde werken voor persoonlijk gebruik zouden naar onze mening een bijzondere bescherming moeten krijgen, waarbij het systeem als een 'besloten ruimte' zou kunnen worden beschouwd.

De vraag rijst echter of de Nederlandse en Belgische wetgever dit beschermingswaardige karakter van private informaticasystemen voldoende erkennen. In Nederland kunnen de zoeking ter vastlegging van gegevens en de netwerkzoeking slechts worden toegepast in het kader van een andere zoeking met bijhorende voorwaarden. Zoals in de vorige paragraaf is opgemerkt is afhankelijk van het soort zoeking een opsporingsambtenaar, (hulp)officier van justitie of rechter-commissaris bevoegd. Tijdens een doorzoeking bij een kantoor kan bijvoorbeeld een (hulp)officier van justitie in het kader van de netwerkzoeking toegang nemen tot persoonlijke aanliggende systemen in de woning van de verdachte, zonder dat daartoe een machtiging van een rechter-commissaris vereist is. Dat lijkt ons echter helemaal niet vanzelfsprekend wegens de ernstige inbreuk op de persoonlijke levenssfeer van de verdachte. Hetzelfde probleem doet zich voor bij een zoeking bij een voertuig waarbij, indien daartoe aanleiding bestaat, door de opsporingsambtenaar een netwerkzoeking op aangetroffen computersystemen kan worden uitgevoerd.[27] Kortom, in verschillende situaties lijkt er in Nederland een discrepantie te bestaan tussen de waarborgen die gepast zijn bij een zoeking in een computersysteem voor persoonlijk gebruik en de garanties vereist in het kader van de verschillende doorzoekingsmogelijkheden.

Naar Belgisch recht vereist art. 88 ter B-Sv steeds een bevel van de onderzoeksrechter voordat kan worden overgaan tot een netwerkzoeking.[28] De toepassingsvoorwaarden van de informaticazoeking zijn daarentegen minder makkelijk vast te stellen, door het gebrek aan een duidelijke wettelijke grondslag. Toch lijkt ook voor de informaticazoeking een bevel van de onderzoeksrechter vereist. Art. 88 ter B-Sv, dat de netwerkzoeking nader regelt, haalt de informaticazoeking zijdelings aan en lijkt daarbij melding te maken van

24 M.M. Groothuis & T. de Jong, 'Is een nieuw grondrecht op integriteit en vertrouwelijkheid van ICT-systemen wenselijk?', *P&I* 2010, nr. 6, p. 280. Zie in dit kader ook het unieke Duitse grondrecht op de 'vertrouwelijkheid en integriteit van informatiesystemen' (afgeleid van het meer algemene privacyrecht), geformuleerd in een zaak over het op afstand doorzoeken van gegevens in geautomatiseerde werken (BVerfG 27 februari 2008, 'Online-Durchsuchung', m.nt. W.A.M. Steenbruggen, *Tijdschrift voor Media en Communicatierecht* 2008, nr. 5, p. 233-255). Daarbij is het van belang op te merken dat slechts geautomatiseerde werken *voor persoonlijk gebruik* onder het Duitse grondrecht vallen en bijv. geen 'intelligente huishoudelijk apparaten', zie BVerfG 27 februari 2008, r.o. 202.

25 Zie ook Y.G.M. Baaijens-van Geloven & J.B.H.M. Simmelink, *Normering in de opsporing*, in: M.S. Groenhuijsen & G. Knigge (red.), *Dwangmiddelen en rechtsmiddelen. Derde interimrapport onderzoeksproject Strafvordering 2001*, Deventer: Kluwer 2002, p. 491 met verwijzing naar EHRM 6 september 1978, *AA* 1979, 28, m.nt. E.A. Alkema (*Klass e.a./Duitsland*) en EHRM 2 augustus 1984, *NJ* 1988, m.nt. P. van Dijk (*Malone/Verenigd Koninkrijk*).

26 Zie in dit kader ook M.E. Koning, 'Van teugelloos "terughacken" naar "digitale toegang op afstand"', *P&I* 2012, afl. 2, p. 46-52. Toezicht is bijv. van belang teneinde na te gaan dat niet meer bestanden worden doorzocht dan noodzakelijk is.

27 Daarbij zal het overigens in de praktijk wellicht nog niet zo vaak voorkomen dat een persoon de geautomatiseerde werken in het voertuig via een netwerk heeft verbonden met computers thuis. Indien de netwerkzoeking tevens zou uitstrekken tot persoonlijke accounts op sociale mediadiensten, webmaildiensten en online-opslagdiensten zou dit scenario veel plausibeler zijn.

28 Brussel 26 juni 2008, *T. Strafr.* 2008, afl. 6, p. 467-468.

die toepassingsvoorwaarde. Het artikel vangt namelijk aan met de zinsnede '*wanneer de onderzoeksrechter een zoeking beveelt in een informaticasysteem of een deel daarvan…*'. De wetgever benadert de informaticazoeking bijgevolg als een onderzoeksdaad *sui generis*. Waar hij enerzijds immers erkent dat een informaticazoeking ook buiten het kader van een huiszoeking kan plaatsvinden, spreekt hij anderzijds toch van een bevel van de onderzoeksrechter. Dit terwijl een dergelijk bevel bijvoorbeeld voor een gerechtelijke fouillering niet is vereist.[29] Tenzij dit slechts een ondoordachte formulering uitmaakt,[30] erkent de wetgever blijkbaar het beschermingswaardige karakter van informaticasystemen door ook voor de zoeking in een informaticasysteem het bevel van de onderzoeksrechter voorop te stellen.[31] Het blijft echter vooralsnog onduidelijk over welk soort bevel dit gaat[32] en of een afzonderlijk bevel vereist is wanneer de informaticazoeking plaatsvindt in het kader van een huiszoeking.[33] Een optreden van de Belgische wetgever op dit vlak lijkt ons dan ook noodzakelijk aangezien de onduidelijkheid inzake de informaticazoeking ook het daaropvolgend databeslag en de netwerkzoeking op losse schroeven plaatst.

