UNIVERSITEIT VAN TILBURG

Misdaad en opsporing in de wolken

Knelpunten en kansen van cloud computing *voor de Nederlandse opsporing*

Bert-Jaap Koops
Ronald Leenes
Paul De Hert
Sandra Olislaegers

Universiteit van Tilburg
TILT – Tilburg Institute for Law, Technology, and Society

oktober 2012

Colofon

Auteurs
prof.dr. Bert-Jaap Koops
prof.dr. Ronald Leenes
prof.dr. Paul De Hert
Sandra Olislaegers, LL.M.

Uitgave
Universiteit van Tilburg
TILT – Tilburg Institute for Law, Technology, and Society
Postbus 90153
5000 LE Tilburg

Opdrachtgever
WODC, Ministerie van Veiligheid en Justitie
Schedeldoekshaven 131
2511 EM Den Haag

Datum
oktober 2012

Inhoudsopgave

Afkortingen

BSv	Wetboek van Strafvordering [België]
BW	Burgerlijk Wetboek
CBP	College Bescherming Persoonsgegevens
CCV	Cybercrime-Verdrag
DDoS	distributed denial of service
EaaS	Exploits as a Service
EHRM	Europees Hof voor de Rechten van de Mens
EVRM	Europees Verdrag voor de Rechten van de Mens
HR	Hoge Raad
IaaS	Infrastructure as a Service
ICT	informatie- en communicatietechnologie
ISP	Internetaanbieder
MLAT	Mutual Legal Assistance Treaty
NJ	*Nederlandse Jurisprudentie*
p2p	peer-to-peer
PaaS	Platform as a Service
Rb.	Rechtbank
SaaS	Software as a Service
SHA	Secure Hash Algorithm
Sr	Wetboek van Strafrecht
Sv	Wetboek van Strafvordering
TOR	The Onion Router
Tw	Telecommunicatiewet
VM	virtuele machine
Wbp	Wet bescherming persoonsgegevens
Wiv 2002	Wet op de inlichtingen- en veiligheidsdiensten 2002
WODC	Wetenschappelijk Onderzoek- en Documentatiecentrum

Samenvatting

Achtergrond en vraagstelling
Cloud computing is het uitbesteden van gegevensbeheer of computerapplicaties aan een dienstverlener, waarbij gegevens – meestal zonder regie over de precieze locatie – verspreid over verschillende servers worden opgeslagen. Verschijningsvormen die 'typisch' cloud computing zijn, zijn emaildiensten als Gmail en Hotmail, diensten voor opslag of delen van bestanden (zoals DropBox of Megaupload), applicatiediensten als Google Docs en ontwikkelplatforms als Amazon AWS. De verwachting is dat cloud computing een belangrijk onderdeel gaat vormen van het Internetlandschap. Dat leidt tot verschuivingen in patronen van gegevensverwerking en gegevensopslag. In essentie betekent dit dat gegevens niet meer in het bedrijf of bij mensen thuis opgeslagen liggen, maar elders. Dit kan tot kwetsbaarheden leiden, zowel bij bedrijven en burgers die de controle over gegevens uit handen geven, als bij opsporingdiensten die in de praktijk sterk leunen op locaal onderzoek van gegevens. Cloud computing heeft dus potentieel belangrijke gevolgen voor het plegen van gegevensgerelateerde criminaliteit en voor digitale opsporing en vervolging van misdrijven.

Dit biedt aanleiding voor een verkennend onderzoek naar de feitelijke en potentiële gevolgen van cloud computing voor de Nederlandse opsporing en vervolging van misdaad. Dit rapport geeft een antwoord op twee vragen: wat zijn (mogelijke) problemen en kansen van cloud computing voor het plegen van strafbare feiten en voor de opsporing en vervolging van strafbare feiten in en vanuit Nederland? En wat zijn geschikte richtingen om gesignaleerde problemen aan te pakken en gesignaleerde kansen voor misdaadbestrijding te benutten?

Het onderzoek is uitgevoerd door middel van literatuuronderzoek en bevraging van deskundigen, via vijf interviews met Nederlandse experts en een kleine enquête onder buitenlandse deskundigen.

Criminaliteit en materieel strafrecht
De rechtspraktijk kent nog weinig gevallen van criminaliteit waarin de cloud een substantiële rol heeft gespeeld. Het is wel bekend dat clouddiensten worden gebruikt voor opslag en uitwisseling van illegaal materiaal en voor het plegen van botnetaanvallen, maar hierin verschilt de cloud niet direct van andere Internetgebaseerde diensten. Er lijken geen bijzondere aspecten te bestaan die cloudgerelateerde criminaliteit substantieel anders maken dan andere vormen van cybercriminaliteit voor wat betreft het materiële strafrecht. Het Wetboek van Strafrecht (Sr) lijkt vooralsnog voldoende geschikt te zijn om criminaliteit gepleegd in of via de cloud te kunnen vervolgen.

Op twee onderdelen kan worden bekeken of aanpassingen wenselijk zijn. Ten eerste zou de wetgever nader kunnen onderzoeken of bepalingen betreffende telecommunicatieaanbieders van toepassing zijn of zouden moeten zijn op cloudopslagaanbieders. Nu mensen hun bestanden langdurig toevertrouwen aan Internetdienstverleners, gaat het immers niet alleen om bescherming van communicatie maar ook om bescherming van aan dienstverleners toevertrouwde gegevens in het algemeen. Het ligt voor de hand om art. 273d Sr (het verbod voor telecomaanbieders om kennis te nemen van de inhoud van aan hen toevertrouwde informatie) in dat licht uit te breiden tot opslagaanbieders.

Ten tweede zou de wetgever kunnen afwegen of het kraken van wachtwoorden en versleutelde bestanden, dat door de rekenkracht van cloudinfrastructuur gefaciliteerd wordt, dusdanig gevaarzettend is dat dit zelfstandig strafbaar gesteld zou moeten worden. Een alternatief is om te volstaan met zelfregulering door cloudaanbieders, waarbij de reeds bestaande strafbepalingen die het misbruik van (al dan niet gekraakte) wachtwoorden strafbaar stellen (zoals hacken en oplichting) als vangnet dienen.

Opsporing in de cloud
De ervaringen met cloud computing in opsporing en vervolging in de praktijk lijken tot nu toe gering, zowel in Nederland als in het buitenland. De enige uitzondering betreft de al lang bestaande webmaildiensten, die regelmatig in opsporingsonderzoeken voorkomen. De

verwachting is dat cloud computing wel binnen afzienbare tijd aanzienlijke uitdagingen voor de opsporing zal opleveren.