4. Grensoverschrijdende netwerkzoeking?

Steeds meer mensen maken tegenwoordig gebruik van populaire diensten die via internet worden aangeboden of via internet worden gefaciliteerd. Daarbij kan gedacht worden aan buitenlandse communicatie- en opslagdiensten, zoals de webmail diensten Hotmail en Gmail of de online-opslagdienst Google Drive. Die diensten maken bovendien dikwijls gebruik van de techniek van *cloud computing*. Bij cloud computing kunnen mensen via een netwerkinfrastructuur op afstand gebruikmaken van computerdiensten (bijv. voor opslag en verwerking), die primair door derde partijen worden beheerd.[34] Rechtstreekse toegang voor opsporingsdiensten tot de relevante gegevens is slechts mogelijk door toegang te verschaffen tot de accounts van de gebruiker. De lokalisatie van de gegevens is daarbij om verscheidene redenen een erg ingewikkeld gegeven.[35]

Het grenzeloze karakter van het internet zorgt voor een reële kans dat de gezochte gegevens zich op informaticasystemen in het buitenland bevinden. Ook in het geval van cloud computing is het 'vrij aannemelijk' dat het merendeel van de gegevens zich in het buitenland bevindt.[36] De vraag rijst bijgevolg of de netwerkzoeking toegang tot gegevens, opgeslagen in het buitenland, mogelijk maakt en of het internationale recht zich tegen een dergelijke rechtstreekse toegang verzet.

4.1 *Computer-georiënteerde benadering*

Nederland houdt een zogenaamd 'computer-georiënteerd jurisdictiebeginsel' aan, waarbij de zoeking in een geautomatiseerd werk verloopt volgens de regels van de staat waar dat geautomatiseerde werk zich bevindt.[37] De Nederlandse wetgever redeneert dat het doorzoeken van een geautomatiseerd werk in een andere staat als een handeling moet worden beschouwd die daar juridisch relevante gevolgen met zich meebrengt en mogelijk in strijd is met het recht van de staat waar de computer zich bevindt.[38] De staatssoevereiniteit beperkt zodoende de mogelijkheid tot het doorzoeken van een (deel van een) computer op het grondgebied van een andere staat. Soevereine staten bepalen zelf welk recht van toepassing is en welke instanties bevoegd zijn tot opsporing binnen hun territorium. Strafvorderlijk optreden houdt dan ook op bij de landsgrens.[39] Indien een overheid alsnog onderzoekshandelingen in het buitenland wenst, dient zij dat te doen via de geijkte wegen voorzien in het internationale recht. Zo is er bijvoorbeeld geen sprake van een soevereiniteitsschending indien toestemming wordt verkregen van de aangezochte staat, die

29 I. Delbrouck, 'Fouillering', in: X., *Postal Memorialis. Lexicon strafrecht, strafvordering en bijzondere wetten*, Mechelen: Kluwer 2006, F20/13.

30 In welk geval we dit geen *ongelukkige* formulering zouden noemen en we het bevel van de onderzoeksrechter minstens *de lege ferenda* zouden vooropstellen.

31 Net zoals de rechtsleer: zie: H. Bosly, D. Vandermeersch & M-A Beernaert, *Droit de la procédure pénale*, Brugge: La Charte 2010, p. 619-620; C. De Valkeneer, *Manuel de l'enquête pénale*, Brussel: Larcier 2011, p. 448 (zie hierna: De Valkeneer 2011); C. Meunier, 'La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique', *Rev. dr. pén. crim.* 2001, p. 663-664 (hierna: Meunier 2001); R. Verstraeten, *Handboek strafvordering*, Antwerpen: Maklu 2007, p. 459 (hierna: Verstraeten 2007); Zie echter *contra*: Dewandeleer 2009-2010, p. 139.

32 Enkele auteurs verwijzen voor de toe te passen voorwaarden naar het klassieke bevel van de huiszoeking: De Valkeneer 2011, p. 448; Meunier 2001, p. 663-664; Verstraeten 2007, p. 459. Het huiszoekingsbevel lijkt echter niet altijd geschikt, onder andere door de uitsluiting van de mini-instructie uit art. 28septies B-Sv. Dit terwijl een netwerkzoeking, die minstens even ingrijpend is als de informaticazoeking, wel via mini-instructie kan worden bevolen.

33 In het kader van de huiszoeking lijkt de vereiste van een afzonderlijk bevel te verregaand. Aangezien de huiszoeking, buiten de gevallen van heterdaad en toestemming van de betrokkenen, eveneens een bevel van de onderzoeksrechter vereist, is de bescherming van de privacy onzes inziens voldoende gewaarborgd. De bevoegdheid tot huiszoeking behelst zodoende het doorzoeken van alle, ter plaatse aangetroffen informaticasystemen. Uiteraard moeten de uit het bevel voortvloeiende beperkingen daarbij steeds worden gerespecteerd. De Hert & Lichtenstein 2004, p. 64; Verstraeten 2007, p. 459. Zie echter *contra*: De Valkeneer 2011, p. 448. (De auteur stelt dat 2 bevelen vereist zijn die echter wel in hetzelfde instrument kunnen worden opgenomen.)

34 Zie J.J. Schwerha IV, 'Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers"', Project on Cybercrime (discussion paper) January 2010, p. 6. Beschikbaar via www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_reps_joeschwerha1a.pdf (laatst geraadpleegd op 17 december 2012).

35 Zie hierover uitgebreid: B.J. Koops e.a., *Misdaad en opsporing in de wolken*, Den Haag: WODC 2012, p. 30 (nog te verschijnen) (hierna: Koops e.a. 2012).

36 Koops e.a. 2012, p. 36.

37 *Kamerstukken II* 2004/05, 26 671, nr. 10, p. 13: 'Onder de plaats waar een computersysteem zich bevindt dient te worden verstaan de fysieke locatie waar het systeem is opgesteld of – indien het systeem uit verschillende componenten bestaat – de plaats waar een of meer van die componenten zich bevinden'.