Ten eerste roept het wettelijke kader enkele juridische vragen en knelpunten op. Het is onduidelijk wanneer precies een cloudaanbieder als een communicatieaanbieder of openbare telecommunicatieaanbieder kan worden gekwalificeerd. Verder maakt het Wetboek van Strafvordering een onderscheid tussen opgeslagen en getransporteerde gegevens en tussen communicatie en niet-communicatie. Bij cloudopslag- en verwerkingsdiensten zijn deze onderscheiden soms moeilijk te maken en lijken ze ook minder relevant te worden. Ook versterkt de opkomst van cloud computing, samen met het toenemend gebruik van versleuteling, de al bestaande vraag of het noodzakelijk is om een bevoegdheid in te voeren waarmee de politie heimelijk op afstand toegang kan krijgen tot computers van verdachten.

Ten tweede zal de opsporingspraktijk een omslag moeten maken om in te spelen op de verschuiving van gegevens van harde schijf naar cloud. Bij doorzoekingen zal men zich, meer dan momenteel al gebeurt, moeten richten op onderzoek van geactiveerde computers, om het werkgeheugen en openstaande verbindingen (bijvoorbeeld met clouddiensten) veilig te stellen. De klassieke doorzoeking en de klassieke telefoontap zullen geleidelijk aan plaats moeten maken voor meer Internettaps, waar praktijk en wetgeving momenteel nog niet goed op zijn ingespeeld.

Een derde en belangrijkste constatering is dat de meest gebruikte methoden om digitale gegevens te verzamelen (doorzoeking, vorderen van gegevens, onderscheppen van gegevens) beperkingen hebben bij gegevens die in een cloud liggen opgeslagen of wanneer via de cloud worden gecommuniceerd. Het voornaamste knelpunt daarbij vormen de territoriale grenzen waaraan de Nederlandse opsporing nog steeds is gebonden. Aangezien een grensoverschrijdende netwerkzoeking niet is toegestaan (behalve in de weinig voorkomende gevallen van toestemming van de verdachte of vrijwillige medewerking van een buitenlandse aanbieder), moet justitie zich verlaten op wederzijdse rechtshulp met een vordering aan de buitenlandse cloudaanbieder om gegevens te leveren. Dat is geen nieuw gegeven: cyberopsporing heeft van oudsher al te maken met vragen rond grensoverschrijdende toegang tot gegevens. Deze vragen worden echter op scherp gesteld door de het verlies aan locatie (‘loss of location’) dat de cloud met zich meebrengt. Bestanden die in de cloud liggen opgeslagen, zijn veelal in meerdere kopieën en in stukjes opgeknipt opgeslagen op verschillende servers, waarbij het systeem zelf, op basis van vraag en aanbod, de meest efficiënte opslag berekent en bestanddelen verplaatst. Het is daarom op vrijwel elk moment moeilijk te bepalen, ook voor de cloudaanbieder zelf, op welk(e) plaats(en) een bestand ligt opgeslagen. De locatie waar gegevens ‘zich bevinden’ werkt niet meer als leidend aanknopingspunt bij de bepaling van rechten en plichten in relatie tot de cloud.

Op het concrete niveau van de praktijk is het ‘verlies van locatie’ bijzonder relevant, in het bijzonder in de strafvorderlijke context waar territoriale soevereiniteit nog altijd een zeer bepalende rol speelt. Wanneer de gegevenshuishouding van misdadigers migreert naar de cloud, zal de Nederlandse opsporingspraktijk hard tegen de territoriale beperkingen oplopen. Dit vraagt om aandacht van wetgeving en beleid. Nederland zal moeten investeren in samenwerking, zowel met buitenlandse overheden als met cloudaanbieders. Verdere stroomlijning van procedures rond (rechtshulp)verzoeken is van wezenlijk belang voor opsporing in de cloud.

Ook op het abstracte niveau van de theorievorming rond jurisdictie en soevereiniteit is het verlies van locatie belangrijk. De theorie kent grofweg twee scholen: de ‘cybernauten’ en de ‘territorialisten’. De laatsten, die cyberspace niet als zelfstandige ruimte benaderen maar de nadruk leggen op de fysieke plaats van servers en routerende computers, zullen terrein moeten prijsgeven aan de eersten wanneer cloud computing een vaste plaats verovert in het internationale Internetlandschap. Dit sluit aan bij literatuur over de cloud die, voor de bepaling van rechtsmacht, aanknopingspunten zoekt bij de plaats(en) van degenen die beschikkingsmacht hebben over gegevens (zoals de aanbieder en de klant) in plaats van bij de locatie van de server waar de gegevens opgeslagen liggen.

Dit betekent ook de cloud het klassieke strafrechtelijke model om alles via rechtshulp te laten verlopen, uitdaagt en dat nadere reflectie nodig is op de rol van soevereiniteit bij de opsporing van strafbare feiten. Mede vanwege de moeilijke bepaalbaarheid van de locatie van gegevens in de cloud, alsook omdat opsporing in de cloud soms om snelle actie vraagt waarvoor rechtshulp – hoe gestroomlijnd ook – te traag kan zijn, zijn er goede argumenten om een grensoverschrijdende netwerkzoeking toe te staan. Het Belgische model, om onder bepaalde voorwaarde een doorzoeking uit te breiden tot netwerkverbindingen over de grens met

aansluitend notificatie aan de desbetreffende staat, zou daarbij als inspiratie kunnen dienen. Daarnaast is ook de vraag onder welke voorwaarden Nederland het toelaatbaar acht voor justitie om zich rechtstreeks te wenden tot buitenlandse aanbieders in plaats van via de weg van rechtshulp. Voor beide zou vanzelfsprekend het reciprociteitsbeginsel moeten gelden: Nederland mag gegevens uit het buitenland vergaren als het buitenland dat ook in Nederland mag. Op deze manier zou de soevereiniteit in een genetwerkte wereld een moderne invulling kunnen krijgen.

Vervolging en de cloud: bewijsaspecten

Naast knelpunten in de opsporing ontstaan mogelijk ook knelpunten in de vervolging, wanneer bewijs 'uit de cloud' afkomstig is waarvan de betrouwbaarheid betwist kan worden in de rechtszaal. Procedures en standaarden voor bewijsvergaring uit de cloud zijn nog in een vroeg stadium van ontwikkeling en nog niet getoetst in de rechtspraktijk. Materiaal dat op verzoek of vordering van buitenlandse cloudaanbieders wordt verkregen, kent technische en enigermate ook juridische risico's voor gebruik als bewijs.

Technisch is het niet eenvoudig bewijsbaar, gezien de gedistribueerde en geautomatiseerd-dynamische opslag, dat een document dat uit de cloud wordt gehaald hetzelfde is als dat wat erin is gestopt. Het zal niet altijd duidelijk zijn welke forensische procedures de cloudaanbieder gehanteerd heeft om het document te verkrijgen; momenteel ontbreken vaak ook technische voorzieningen in de cloudinfrastructuur die voor forensisch onderzoek nodig zijn (zoals logs en *audit-trails*). Er is daarom behoefte aan de ontwikkeling van procedures en standaarden, alsmede aan nauwe samenwerking met cloudaanbieders om basisvoorzieningen voor forensisch onderzoek in cloudinfrastructuren en -praktijken in te bouwen.

Formeel-juridisch zijn er niet veel complicaties te verwachten bij cloudbewijs. Bewijs dat uit het buitenland wordt verkregen, kan als zodanig worden gebruikt. In sommige situaties – als de verdediging de toelaatbaarheid of betrouwbaarheid betwist – zal de officier van justitie wel de rechtmatigheid en betrouwbaarheid van cloudbewijs nader moeten motiveren. Of dat substantiële problemen zal opleveren – meer dan bij andere vormen van digitaal bewijs – zal de rechtspraktijk moeten uitwijzen.

Kansen

Hoewel de onderzoeksbronnen zich hoofdzakelijk richten op bedreigingen, biedt de cloud op drie vlakken ook mogelijke kansen voor opsporing en vervolging. De belangrijkste is dat door de migratie van gegevens van de harde schijf van verdachte naar de cloud er in potentie meer gegevens binnen bereik komen om heimelijk te onderzoeken, voordat de verdachte via een doorzoeking wordt gealerteerd op het feit dat er een opsporingsonderzoek loopt. Met een Internettap of gegevensbevraging (met oplegging van geheimhouding) bij de cloudaanbieder kunnen nu ook gegevens worden vergaard die vroeger alleen via een doorzoeking en onderzoek van de harde schijf in beeld kwamen. Hierdoor kan het vooronderzoek langer doorlopen, wat bij bepaalde onderzoeken tactische voordelen zal hebben. Deze kans kan echter alleen worden benut als de knelpunten ten aanzien van cloudopsporing, in elk geval rond de Internettap en de 'locatiegerichte' opsporingspraktijk, worden aangepakt.

De andere vlakken waarop potentiële kansen bestaan liggen in de rekencapaciteit van de cloud, die door justitie zou kunnen worden benut om bijvoorbeeld versleutelde bestanden te kraken, en in de opslagcapaciteit van de cloud, die een kostenefficiënte oplossing zou kunnen bieden voor de grote hoeveelheden data die de politie bewaart. Het gebruiken van rekencapaciteit betreft een relatief klein onderdeel van de politiepraktijk en zou zonder veel obstakels kunnen worden uitgevoerd, maar het benutten van cloudopslagcapaciteit voor politiegegevens is een complex vraagstuk dat nadere reflectie vergt. Meer onderzoek en een complexe beleidsafweging is nodig of de mogelijke kostenbesparing opweegt tegen de (afbreuk)risico's van cloudopslag van politiegegevens.

Conclusies en oplossingsrichtingen

Cloud computing heeft als zodanig weinig fundamenteel nieuwe gevolgen voor opsporing en vervolging. Het roept wel enkele vragen op over de toepassing van het straf(proces)recht, maar dat zijn vragen die passen binnen het reguliere 'groot onderhoud' dat de wetgeving rond cybercriminaliteit sowieso moet plegen. Toch kunnen de verschuivingen die cloud computing teweegbrengt, wel degelijk verschil maken. Bij nadere beschouwing heeft de opkomst van de

cloud namelijk wel degelijk belangrijke gevolgen, doordat de migratie van gegevensverwerking naar de cloud bepaalde ontwikkelingen en al langer bestaande problemen op scherp stelt. Dat heeft vooral te maken met het feit dat het 'verlies van locatie' van de cloud een fundamentele uitdaging vormt voor de territoriaal georiënteerde strafvordering. Die uitdaging zou opgepakt moeten worden op het niveau van wetgeving, beleid en praktijk.

Voor de wetgever past een herbezinning op de systematiek van het materiële en procedurele strafrecht in relatie tot Internetaanbieders, bijvoorbeeld de reikwijdte van de begrippen communicatie- en telecommunicatieaanbieder en het onderscheid tussen stromende en opgeslagen gegevens. Ook zou de grondwetgever bij de herziening van art. 13 Grondwet de rol van clouddiensten moeten meenemen wanneer hij het object en de reikwijdte van het (tele)communicatiegeheim opnieuw inkadert. Verder zou de wetgever zich kunnen buigen over de adequaatheid van sommige opsporingsbevoegdheden om gegevens uit de cloud te vergaren, zoals de voorwaarden waaronder een netwerkzoeking (art. 125j Sv) binnen Nederland kan worden uitgevoerd; een vraag is bijvoorbeeld of het onderscheid bij de doorzoeking in rechtsbescherming tussen voertuigen, plaatsen en woningen (art. 96b, 96c, 97/110 Sv) nog terecht is wanneer gegevens vanaf elke plaats toegankelijk zijn. Ook de juridische knelpunten rond de Internettap (betreffende onder andere verbalisering, geheimhoudergegevens en selectie vooraf) verdienen aandacht. Tot slot maakt de cloud de reeds bestaande vraag prangender of, en zo ja onder welke voorwaarden, een bevoegdheid tot heimelijke toegang op afstand ('hacken' door plaatsing van een afluisterprogrammaatje) zou moeten worden ingevoerd.

Voor het beleid ligt er ten eerste de uitdaging om barrières op te werpen die het plegen van cloudcriminaliteit in en vanuit Nederland moeilijker maken. Voor cybercriminaliteit, inclusief de mogelijkheden die de cloud daarvoor biedt, zou een barrièremodel kunnen worden ontwikkeld, waarin voor elke stap in het plegen van (cloudgerelateerde) cybercriminaliteit interventiemogelijkheden worden gesignaleerd gericht op de misdadiger, burgers en bedrijven, Internetaanbieders en overheid. Een tweede beleidsveld is de beveiliging van cloud computing. Het stimuleren daarvan past binnen het bredere beleid rond cybersecurity, zeker wanneer de cloud meer het karakter krijgt van een vitale infrastructuur als belangrijke gegevensprocessen in substantiële mate worden verplaatst naar de cloud. Beveiliging van de cloud zou dan ook op de agenda moeten staan van de Nationale Cyber Security Raad. Ten derde ligt er voor het beleid de uitdaging om een strategie te ontwikkelen voor het omgaan met het 'verlies van locatie'. Dat betekent naast investeren in samenwerking met buitenlandse overheden en cloudaanbieders vooral ook een herbezinning op de invulling die Nederland wil geven aan soevereiniteit in een genetwerkte samenleving. Het klassieke strafrechtelijke model om alles via rechtshulp te laten verlopen, zal in toenemende mate tegen zijn eigen grenzen aanlopen. Nederland zou moeten bepalen hoever zij zelf zou willen gaan in het grensoverschrijdend vergaren van gegevens uit het buitenland – gekoppeld aan de reciproke bereidheid om toegang toe te staan van buitenlandse autoriteiten tot in Nederland opgeslagen gegevens.