38 *Kamerstukken II* 2004/05, 26 671, nr. 10, p. 23: 'Een onderzoek in die computer betekent immers het verrichten van opsporingshandelingen buiten de landsgrenzen. Dit soort optreden is verdragsrechtelijk geregeld.'

39 A.H. Klip, 'Soevereiniteit in het strafrecht', in: G.J.M. Corstens & M.S. Groenhuijsen, *Rede en Recht: opstellen ter gelegenheid van het afscheid van prof. mr. N. Keijzer van de Katholieke Universiteit Brabant*, Deventer: Gouda Quint 2000, p. 140.

volgens Nederlandse rechtspraak en rechtsleer zowel vooraf als (stilzwijgend) achteraf kan worden verleend.[40] Grensoverschrijdende opsporingshandelingen kunnen uiteraard ook plaatsvinden als het handelen in lijn is met een verdrag.

Het verbod om opsporingshandelingen in het buitenland uit te voeren kan worden afgeleid uit het internationaal recht.[41] In Nederland is het verbod bovendien gecodificeerd in art. 539a lid 3 Sv. In de behandeling van de wetgeving inzake de netwerkzoeking staat dan ook aangegeven dat geen toegang mag worden verschaft tot een computer die zich in het buitenland bevindt.[42] Wel geeft de Nederlandse wetgever aan dat indien de locatie van de server niet duidelijk is en opsporingsambtenaren te goeder trouw handelen (niet wetende dat de computersystemen zich buiten Nederlands territorium bevinden) de gegevens wel in een strafrechtelijk onderzoek kunnen worden gebruikt.[43] Het is echter niet duidelijk hoe in de praktijk met deze uitzondering moet worden omgegaan.

4.2 *De Belgische 'pragmatische' oplossing*

Naar Belgisch recht bestaat daarentegen een beperkte mogelijkheid tot een grensoverschrijdende netwerkzoeking. De Belgische wetgever schuift daarmee naar eigen zeggen een 'voorzichtige, maar pragmatische' oplossing naar voren.[44] De grensoverschrijdende zoeking moet mogelijk zijn, doch mag niet de regel zijn, want '*wanneer voldoende tijd en kennis voorhanden is, moet de weg van de klassieke internationale rogatoire commissies worden gevolgd […]*', aldus de wetgever.[45]

De Belgische wetgever schetst zelf de situaties waarin de grensoverschrijdende zoeking mogelijk moet zijn. Het gaat daarbij op de eerste plaats om situaties waarin onderzoekers per toeval of onopzettelijk op data uit het buitenland stuiten. Ten tweede vermeldt de wetgever de situaties waarin de onderzoekers tijdens de zoeking kennis hebben van het grensoverschrijdende aspect ervan, maar er redelijkerwijze niet in slagen de betrokken staat te identificeren. Een grensoverschrijdende zoeking is tot slot eveneens mogelijk indien de hoogdringendheid gebiedt de netwerkzoeking over de grenzen heen verder te zetten om op die manier voorlopige maatregelen te kunnen treffen ter vrijwaring van het bewijsmateriaal.[46] In geval van een grensoverschrijdende netwerkzoeking mogen de aangetroffen gegevens op grond van art. 88 ter § 3 B-Sv enkel worden gekopieerd. De onderzoeksrechter moet, via het Openbaar Ministerie, het Ministerie van Justitie hiervan onverwijld op de hoogte brengen. Het ministerie stelt op zijn beurt de bevoegde overheid van de betrokken staat van de zoeking in kennis. Wanneer vervolgens geen bezwaar rijst, kan dat onzes inziens in aanmerking worden genomen als een stilzwijgende toestemming achteraf. De kennisgeving aan de betrokken staat dient echter enkel te gebeuren indien zij redelijkerwijze kan worden geïdentificeerd.[47]

De vraag rijst hoe deze Belgische regeling zich verhoudt tot het internationale recht. We dienen daarbij in de eerste plaats een blik te werpen op het Cybercrimeverdrag, waarvan Nederland en België beiden verdragsstaten zijn.[48]

4.3 *De netwerkzoeking en het Cybercrimeverdrag*

Art. 19 lid 2 Cybercrimeverdrag verplicht de ratificerende staten een netwerkzoekingsbevoegdheid in hun regelgeving op te nemen. Die plicht is beperkt tot de netwerkzoeking in systemen die zich op het *nationale territorium van de staat* bevinden. In de onderhandelingen bij de totstandkoming van het Cybercrimeverdrag werd uitvoerig gedebatteerd over de mogelijkheid van een grensoverschrijdende netwerkzoeking. Kaspersen, die betrokken was bij de totstandkoming van het Verdrag, geeft aan dat de betrokken staten geen consensus konden bereiken over het feit of de grensoverschrijdende zoeking in een computersysteem al dan niet een soevereiniteitsschending tot gevolg had.[49] Het aannemen van internationale regels hieromtrent leek voorlopig dan ook de enige mogelijkheid om enigszins de tegengestelde meningen te verzoenen. Aangezien het internationale publiekrecht weinig ruimte laat voor grensoverschrijdende zoekingen achtten de staten specifieke afspraken voor de netwerkzoeking noodzakelijk.[50] Die concrete afspraken bleven echter zeer beperkt, aangezien de staten van mening waren dat de nodige kennis en praktijkervaring hen voorlopig ontbrak en ze daarom de tijd niet rijp achtten om een weloverwogen standpunt op dat vlak in te nemen.[51]

40 P.J.P. Tak (red.), *Heimelijke opsporing in de Europese Unie. De normering van bijzondere opsporingsmethoden in de landen van de Europese Unie*, Antwerpen: Intersentia 2000, p. 816. Zie ook A. Klip, 'Extraterritoriale strafvordering', *DD* 1995, p. 1075 met een verwijzing naar HR 16 april 1984, *NJ* 1986/769.

41 P.L. Bellia, 'Chasing Bits across Borders', *The University of Chicago Legal Forum* 2001, p. 28 (hierna: Bellia 2001). Zie ook PCIJ 27 september 1927, *PCIJ Reports*, Series A, nr. 10 (*Lotus*), p. 18-19: 'the first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention.'

42 Zie ook *Kamerstukken II* 1989/90, 21 551, nr. 3 (MvT Wet Computercriminaliteit I), p. 11-12: 'Behoudens een uitdrukkelijke verdragsrechtelijke grondslag mag geen onderzoek worden verricht in een computersysteem dat zich kennelijk in het buitenland bevindt'.

43 Zie ook *Kamerstukken II* 2004/05, 26 671, nr. 10, p. 23: 'In beginsel dient men in een rechtshulpverzoek aan het desbetreffende land om de gegevens te vragen. Men kan echter niet altijd van te voren weten of een netwerkzoeking leidt tot een zoeking in een computer in het buitenland. In dat geval zijn de gegevens te gebruiken voor het onderzoek. Als men dit echter wel weet, ontdekt of zou behoren te weten, is internationale rechtshulp noodzakelijk'.

44 *Parl. St.*, Kamer 1999/00, 213/1 (MvT), p. 24.

45 *Parl. St.*, Kamer 1999/00, 213/1 (MvT), p. 24.

46 *Parl. St.*, Kamer 1999/00, 213/1 (MvT), p. 24-25.

47 Zie in dit kader ook De Hert & Lichtenstein 2004, p. 64.

48 Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, *Trb.* 2002, 18. België ratificeerde dit Verdrag op 20 augustus 2012 (inwerkingtreding: 1 december 2012). Zie ook het *Belgisch Staatsblad* 2012, editie N.365.

49 H.W.K. Kaspersen, 'Jurisdiction in the Cybercrime Convention', in: B.J. Koops & S.W. Brenner (red.), *Cybercrime and Jurisdiction, A Global Survey*, Information Technology & Law Series, nr. 11. T.M.C. Asser Press, Den Haag 2006, p. 20 (hierna: Kaspersen 2006).

50 Kaspersen 2006, p. 20.

51 Zie ook het Explanatory Report bij het Cybercrimeverdrag, § 293.

De staten konden slechts een overeenkomst bereiken inzake de mogelijkheid tot een grensoverschrijdende zoeking in twee gevallen. Ten eerste kunnen opsporingsinstanties op basis van art. 32 onder a Cybercrimeverdrag kennisnemen van publiekelijk toegankelijke gegevens, onafhankelijk van waar zij staan opgeslagen.[52] Ten tweede kunnen opsporingsinstanties op grond van art. 32 onder b Cybercrimeverdrag toegang nemen tot in het buitenland opgeslagen gegevens indien toestemming wordt verkregen van een rechthebbende, dat wil zeggen degene die de wettelijke bevoegdheid heeft om de betrokken gegevens prijs te geven. Met toestemming van de betrokken persoon of de dienstaanbieder die dat bijvoorbeeld in zijn algemene voorwaarden heeft geregeld kan aldus rechtmatig direct toegang worden verkregen tot de gegevens in het besloten systeem.[53]

De Belgische extraterritoriale toepassing van de netwerkzoeking gaat dus een stap verder dan de regeling uit het Cybercrimeverdrag, aangezien onder omstandigheden toegang kan worden verschaft tot gegevens op servers die zich in het buitenland bevinden, met een in kennis stelling van de betrokken staat die achteraf plaatsvindt.[54]

Toch lijkt het Cybercrimeverdrag enige ruimte te laten. Het *explanatory report* bij het Cybercrimeverdrag verwijst expliciet naar art. 39 par. 3 Cybercrimeverdrag om duidelijk te maken dat het niet de bedoeling was verregaandere bevoegdheden toe te laten noch uit te sluiten.[55] Ruimere bevoegdheden blijven bijgevolg mogelijk, voor zover zij in overeenstemming zijn met de algemene internationale regels over soevereiniteit, territorialiteit en wederzijdse rechtshulp in strafzaken, waarnaar het Cybercrimeverdrag eveneens uitdrukkelijk verwijst.[56]

4.4 *De netwerkzoeking en het internationale recht*

Zowel de nationale wetgevers als de Raad van Europa (uit gebrek aan overeenstemming) blijken aldus uit te gaan van een computer-georiënteerde benadering voor de lokalisering van de netwerkzoeking. De unilaterale toepassing van de opsporingsmethode van een doorzoeking in systemen in het buitenland is in deze visie in principe dan ook in strijd met het geldende internationaal recht.[57] Seitz merkt in dit verband op dat strikt theoretisch gezien de grensoverschrijdende zoeking niet door de beugel kan, zolang daar geen toestemming voor is, een verdragsbasis voorhanden is, of geen internationaal gewoonterecht is geworden. Zuiver praktische overwegingen kunnen de soevereiniteitsinbreuk niet rechtvaardigen, aldus Seitz.[58]

Concreet toegepast op de netwerkzoeking betekent dit dat de geijkte internationale wegen moeten worden gevolgd zodra de gezochte gegevens opgeslagen staan op een computer in het buitenland, met een onvermijdelijke vertraging van de opsporing tot gevolg. Door het grenzeloze karakter van het internet zullen dergelijke situaties zich echter erg vaak voordoen. In de praktijk zullen als alternatief de gegevens dikwijls bij Amerikaanse dienstaanbieders moeten worden gevorderd.[59] Niet in alle gevallen biedt deze mogelijkheid echter voldoende soelaas. Opvallend is bijvoorbeeld dat in het eerder aangehaalde WODC-rapport wordt aangegeven dat bestanden uit dataopslagdiensten (zoals Google Drive en Microsofts' Skydrive) lastig te verkrijgen zijn.[60]

Deze computer-georiënteerde benadering zorgt echter voor heel wat moeilijkheden in de praktijk. De Hert identificeert naar onze mening goed waar het probleem ligt. Een 'hard' verbod op een grensoverschrijdende zoeking maakt het wel erg gemakkelijk voor burgers om opsporingsdiensten te frustreren in hun opsporingsactiviteiten door gebruik te maken van cloud-diensten of handig gebruik te maken van diensten afkomstig uit andere staten.[61] Niet alleen moet vanuit de computer-georiënteerde benadering op disproportionele wijze beroep worden gedaan op (trage) internationale instrumenten, ook is de correcte toepassing daarvan vaak niet vanzelfsprekend. Zoals reeds aangegeven is de fysieke locatie van data vaak moeilijk te achterhalen en kan ze erg veranderlijk zijn. Cloud computing draagt in belangrijke mate bij aan deze '*loss of location*'-problematiek.[62] Het identificeren van de staat die toestemming dient te verlenen is in die omstandigheden dan ook een moeilijke, zo niet onmogelijke, opgave. Naar Belgisch recht zou de noodtoestand[63] hier eventueel een oplossing kunnen bieden. De vraag in welke mate deze rechtvaardigingsgrond internationale gelding heeft.