Voor de praktijk ligt er, naast het beter leren omgaan met computerdoorzoekingen en Internettaps, vooral de uitdaging om een weg te vinden in de omgang met bestaande bevoegdheden en de beperkingen daarvan, zolang de juridische knelpunten – waaronder de territoriale begrenzing – niet zijn opgelost. Over het algemeen zal justitie de koninklijke weg van rechtshulp moeten blijven bewandelen. In uitzonderlijke en urgente gevallen – wanneer rechtshulp niet goed werkt – zou de praktijk echter misschien kunnen experimenteren met niet-koninklijke maatregelen. Transparantie en het afleggen van verantwoording zijn daarbij cruciaal, zodat de activiteit in rechte getoetst kan worden en de rechtsontwikkeling een stap verder komt. Niet-koninklijke maatregelen in cloud-opsporing – ook als ze alleen sturingsinformatie opleveren – zouden daarom altijd in het strafdossier moeten worden vermeld. Dat zal dan ook de urgentie onderstrepen voor wetgever en beleidsmakers om in supranationaal verband te komen tot een betere regeling van grensoverschrijdende gegevensvergaring in het tijdperk van cloud computing.

Samenvattend kunnen we concluderen dat cloud computing vooralsnog meer knelpunten dan kansen oplevert voor de opsporing en vervolging van strafbare feiten. Als wetgeving, beleid en praktijk echter in staat zijn de handschoen op te pakken en een nieuwe, systematische en uitgebalanceerde regeling en praktijk ontwerpen voor opsporing in de cloud, kan van deze nood een deugd worden gemaakt. Vroeg of laat zullen ook de strafrechtelijke rechtsleer en rechtspraktijk in een ICT-samenleving moeten leren leven met het verlies van locatie. Dat kan maar beter vroeg dan laat zijn.

1. Inleiding

1.1. Achtergrond

Cloud computing is een verzamelterm voor het via Internet aanbieden van gegevensverwerkingsdiensten in de vorm van opslag- en rekencapaciteit. Vanwege de flexibiliteit en schaalbaarheid levert dit aantrekkelijke mogelijkheden op voor bedrijven en individuen om goedkoop en laagdrempelig gegevensverwerkingsdiensten af te nemen. Steeds meer bedrijven stappen dan ook over op clouddiensten, die vaak in de plaats komen van hardware, software en gegevensopslag bij en door het bedrijf zelf. Ook individuen maken toenemend gebruik van clouddiensten, zoals Google Docs, Google Drive, Dropbox en iCloud. Cloud computing wordt daarmee, zo is de verwachting, een belangrijk onderdeel van het Internetlandschap.

Cloud computing kent naast kansen ook bedreigingen. Misdadigers kunnen de cloud gebruiken om cybercriminaliteit te plegen, terwijl de opsporing en vervolging van (cyber)misdaad kan worden bemoeilijkt, bijvoorbeeld door het grensoverschrijdende karakter van de cloud en het toenemende gebruik van versleuteling van gegevens.

Het is daarom belangrijk om zicht te krijgen op de gevolgen van de opkomst en het toenemend gebruik van cloud computing voor de toepassing van het strafrecht en de strafvordering. Dit is tot op heden nog niet systematisch onderzocht. In de literatuur wordt veel aandacht besteed aan privacy en de bescherming van persoonsgegevens, contractuele aspecten en beveiligingsaspecten.[1] In sommige literatuur worden strafrechtelijke deelaspecten besproken, zoals forensisch bewijs[2] en toegang tot in de cloud opgeslagen gegevens door (ook buitenlandse) opsporingsdiensten.[3] Een geïntegreerd overzicht van de materieelrechtelijke en strafvorderlijke aspecten van cloud computing is echter niet voorhanden. Bovendien is de problematiek van cloud & strafrecht nog niet onderzocht vanuit Nederlands perspectief en naar het Nederlandse recht.

Deze achtergrond gaf aanleiding voor het WODC van het Ministerie van Veiligheid en Justitie een verkennend onderzoek te laten uitvoeren naar de mogelijke gevolgen van cloud computing voor opsporing en vervolging van criminaliteit in Nederland. Daarbij zou zowel aandacht moeten worden besteed aan mogelijke problemen als aan mogelijke kansen voor criminaliteitsbestrijding. Het Tilburg Institute for Law, Technology, and Society (TILT) heeft in opdracht van het WODC dit onderzoek uitgevoerd, in de periode december 2011 tot juli 2012. De rapportage is afgerond in oktober 2012.

1.2. Doelstelling en vraagstelling

De **doelstelling** van dit onderzoek is inzicht te bieden in de feitelijke en potentiële gevolgen van cloud computing voor de Nederlandse opsporing en vervolging van misdaad, teneinde bij te dragen aan de Nederlandse bestrijding van (cyber)criminaliteit. Daarbij moet duidelijk worden gemaakt welke knelpunten en kansen zich voordoen in de opsporing en vervolging vanuit Nederland wanneer (mogelijk) strafbare feiten worden gepleegd in of via de cloud.

De **vraagstelling** die centraal staat is tweeledig:

> Wat zijn (mogelijke) problemen en kansen van cloud computing voor het plegen van strafbare feiten en voor de opsporing en vervolging van strafbare feiten in en vanuit Nederland? Wat zijn geschikte oplossingsrichtingen voor gesignaleerde problemen en hoe kunnen gesignaleerde kansen voor misdaadbestrijding worden benut?

1.3. Afbakening

Deze studie heeft een verkennend karakter naar een nieuw fenomeen dat nog niet systematisch in kaart is gebracht. Daarom is gekozen voor een korte schets van mogelijk relevante aspecten, waarbij alleen die aspecten nader worden uitgediept die hetzij van essentieel belang zijn voor de

[1] Zie bijvoorbeeld Cuijpers et al. 2011; Cavoukian 2008.
[2] Bijvoorbeeld Ruan e.a. 2011a; Taylor e.a. 2010.
[3] Walden 2011.

Nederlandse strafrechtspraktijk, hetzij illustratief zijn voor de karakteristieke eigenschappen van de cloud. Dat betekent dat waar de cloud vormen van misdaad of van opsporing faciliteert of bemoeilijkt op eenzelfde manier als andere verschijningsvormen van Internet of cybercrime, we volstaan met een korte aanduiding en verwijzing naar bestaande literatuur. Het onderzoek is verder beperkt tot commune delicten (dat wil zeggen strafbare feiten zoals strafbaar gesteld (of te stellen) in het Wetboek van Strafrecht) en tot commune strafvordering (dat wil zeggen reguliere opsporing en vervolging van strafbare feiten zoals geregeld (of te regelen) in het Wetboek van Strafvordering).