Het is vreemd te moeten vaststellen dat de fysieke locatie van data blijkbaar één van de belangrijkste criteria uitmaakt voor de uitoefening van opsporingsbevoegdheden, in een

52 Zie J.J. Oerlemans & B.J. Koops, 'Surveilleren en opsporen in een internetomgeving', *Justitiële Verkenningen* 2012, 5, p. 38-39.

53 Koops e.a. 2012, p. 36 met verwijzing naar § 294 van het Explanatory Report bij het Cybercrimeverdrag.

54 Zie ook P. de Hert, 'Cybercrime and Jurisdiction in Belgium and the Netherlands. Lotus in Cyberspace – Whose Sovereignty is at stake?', in: B.J. Koops & S.W. Brenner (red.), *Cybercrime and Jurisdiction, A Global Survey*, Information Technology & Law Series, nr. 11. T.M.C. Asser Press, Den Haag 2006, p. 107; Hildebrandt & Koning 2012, p. 203; Koops e.a. 2012, p. 37-38 (nog te verschijnen).

55 Zie art. 39 lid 3 Cybercrimeverdrag en het Explanatory report, par. 131 en 293.

56 Zie o.a. art. 25 Cybercrimeverdrag.

57 Bellia 2001, p. 44 en 59. Zie ook p. 62: 'I ultimately conclude that remote cross-borders searches are not distinguishable in legally relevant ways from physical searches. As a result, at least at present, unilateral cross-border searches generally will violate customary international law'. Zie ook Hildebrandt & Koning 2012, p. 203 en Koops e.a. 2012, p. 36 (nog te verschijnen).

58 N. Seitz, 'Transborder Search: A New Perspective in Law Enforcement?', *Yale Journal of Law & Technology* 2005, nr. 7, p. 24-50 (hierna: Seitz 2005).

59 Zie hierover o.a. uitgebreid: Koops e.a. 2012, p. 38 e.v.

60 Koops e.a. 2012, p. 20.

61 P. de Hert, 'Cybercrime and Jurisdiction in Belgium and the Netherlands. Lotus in Cyberspace – Whose Sovereignty is at stake?', in: B.J. Koops & S.W. Brenner (red.), *Cybercrime and Jurisdiction, A Global Survey*, Information Technology & Law Series, nr. 11. T.M.C. Asser Press, Den Haag 2006, p. 109 (hierna: De Hert 2006).

62 Zie hierover uitgebreid: Koops e.a. 2012, p. 35-38 en 55-57.

63 Een rechtvaardigingsgrond waarbij een belangenconflict een delictstypische gedraging rechtvaardigt. De delictstypische gedraging vormt daarbij de enige mogelijkheid om een rechtsgoed met een hogere waarde dan het rechtsgoed dat wordt beschermd door het strafbaar gesteld gedrag, te vrijwaren.

wereld waar die fysieke locatie nauwelijks belang heeft. Gelet op de geschetste problematiek moeten we de houdbaarheid van het computer-georiënteerd uitgangspunt dan ook in twijfel durven trekken.

4.5 *Naar een toegang-georiënteerde benadering?*

Onder de Belgische interpretatie over de reikwijdte van de netwerkzoeking is het wel mogelijk toegang te verschaffen via internet tot de gegevens in het buitenland en in de cloud, indien alternatieve methoden onvoldoende soelaas bieden. De Belgische regeling sluit onzes inziens meer aan bij de realiteit waarbij relevante gegevens in een opsporingsonderzoek zich in toenemende mate op servers elders bevinden. De pragmatische benadering lijkt eerder aan te knopen bij de toegangsbevoegdheid van de betrokken persoon als criterium voor jurisdictie in plaats van een computer-georiënteerd jurisdictiebeginsel.

Spoenle hanteert een gelijkaardig criterium voor jurisdictie, namelijk de beschikkingsmacht dat hij aanduidt met de term '*power of disposal*'. Indien de accountgegevens (inlognaam en wachtwoord) van de verdachte beschikbaar zijn zouden staten onder voorwaarden gerechtigd moeten zijn op de cloud-toepassingen van de verdachte in te loggen.[64] Spoenle reikt daarbij zelf mogelijke voorwaarden aan, zoals:

1. opsporingsinstanties kunnen de gegevens niet vorderen van de cloud-aanbieder;
2. verdachten moeten de nationaliteit hebben van de staat of ingezetenen zijn van de staat waar de zoeking wordt uitgevoerd;
3. de accountgegevens moeten op een legale wijze zijn verkregen; en
4. een machtiging van een rechter-commissaris (Nederland) of onderzoeksrechter (België) moet worden verkregen als extra waarborg voor de privacyinbreuk.[65]

Onzes inziens valt er veel te zeggen voor de toegangsbevoegdheid van de verdachte tot gegevens als criterium voor jurisdictie. Het biedt immers een goede oplossing voor het jurisdictieprobleem bij het grensoverschrijdend verzamelen van gegevens. Het moet daarbij wel gaan om de beschikkingsmacht van eigen burgers of personen op het eigen territorium. Dit vereiste zal bij de netwerkzoeking in de praktijk geen probleem zijn, omdat die noodzakelijkerwijze in het verlengde ligt van een zoeking op informatiesystemen in het eigen territorium. De toegangsbevoegdheid als criterium voor jurisdictie zorgt er in ieder geval voor dat het nationale recht van een land enkel wordt toegepast ten aanzien van personen die zich ook daadwerkelijk in dat land bevinden. Dat neemt echter niet weg dat bedrijven te maken zullen krijgen met overheden die onder hun eigen nationale regels toegang verschaffen tot accounts van hun klanten en dit kunnen aanmerken als een beveiligingsincident of zelfs aangifte kunnen doen van het strafbare feit computervredebreuk ('hacken'). Het criterium van toegangsbevoegdheid voor jurisdictie behoeft aldus nadere bestudering.[66]

4.6 *Een theoretische discussie?*

Het feit dat een grensoverschrijdende zoeking in de huidige computer-georiënteerde benadering in principe in strijd is met internationaal (straf)recht weerhoudt sommige staten er niet van onder omstandigheden toch ervoor te kiezen via internet de territoriale grenzen te overschrijden. De realiteit wijkt nu eenmaal soms af van de theorie, zeker wanneer grote (dikwijls economische) belangen op het spel staan.[67] In dat kader kan ook gewezen worden op de Amerikaanse uitzondering van 'exigent circumstances', waarbij grensoverschrijdende opsporingshandelingen toch onder omstandigheden kunnen worden toegepast. Die uitzonderingsgrond heeft meer bepaald betrekking op gevallen van levensgevaar of bij bedreiging van de nationale veiligheid.[68] Daarnaast lijken de sancties op een dergelijk grensoverschrijdend optreden in de praktijk vaak mee te vallen. In Nederland heeft de schending van de soevereiniteit van een land in veel gevallen geen consequenties voor de vervolging, omdat de verdachte niet direct in zijn rechten zou worden geschonden.[69] Er is dan ook opvallend weinig jurisprudentie over de 'bijzonder ingrijpende opsporingsbevoegdheid' te vinden.[70] Het gebrek aan jurisprudentie kan wellicht worden verklaard omdat verdachten weinig kans zien in een succesvol verzet tegen een dergelijke toepassing van de bevoegdheid. Het is tevens mogelijk dat de bijzondere opsporingsbevoegdheid in de praktijk weinig wordt toegepast.

Het Hof van beroep Brussel benaderde deze problematiek op een gelijkaardige wijze. In de uitspraak van 26 juni 2008 oordeelde het Brusselse Hof van beroep dat een gebrek aan notificatie van de buitenlandse betrokken staat, in strijd met art. 88 ter § 3 lid 2 B- Sv, niet tot bewijsuitsluiting moet leiden aangezien de rechten van verdediging er niet

64 J. Spoenle, 'Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?', Project on Cybercrime (discussion paper), augustus 2010. Beschikbaar via: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf (laatst geraadpleegd op 17 december 2012) (hierna: Spoenle 2012). Zie ook Hildebrandt & Koning die in dit verband stellen dat de extraterritoriale jurisdictie voor toegang op afstand 'de facto' als universele handhavingsjurisdictie kan worden gezien (Hildebrandt & Koning 2012, p. 198).

65 Spoenle 2012.

66 C. Conings en F. Verbruggen werken op dit ogenblik aan een publicatie over een alternatieve benadering van lokalisatie in cyberspace.

67 Zie ook De Hert 2006, p. 72-73: 'The presentation of concept is hiding a reality which is unwilling to subordinate itself to the legal principles of international law'.

68 Zie M.A. Sussmann, 'The Critical Challenges From High-Tech And Computer-Related Crime At The Millennium', *Duke Journal of Comparative & International Law* 1999, p. 451-490; J.L. Goldsmith, 'The Internet and the Legitimacy of Cross-border Searches', *University of Chicago Legal Forum* 2001, p. 103-118; en Bellia 2001, p. 35-101.

69 Met andere woorden: de *Schutznorm* wordt niet overtreden. Zie uitgebreid F.P.E. Wiemans, *Onderzoek van gegevens in geautomatiseerde werken* (diss. Tilburg), Nijmegen: Wolf Legal Publishers 2004, p. 157-163. Zie ook Melai Strafvordering, art. 125j Sv, aant. 6.2. De verdachte moet overigens zelf bezwaar maken tegen het vormverzuim, want de rechter toetst niet verplicht ambtshalve (Zie ook HR 30 maart 2004, *NJ* 2004/376, m.nt. Y. Buruma). B.J. Koops e.a. 2012 spreken ook wel over het 'wegschutz-normen' van de eventuele soevereiniteitsschending.

70 Onderzoek naar jurisprudentie heeft plaatsgevonden door middel van de zoektermen '125i Sv' en '125j Sv' in de databank van rechtspraak.nl.

door worden aangetast.[71] In het kader van de Belgische grensoverschrijdende netwerkzoeking hebben zich in de rechtspraak tot op heden voor justitie geen problemen voorgedaan. Bijgevolg lijkt er op dit vlak sprake van enige tolerantie. Dat staten tot op zekere hoogte de grensoverschrijdende aanpak lijken te gedogen maakt dat dit na verloop van tijd zou kunnen uitgroeien tot een internationaalrechtelijke gewoonte.[72]

5. Van een netwerkzoeking naar een online doorzoeking?

De online doorzoeking onderscheidt zich van de netwerkzoeking doordat deze vanaf de computers van de opsporingsinstanties zelf wordt uitgevoerd en zo een heimelijke opsporing faciliteert. In deze paragraaf staat de vraag centraal of er een juridische grondslag bestaat voor de (grensoverschrijdende) online doorzoekingsbevoegdheid.