1.4. Methoden van onderzoek

Vanwege het verkennende karakter is gekozen voor een combinatie van literatuuronderzoek en bevraging van deskundigen. Het literatuuronderzoek is gebaseerd op academische publicaties, beleidsrapporten en rapporten en *position papers* van (internationale) overheden, organisaties en bedrijven, in de technische, juridische en organisatorische disciplines.

De bevraging van deskundigen bestond uit een aantal interviews met deskundigen in Nederland en een kleine enquête onder buitenlandse deskundigen. Er zijn vijf semi-gestructureerde interviews gehouden met sleutelfiguren bij politie, Openbaar Ministerie en bedrijfsleven die veel ervaring hebben met cybercriminaliteit. Deze interviews bieden geen generaliseerbare inventarisatie van de ervaringen met of meningen over 'cloudmisdaad' in Nederland, maar wel een kwalitatieve inventarisatie van illustratieve ervaringen en relevante verwachtingen en standpunten. Verder is onder buitenlandse deskundigen in het netwerk van de onderzoekers een korte vragenlijst verspreid. Hierin is gevraagd naar ervaringen en lopende of afgeronde zaken waarin de cloud een substantiële rol speelt of heeft gespeeld, alsook wat naar de mening van deze deskundigen de grootste knelpunten zijn voor opsporing en vervolging van strafbare feiten in de cloud. De ervaringen en standpunten uit het buitenland zijn gebruikt om de veldverkenning te completeren. Bijlage 1 geeft een overzicht van de geïnterviewde personen en respondenten.

1.5. Leeswijzer

Het rapport begint met een beschrijving van cloud computing; om een goed begrip te krijgen van wat cloud computing wel of niet is, wordt daarbij ook ingegaan op enkele aanpalende fenomenen (hfd. 2). Vervolgens worden de – tot nu toe beperkte – ervaringen beschreven in Nederland en het buitenland met misdaad en opsporing in de cloud (hfd. 3). De kern van het rapport bestaat vervolgens uit een beschrijving en analyse van de mogelijke gevolgen van cloud computing voor het plegen van misdrijven (materieel strafrecht, hfd. 4), opsporing van misdrijven (procedureel strafrecht, hfd. 5) en vervolging van misdrijven (forensisch onderzoek en bewijsrecht, hfd. 6). In de conclusie worden de belangrijkste knelpunten en kansen van cloud computing voor de misdaadbestrijding samengevat, waarna oplossingsrichtingen worden geschetst om knelpunten aan te pakken en kansen te benutten (hfd. 7).

Lezers met beperkte tijd kunnen volstaan met de conclusie en, voor degenen die vooral geïnteresseerd zijn in vormen van cloudcriminaliteit en de technisch-organisatorische kant van opsporing, de analyses in par. 4.3, 5.2.5 en 6.1, terwijl voor degenen met een primair juridische interesse met name de analyses in par. 4.4, 4.5, 5.2 en 6.2 relevant zullen zijn.

2. Cloud computing en aanpalende begrippen

2.1. Cloud computing

In de jaren ’70 en ’80 van de vorige eeuw werden computerfaciliteiten centraal in rekencentra aangeboden die door gebruikers decentraal werden benaderd via ‘domme’ terminals. Begin jaren ’80 doet de pc zijn intrede en verschuift serieuze rekenkracht naar het bureau van de eindgebruiker. Gelijk met de ontwikkeling van computers zijn ook computernetwerken ontstaan, zowel locaal (Local Area Networks) als bovenlocaal (Wide Area Networks). In de jaren ’90 breekt het Internet door bij het grote publiek. Lokale, dat wil zeggen op de computer van de eindgebruiker draaiende, applicaties en lokale dataopslag worden gecombineerd met het gebruik van (eenvoudige) diensten op Internet. In het nieuwe millennium zien we vervolgens weer een verschuiving naar diensten die conceptueel vergelijkbaar zijn met het klassieke client-server-model[4]. Steeds vaker wordt gebruik gemaakt van applicaties die zich niet op de pc van de gebruiker bevinden, maar ‘ergens’ bij een aanbieder die de dienst via Internet beschikbaar stelt – een Application Service Provider. Geleidelijk aan worden de data daarbij niet langer op de lokale server van de dienstaanbieder opgeslagen, maar verspreid over meerdere servers of serverparken op verschillende locaties. Dit vernieuwde client-server-model is op een bepaald moment aangeduid als cloud computing. De term ‘cloud’ vloeit voort uit de gewoonte om in grafische weergaven van computermodellen een wolk te gebruiken als aanduiding voor het netwerk waarbinnen gegevensverwerking plaatsvindt.

Deze korte geschiedenis van IT-gebruik laat zien dat er in zekere zin weinig nieuws onder de zon is en dat het tevens lastig is een strikt onderscheid te maken tussen cloud computing en andere vormen van gegevensverwerking via netwerken. Cloud computing is gebaseerd op het Internet en clouddiensten zijn doorgaans webgebaseerde diensten.[5] Het gaat echter te ver om iedere webgebaseerde dienstverlening via Internet aan te duiden als cloud computing, omdat cloud computing dan de facto synoniem wordt met het Web. Webpagina’s die informatie ter beschikking stellen voor het publiek vallen bijvoorbeeld niet onder het begrip cloud computing.

Om scherper voor ogen te krijgen wat cloud computing is en wat daarbij komt kijken is het nodig een werkdefinitie te hanteren. Vaak wordt gebruik gemaakt van de **definitie** die door het Amerikaanse standaardisatie instituut NIST is opgesteld. NIST definieert cloud computing als:

> a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[6]

Hierbij vermeldt NIST ook een verzameling karakteristieken en vormen van beheer, die het begrip nader inkleuren. Voordat we daarop ingaan, is het goed om eerst verschillende **typen diensten** te onderscheiden. Met betrekking tot diensten die worden aangeboden in de cloud wordt doorgaans een onderscheid gemaakt tussen Software as a Service (SaaS), Platform as a Service (PaaS) en Infrastructure as a Service (IaaS).