5.1 *De online doorzoeking in de praktijk*

De behoefte van politie en justitie om bijvoorbeeld in webmailaccounts te kunnen kijken kan goed worden geïllustreerd met een beschrijving van een Rotterdamse drugszaak.[73]

Via een informant kwam de Criminele Inlichtingen Eenheid van de politie ter oren dat een Colombiaanse man naar Nederland zou reizen voor het in ontvangst nemen van een partij cocaïne. De informant wist bovendien dat de verdachte een Hotmailadres zou gebruiken voor het ontvangen en verzenden van e-mails met betrekking tot de boot waarin de cocaïne verborgen zat. Het komt vaker voor dat criminelen handig gebruikenmaken van de 'concept-optie' in webmail. Persoon A maakt dan een bericht aan en plaatst deze in de map concepten, waarna persoon B op hetzelfde account inlogt en het bericht leest. De e-mail kan vervolgens worden verwijderd zonder dat het wordt verstuurd.[74] In casu gaf de informant drie mogelijke wachtwoorden voor het account aan de politie, zodat de mogelijkheid tot kennisneming goed mogelijk werd.[75]

In eerste instantie vorderde de officier van justitie de opgeslagen gegevens van Microsoft in de Verenigde Staten, conform art. 126ng lid 2 N-Sv met een machtiging van rechtercommissaris. De officier van justitie wachtte de resultaten van de vordering echter niet af en gaf de opdracht aan een medewerker van de Digitale Expertise van het Korps Landelijke Politiediensten om in te loggen op het e-mailaccount. Uit de inhoud van twee e-mailberichten werd een schip met container met drugs geïdentificeerd en kort daarop werd de container met cocaïne aangetroffen.[76]

De officier van justitie rechtvaardigde 'de inkijk in het Hotmailaccount' door aan te voeren dat de gebruikersnaam en het wachtwoord rechtmatig via de informant waren verkregen. De inkijk was bovendien noodzakelijk omdat '*het wachten op de verlangde informatie van Microsoft Corporation te veel tijd zou kosten, (…) nu bekend was dat de partij cocaïne op korte termijn in Nederland zou aankomen*'. De officier van justitie erkende dat inbreuk was gemaakt op de soevereiniteit van de Verenigde Staten, maar stelde dat het belangenconflict zijn keuze rechtvaardigde.[77] In eerste instantie veroordeelde de rechter het handelen van de officier van justitie door op te merken dat de inkijk in het Hotmailaccount zonder toestemming van de gebruiker niet geoorloofd is en bovendien sprake was van een soevereiniteitsschending van de Verenigde Staten. Als sanctie paste de rechter strafvermindering toe op de opgelegde gevangenisstraf. In hoger beroep oordeelde het Hof 's-Gravenhage echter dat niet aan het Schutznorm-vereiste was voldaan: het Hotmailaccount behoorde niet toe aan de verdachte en daarom was geen inbreuk gemaakt op de rechtens te respecteren belangen van de verdachte.[78] Het gerechtshof ging verder niet in op de rechtmatigheid van de inkijk in het Hotmailaccount.

De vraag blijft onder welke opsporingsbevoegdheid de inkijk in een Hotmailaccount kan worden ondergebracht. Zowel in Nederland als in België biedt de netwerkzoekingsbevoegdheid daar naar onze mening onvoldoende grondslag voor, omdat de tekstuele uitleg van de wet dit niet toelaat. De netwerkzoeking ligt immers *in het verlengde van de doorzoeking* ter vastlegging van gegevens of de informaticazoeking. Enkele Belgische auteurs stellen dat aangezien de verdachte vanaf iedere computer toegang kan krijgen tot bepaalde delen van zijn netwerk (zoals zijn Hotmailaccount) de politie dit ook op afstand via internet kan in het kader van de netwerkzoeking.[79] Onder Belgisch recht is dat onzes insziens inderdaad te billijken, indien de zoeking met medeweten (en eventueel in aanwezigheid) van de verdachte zou gebeuren, aangezien politie en justitie op deze manier met gelijke waarborgen een gelijk resultaat bekomen. Het op heimelijke wijze toegang nemen ligt echter veel gevoeliger en vereist volgens vaste rechtspraak van het EHRM een duidelijke wettelijke grondslag met afdoende waarborgen.[80]

71 Brussel 26 juni 2008, *T. Strafr.* 2008, afl. 6, p. 467; Koops e.a. 2012, p. 38.

72 Zie ook Seitz 2005, p. 48-49 en De Hert 2006, p. 109.

73 Rb. Rotterdam 26 maart 2010, *LJN* BM2520 en Hof 's-Gravenhage 27 april 2011, *LJN* BR6836.

74 Zie R.C. van der Hulst & R.J.M Neve, *High-tech crime, soorten criminaliteit en hun daders*, Den Haag: WODC 2008, p. 46. Zie ook Koops e.a. 2012, p. 20.

75 Zie Rb. Rotterdam 26 maart 2010, *LJN* BM2520.

76 Rb. Rotterdam 26 maart 2010, *LJN* BM2520.

77 Rb. Rotterdam 26 maart 2010, *LJN* BM2520. Welk belangenconflict precies in het spel is wordt in de uitspraak niet duidelijk gemaakt. Mogelijk heeft het betrekking op het Nederlandse doorlaatverbod van art. 126ff N-Sv, welke onder omstandigheden een inbeslagnemingsverplichting voorschrijft.

78 Hof 's-Gravenhage 27 april 2011, *LJN* BR6836. Of een gedeeld account inderdaad niet toebehoort aan de verdachte is naar onze mening voor discussie vatbaar.

79 Van Linthout & Kerkhofs 2008, p. 90.

80 Zie algemeen: EHRM 25 maart 1983, *Publ. Eur. Court. H.R.* 1983, serie A, vol. 61, nr. 97 (*Silver e.a./Verenigd Koninkrijk*); het Hof vult deze voorwaarde bovendien strenger in in het kader van ernstige inbreuken op de privacy: EHRM 24 april 1990, *Publ. Eur. Court. H.R.* 1990, serie A, nr. 176-A (*Kruslin/Frankrijk*); EHRM 25 maart 1998, *Journ. Procès* 1998, nr. 347 (*Kopp/Zwitserland*).

5.2 *De digitale inkijkoperatie?*

Eventueel kan worden bepleit dat de artikelen omtrent de inkijkoperatie een wettelijke grondslag bieden voor het op afstand – via internet – inkijken in een account.[81] Het is echter in geen geval evident om de toepassingsvoorwaarden en doelen, omschreven in de wet met de fysieke inkijkoperatie in het achterhoofd, toe te passen in een virtuele context.[82] Het 'zoekend rondkijken' bij een inkijkoperatie is niet hetzelfde als een 'doorzoeking'. Hoe die grens getrokken moet worden in een virtuele context is niet duidelijk. Bovendien moeten de uitvoeringsagenten alles achterlaten in de aangetroffen staat. In een digitaal opsporingsonderzoek zal dit erg moeilijk te verwezenlijken zijn gelet op automatische processen die plaatsvinden wanneer verbinding wordt gemaakt met een account. Tijdens de inkijk zelf verandert de samenstelling van de gegevensdrager en bestaat bovendien de kans dat bijvoorbeeld nieuwe e-mails automatisch worden opgehaald en nieuwe loggegevens worden aangemaakt.

Naar onze mening is het daarom wenselijk dat de wetgever duidelijk maakt in hoeverre een online doorzoeking mogelijk is. Indien de wetgever de opsporingsmethode wenselijk vindt moet expliciet in een rechtsgrond worden voorzien die omgeven wordt door voldoende waarborgen. In ieder geval lijkt de Nederlandse Minister van Veiligheid en Justitie een eerste stap te zetten richting de online doorzoeking met de aankondiging van een conceptwetsvoorstel daartoe.[83] Daarbij zouden onlinesystemen tevens gehackt mogen worden teneinde toegang tot de gegevens te verkrijgen.

5.3 *De online doorzoeking en jurisdictie*

De vraag naar territoriale afbakening van opsporingsbevoegdheden stelt zich uiteraard eveneens in het kader van de online doorzoekingsbevoegdheid. Vanuit een computergeoriënteerde benadering kan de unilaterale online doorzoeking eveneens slechts betrekking hebben op informaticasystemen die op het nationale territorium zijn gelokaliseerd. Hier steekt het probleem van de '*loss of location*' bijgevolg eveneens de kop op.

De focus verleggen van de computer-georiënteerde benadering naar de beschikkingsmacht of toegangsbevoegdheid zou ook hier een oplossing kunnen bieden. De wetgever zou in dat geval de online doorzoeking niet formuleren ten aanzien van de plaats van opslag maar wel ten aanzien van een persoon, betrokken in de zaak, en diens virtuele toegangsbevoegdheid. Indien opsporingsinstanties echter niet weten aan wie een te doorzoeken account toekomt, doet zich in deze toegang-georiënteerde benadering een internationaalrechtelijk probleem voor. De opsporingsbevoegdheid mag immers slechts worden uitgeoefend ten aanzien van personen op het eigen territorium. De kans dat de betrokkene zich in het buitenland bevindt is echter reëel. Op internationaal vlak zou eventueel een beperkte, grensoverschrijdende bevoegdheid kunnen worden gecreëerd met het oog op identificatie en lokalisatie van de betrokkene. Het is daarbij echter de vraag of de politieke bereidheid er is om nieuwe afspraken te maken over grensoverschrijdende zoekingen. Opnieuw wensen we te benadrukken dat we ons beperken tot het aanstippen van een andere zienswijze, die een nadere bestudering en uitvoerige beargumentering behoeft.

6. Afsluitend

De online doorzoeking waarbij op afstand – via internet – heimelijk toegang wordt verschaft tot een besloten computersysteem is onzes inziens niet mogelijk op basis van de netwerkzoeking. De netwerkzoeking ligt immers steeds in het verlengde van een zoeking ter vastlegging van gegevens of een informaticazoeking, terwijl de online doorzoeking een op zichzelf staande opsporingsbevoegdheid zou betreffen. Het heimelijke karakter van de opsporingsbevoegdheid vraagt daarbij om een ondubbelzinnige, wettelijke grondslag.

De mogelijkheid van een grensoverschrijdende netwerkzoeking en online doorzoeking levert interessante rechtsvragen op die nader onderzoek vereisen. Het jurisdictieprobleem bij de grensoverschrijdende toepassing van opsporingsmethoden via internet zou daarbij in het bijzonder meer aandacht moeten krijgen van juristen. Het is naar onze mening belangrijk om in een door technologie constant veranderende wereld nieuwe visies naar voor te schuiven en niet krampachtig aan traditionele uitgangspunten te blijven vasthouden. Wij willen met deze bijdrage hiertoe een aanzet geven, door aan te geven dat de computer-georiënteerde benadering moeilijk werkbaar is en daarom wellicht best wordt verlaten. Het lijkt ons onlogisch de fysieke locatie van data, die in de virtuele wereld nauwelijks een rol speelt, als hoofdcriterium te gebruiken voor de afbakening van de bevoegdheid van opsporingsinstanties. In dit kader is het van groot belang criteria aan te reiken die werkbaar zijn in de praktijk en die kenbaar zijn vooraleer de opsporingsbevoegdheid wordt toegepast. De toegangsbevoegdheid van de verdachte als criterium voor jurisdictie is daarvoor wellicht een goed alternatief. Dit zou immers niet alleen een hele stap vooruit betekenen voor opsporingsinstanties die belast worden met bewijsvergaring via het internet. Tevens zouden burgers op die manier een helder zicht krijgen op de omstandigheden waarin en de voorwaarden waaronder de vertrouwelijkheid en integriteit van hun systemen door de overheid kan worden doorbroken. Het kenbaarheidsvereiste bij opsporingsmethoden is ten slotte een basisprincipe waar het EHRM ons al zo een 30-tal jaren op wijst.

81 Zie: C. Conings & P. Van Linthout, 'Sociale media. Een nieuwe uitdaging voor politie en justitie', *Panopticon* 2012, nr. 3, p. 219-220.

82 Zie ook J.J. Oerlemans, 'Hacken als opsporingsbevoegdheid', *DD* 2011/62, afl. 8, p. 895. Anders: J.L.M. Boek, 'Hacken als opsporingsmethode onder de Wet BOB', *NJB*, afl. 11, p. 589-593.

83 Zie *Kamerstukken II* 2012/13, 28 684, nr. 363 (brief van 15 oktober 2012). In de brief wordt expliciet gerefereerd naar de problematiek van cloud computing en de beperkingen voor de opsporing daardoor.