Bij SaaS gaat het om applicaties die via Internet toegankelijk zijn voor eindgebruikers en die een bepaalde functionaliteit bieden. De applicatie ‘draait’ ofwel op de hardware van de aanbieder van de applicatie, maar vaker zal (een deel van de) benodigde functionaliteit tijdelijk worden gedownload door de apparatuur van de gebruiker (computer, smartphone, tablet). Dit gebeurt volledig transparant voor de gebruiker. De gebruiker heeft doorgaans slechts te maken met haar Internetbrowser, die als onderdeel van het normale webverkeer de benodigde software (vaak JAVA of Javascript) ophaalt van de website van de aanbieder. Wanneer de gebruiker de browser sluit wordt de applicatiesoftware automatisch verwijderd. Voorbeelden van SaaS zijn eenvoudige

[4] Zie http://en.wikipedia.org/wiki/Client%E2%80%93server_model (geraadpleegd 3 juli 2012).
[5] Daarmee bedoelen we diensten die via het http-protocol lopen. Dit is niet hetzelfde als webservices. Webservices zijn machine-machine-processen die via een netwerk verlopen. Webgebaseerde diensten worden gebruikt door menselijke eindgebruikers.
[6] Mell & Grance 2011.

diensten zoals e-mail (bijv. Hotmail) en voorzieningen voor opslag of delen van bestanden (bijv. DropBox, Megaupload), maar ook meer complexe toepassing zoals Office-achtige applicaties (bijv. Google Docs) vallen hier onder.[7] Eigenlijk iedere applicatie die middels een browser kan worden gebruikt, kan als SaaS worden aangeboden. Dat maakt naar ons idee nog niet dat iedere webapplicatie daarmee een SaaS-applicatie is, dat hangt namelijk af van de vraag in hoeverre de dienst voldoet aan de algemene eigenschappen van cloud computing diensten (zie hieronder).

Een variant van SaaS die gebruikt wordt in de ondergrondse markt van cybercriminaliteit, is *Exploits as a Service* (EaaS).[8] Het gaat hier om het leasen van een specifiek type applicatie, 'exploits'. Exploits maken gebruik van fouten (bugs) en zwaktes in systemen om daarmee gerichte aanvallen tegen deze systemen uit te voeren. Dergelijke exploits zijn al langer te koop, maar de cloud computing-variant biedt voor criminele gebruikers voordelen omdat ze altijd over de meest actuele versie beschikken van de 'aanvalssoftware' en gebruik kunnen maken van de infrastructuur van de (illegale) dienstaanbieder.

Bij *Platform as a Service* biedt de Cloud Service Provider een computer- en softwareplatform aan waarop de klant zelf diensten en voorzieningen kan ontwikkelen. Een voorbeeld hiervan is Amazon AWS.[9] Klanten kunnen binnen AWS zelf websites en webapplicaties bouwen die ze ter beschikking kunnen stellen aan hun gebruikers en/of klanten.[10] Voorbeelden van producten die zijn gebouwd op het AWS-platform zijn de bekende filmdatabank IMDb, online winkel Etsy waar eenieder producten kan verkopen, foursquare (een locatiegebaseerd sociaal netwerk), Unilever dat een combinatie van Amazonproducten gebruikt voor biotech- en informaticainnovatie, en Virgin Atlantic die hun VTravelled.com site bij Amazon heeft ondergebracht.

Infrastructure as a Service gaat een stap verder in het uitplaatsen van hardware en software. De Cloud Service Provider levert hier in wezen hardware die via het Internet kan worden benaderd. De klant kan hierop iedere gewenste software installeren, van besturingssysteem (Windows, Linux, Mac OS) tot en met de daarop draaiende applicaties. IaaS maakt het daarmee mogelijk om lokaal met eenvoudige hard- en software te volstaan en krachtige hardware en software van elders te gebruiken.

Mell en Grance beschrijven vijf **kernkarakteristieken** van cloud computing: *on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service*.[11] Deze karakteristieken helpen om cloud computing te onderscheiden van andere Internetdiensten.

Met *On-demand self-service* wordt aangegeven dat gebruikers eenzijdig bepaalde IT-faciliteiten kunnen inschakelen zonder daarbij een beroep te hoeven doen op menselijke tussenkomst.

Diensten worden via netwerken, in het bijzonder het Internet, aangeboden via standaard protocollen en voorzieningen (*broad network access*). Bij SaaS gaat het daarbij vooral om toepassingen die via webbrowsers worden benaderd, maar bij PaaS en IaaS kunnen ook andere communicatieprotocollen worden gebruikt om toegang te verkrijgen tot de geboden voorzieningen. In het geval van desktopvirtualisatie (*virtual desktop infrastructure*) maken gebruikers via het netwerk gebruik van een *host computer* op afstand, bijvoorbeeld via een Citrix-client. Vanuit de gebruiker gezien is er geen verschil tussen interactie met haar eigen pc onder haar bureau en een virtuele pc aan de andere kant van de wereld die via een dergelijke client wordt benaderd.

Er wordt in hoge mate gebruik gemaakt van standaardcontracten en standaardvoorzieningen (*resource pooling*) die middels IT-applicaties zijn te bestellen, af te nemen en te configureren. De aanbieder maakt het de gebruiker zo eenvoudig mogelijk om de benodigde middelen, zoals opslagcapaciteit, servercapaciteit en rekenkracht, naar behoefte in en uit te schakelen (*rapid elasticity*). Cloudcontracten kunnen veelal online worden aangegaan door middel van het invullen van online formulieren en betaling door middel van creditkaarten of facturering. Door middel van

[7] Vaak worden online sociale netwerken onder SaaS gerekend, maar eigenlijk is dit een twijfelgeval. We zijn geneigd een concrete verschijningsvorm van een SNS, zoals Facebook, geen SaaS te noemen; een platform waarmee een SNS kan worden gebouwd, zoals het open source-platform Elgg, is wel een SaaS.
[8] http://www-03.ibm.com/press/us/en/pressrelease/20988.wss.
[9] Zie http://AWS.amazon.com/.
[10] Het in december 2010 in opspraak geraakte WikiLeaks draaide bijvoorbeeld op Amazon AWS. Zie bijvoorbeeld http://AWS.amazon.com/message/65348/.
[11] Mell & Grance 2011, p. 2.

configuratieschermen kunnen gebruikers de verschillende eigenschappen van de dienstverlening zelf aanpassen.

De dienstverlening beweegt mee met de behoeften van de gebruiker. Wanneer de gebruiker meer opslagruimte nodig heeft, dan is dit te realiseren zonder dat deze zich zorgen hoeft te maken over de hardware en software die daarvoor nodig is. Wanneer de behoefte aan middelen daalt, kunnen deze eenvoudig worden afgekoppeld. In sommige gevallen gebeurt dit automatisch en past de totale beschikbare capaciteit zich automatisch aan de vraag. Gebruik van cloudvoorzieningen is dus gebaseerd op het gebruik van de voorzieningen en niet zozeer op de kosten van de onderliggende hard- en software (*measured services*). Opslagruimte bij diensten zoals Dropbox wordt bijvoorbeeld aangeboden in standaardgroottes die geen verband houden met de fysieke schijfruimte op harde schijven. Dit is mogelijk doordat de middelen met vele gebruikers worden gedeeld. Dat maakt het tevens mogelijk kleine hoeveelheden schijfruimte (bijv. 5 Gb) gratis aan te bieden aan gebruikers. De kosten hiervan vallen voor de aanbieder weg in het licht van de benodigde overcapaciteit en de betaalde diensten. Omdat het betaalmodel van cloud computing in veel gevallen is gebaseerd op *measured services*, zullen veel cloudaanbieders het gebruik van hun voorzieningen moeten monitoren. Dit is relevant in het licht van opsporing van crimineel gebruik van de cloud.

Het derde onderdeel van de cloud definitie wordt gevormd door de **beheersvormen**. Clouddiensten kunnen worden aangeboden in een publieke, private of hybride omgeving. Bij een private cloud is de infrastructuur uitbesteed aan een derde partij terwijl de infrastructuur alleen beschikbaar is voor de klant. In deze vorm wordt de IT-dienstverlening buiten de deur gezet, maar dit verschilt in de dagelijkse praktijk en wat betreft toegankelijkheid van voorzieningen niet veel van het in eigen beheer hebben van de infrastructuur.

Bij een publieke cloud wordt de infrastructuur gedeeld met anderen. De aanbieder van de publieke cloud bepaalt in wezen wat er wordt aangeboden en tegen welke voorwaarden. De invloed van gebruikers op de voorzieningen is gering en beperkt zich tot datgene wat de aanbieder configureerbaar maakt.

Bij een hybride cloud is sprake van een combinatie van publiek en privaat. In het private deel worden de kritieke applicaties ondergebracht terwijl minder kwetsbare applicaties via de publieke cloud worden betrokken.

Een belangrijk aspect van de beheersvormen is dat clouddiensten een sterk internationaal karakter hebben. Clouddiensten worden voornamelijk aangeboden door (grote) Amerikaanse aanbieders met serverparken op verschillende locaties in de wereld. Om technische en commerciële redenen wordt de dataopslag en rekencapaciteit veelal dynamisch over de verschillende rekencentra verdeeld. Hierdoor worden data vluchtig. Het ene moment bevinden ze zich fysiek op een server in Ierland, het volgende moment op een server in North Carolina. Doordat de opslag tevens vaak redundant plaatsvindt om de gevolgen van calamiteiten te verkleinen, is het waarschijnlijk dat er verschillende kopieën op verschillende locaties bestaan (redundante opslag, replicatie). Ook is het mogelijk dat logische files (bijvoorbeeld een Word-bestand) in stukjes opgeknipt opgeslagen is op verschillende fysieke locaties (gedistribueerde opslag, *sharding*, *partitioning*)[12]. Dit alles maakt dat het lastig kan zijn vast te stellen 'waar' de data zich op een bepaald moment bevinden. Dit heeft consequenties voor bijvoorbeeld jurisdictievraagstukken.

2.2. Aanpalende begrippen

In discussies over cloud computing in relatie tot misdaad en opsporing wordt soms ook verwezen naar fenomenen die raakvlakken hebben met cloud computing en soms, afhankelijk van de invulling die men geeft aan dit begrip, ook onder cloud computing worden geschaard. Deze fenomenen vertonen familiegelijkenissen met cloud computing, zodat het nuttig is voor de inkleuring van dit begrip hier ook enkele familieleden te bespreken.

2.2.1. Deep Web

In de eerste plaats zijn er de begrippen Deep Web (ook bekend als invisible web, Deepnet, Deep Web, Undernet en hidden Web),[13] dark Internet en darknet. Het Deep Web bestaat uit het deel

[12] Walden 2011, p. 3.
[13] Zie bijv. http://en.wikipedia.org/wiki/Deep_web; Bergman 2001.

van het World Wide Web dat niet door zoekmachines wordt geïndexeerd en derhalve alleen toegankelijk is wanneer de gebruiker de URL van de webserver kent. De omvang van het Deep Web wordt honderden malen groter dan het Surface Web geschat:[14] het via zoekmachines vindbare web is zeg maar het topje van de ijsberg. Cloud services die op het normale web worden aangeboden kunnen ook worden aangeboden op het Deep Web, waarmee ze buiten het blikveld van oningewijden kunnen blijven.

2.2.2. Dark Internet en *darknet*

Het *dark Internet* betreft diensten die niet langer toegankelijk zijn. Dit kan het gevolg zijn van overenthousiast filteren van netwerkverkeer door netwerkbeheerders, misconfiguraties in routers, of het feit dat delen van het netwerk niet goed meegroeien met de veranderende Internetarchitectuur; een voorbeeld van dit laatste zijn militaire netwerken die onderdeel uitmaken van 'milnet', een van de oorspronkelijke onderdelen van Arpanet (de stamvader van het Internet).[15]

Darknet heeft betrekking op private gedistribueerde P2P-netwerken (filesharing) die gebruikmaken van de Internet-infrastructuur voor verkeer en verbindingen en die gebruikmaken van niet-standaard-protocollen en -poorten.[16] Ze opereren daarmee los van het gewone Internet en zijn niet bereikbaar voor niet-ingewijden. Het gaat hierbij niet om de alom bekende P2P-netwerken zoals BitTorrent en Kazaa omdat die door iedereen zijn te gebruiken. Skype voldoet aan een deel van de karakteristieken van Darknet, maar is eveneens voor iedereen toegankelijk. Darknets bestaan onder meer in het militaire domein. Mansfield-Devine beschrijft het Amerikaanse militaire Secret Internet Protocol Router Network (SIPRNet) als voorbeeld.[17] Naast de darknet-P2P-netwerken zijn er open P2P-netwerken, zoals BitTorrent en gedistribueerde dataopslagnetwerken zoals Freenet.

2.2.3. Bittorrent

Bittorrent is een peer-to-peer uitwisselingsnetwerk voor bestanden of verzamelingen bestanden op basis van een door Bram Cohen ontwikkeld protocol.[18] Gebruikers in het netwerk stellen bestanden beschikbaar aan anderen in het netwerk om binnen te halen. De beschikbare bestanden worden aangemeld bij een centraal distributiepunt dat *tracker* wordt genoemd. Deze tracker coördineert het verkeer tussen de plaatsers en binnenhalers binnen de groep gebruikers ('swarm' genaamd, oftewel de 'zwerm') die een bepaald bestand delen. De tracker houdt bij welke gebruikers (TCP-aansluitingen) aan het plaatsen en binnenhalen zijn en hoeveel van het doelbestand iedere gebruiker al heeft. Het eigenlijke uitwisselen van de bestanden vindt plaats door stukken van het bestand op te vragen aan de verschillende andere deelnemers in de zwerm. Om een bestand te kunnen binnenhalen moet de gebruiker beschikken over een *torrent metafile* die informatie bevat over onder meer de bestandsnaam, de omvang en het IP-adres van een *tracker*. De deelnemers aan een zwerm zijn te verdelen in degenen die het bestand al in zijn geheel hebben en onderdelen beschikbaar stellen aan eenieder die daar om vraagt (zogeheten *seeders*) en gebruikers die nog aan het binnenhalen zijn (zogeheten *leechers*).

Bittorrent is een efficiënt protocol om (grote) bestanden uit te wisselen wanneer er voldoende 'seeders' zijn ten opzichte van het aantal 'leechers', omdat de uitwisseling van onderdelen van het bestand plaatsvindt tussen de deelnemers aan de zwerm onderling en de werklast van de aanbieders dus sterk verdeeld kan worden. Bittorrent werkt op basis van reciprociteit, maar uiteraard vindt binnen Bittorrent-netwerken ook 'meelifter'-gedrag plaats, gebruikers die binnenhalen zonder zelf iets aan te bieden.[19]

Bittorrent is vanuit gebruikersperspectief te vergelijken met diensten (downloadsites) zoals MegaUpload, RapidFileShare en FilesTube. De gebruiker kan middels Bittorrent beschikking verkrijgen over bestanden die zich elders bevinden. Technisch is er een verschil omdat een binnengehaald bestand bij een downloadsite vanuit één punt komt,[20] terwijl onderdelen van het

[14] He et al. 2007.
[15] http://www.crt.net.au/About/ETopics/Archives/darkint.html.
[16] Mansfield-Devine 2009.
[17] Ibid.
[18] Cohen 2003.
[19] Locher e.a. 2006.
[20] Dat laat onverlet dat het bestand bij de aanbieder van de dienst gedistribueerd kan zijn opgeslagen over meerdere servers op meerdere locaties.

gevraagde bestand bij Bittorrent afkomstig zijn van vele verschillende computers in de zwerm. De computers in een Bittorrent-netwerk zijn doorgaans eigendom van individuen die elk bovendien een relatief beperkt aantal bestanden aanbieden. De beschikbaarheid van de bestanden en van de knooppunten in een Bittorrentzwerm is onberekenbaar, doorgaans ad hoc en sterk dynamisch.

2.2.4. Freenet

Freenet is een gedistribueerd opslagsysteem voor bestanden gebaseerd op het werk van Ian Clarke.[21] De gebruikers van Freenet stellen elk een deel van hun harde schijf, doorgaans enige gigabytes, ter beschikking aan het netwerk ter opslag van versleutelde (delen van) bestanden van andere gebruikers. Bestanden die aan het netwerk beschikbaar worden gesteld (als *upload*) worden in een groot aantal delen gesplitst die vervolgens willekeurig en redundant over een groot aantal punten in het netwerk worden verspreid. Na het aanbieden van een bestand hoeft de aanbieder niet meer beschikbaar te zijn – het bestand bevindt zich dan gedistribueerd in het netwerk. Wanneer de opslagcapaciteit van een knoop vol raakt, wordt informatie die langere tijd niet is opgevraagd gewist om plaats te maken voor nieuwe onderdelen (*cache)*. Het is niet mogelijk om bestanden uit het netwerk te verwijderen, maar door het doorschuifsysteem van de *caches* wordt gedateerde informatie gaandeweg verdrongen door nieuwe informatie.

Het systeem ontbeert iedere vorm van centrale coördinatie. De knopen communiceren alleen met knopen die ze direct kunnen benaderen (conceptueel zijn dit buren). Een bestand binnenhalen uit het netwerk bestaat uit het rondsturen van een verzoek om de op een knoop aanwezige onderdelen van het bestand te verstrekken op basis van een sleutel die elk bestandsonderdeel koppelt aan het geheel. Een knoop zal ofwel de gevraagde onderdelen leveren wanneer het daarover beschikt, dan wel het verzoek doorsturen naar de volgende knopen in het netwerk.

Door de combinatie van encryptie van de gegevens en het doorsturen van verzoeken (*relaying*) biedt Freenet sterke anonimiteit voor zowel de plaatsers als de binnenhalers. De individuele knopen kunnen de informatie die ze *cachen* niet ontsleutelen en weten ook niet van wie of naar wie de data gaat (de knopen weten immers niet van welk eindpunt een verzoek komt). Hierdoor ontstaat een sterke mate van 'plausible deniability' voor de eigenaren van de knopen, dat wil zeggen dat elke knoop aannemelijk kan maken dat het niet weet welke informatie hij in opslag heeft.[22]

Freenet kan zowel in een *darknet*-modus opereren, waarin iedere knoop alleen communiceert met vertrouwde knopen die onderdeel uitmaken van een handmatig aangelegde lijst, als in een *opennet*-modus waarin elke knoop met alle andere Freenetgebruikers kan communiceren. In *darknet*-modus is Freenet erg lastig door buitenstaanders te detecteren.[23]

2.2.5. TOR

The Onion Router (TOR) wordt grotendeels bekostigd door de *Electronic Frontier Foundation* en is met name gericht op het faciliteren van anonimiteit. TOR bestaat uit een netwerk van door vrijwilligers aanboden servers verspreid over de hele wereld waarbinnen communicatie wordt gerouteerd en versleuteld. Gebruikers communiceren met een willekeurige ingang tot het TOR-netwerk. Het verkeer wordt vervolgens willekeurig over verschillende knopen in het netwerk naar een willekeurige uitgang geleid. Hiermee wordt het lastig om de bron en bestemming van verkeer te achterhalen; het systeem biedt daarom een effectieve methoden om verkeersanalyse tegen te gaan.[24] Echter, omdat TOR alleen maar gericht is op het anonimiseren van het *transport* van gegevens, garandeert het nooit absolute anonimiteit. Zo beschermt TOR niet tegen zogeheten *end-to-end timing attacks*, waarbij een persoon registreert welk dataverkeer van en naar je computer gaat en met behulp van statistische analyse kan herleiden binnen welk circuit een computer opereert.[25]

---

[21] Clarke e.a. 2001.
[22] Clarke e.a. (ibid, p. 2) noemen als centrale ontwerpeisen: 'anonymity for both producers and consumers of information, deniability for storers of information, resistance to attempts by third parties to deny access to information, efficient dynamic storage and routing of information, decentralization of all network functions.'
[23] Clarke e.a. 2010.
[24] Voor een gedetailleerde beschrijving van de werking van TOR, zie bijvoorbeeld Goldschlag, Reed & Syverson 1999.
[25] https://www.torproject.org/about/overview.html.en#stayinganonymous (geraadpleegd 3 juli 2012).

TOR is geen p2p-netwerk, en hoewel de organisatie zelfs p2p-verkeer op het TOR-netwerk afraadt omdat dat een te grote belasting voor het netwerk vormt en TOR bovendien geen (extra) privacywaarborgen biedt bij gebruik van bijvoorbeeld BitTorrent,[26] blijkt uit onderzoek dat TOR-verkeer niettemin voor het grootste deel uit p2p-verkeer bestaat (met name BitTorrent), en dat veel van dat verkeer in eerste instantie onzichtbaar is omdat het versleuteld is.[27]

2.3. Perspectieven op de ontwikkeling van cloud computing

Er wordt veel gesproken over cloud computing, en veel bedrijven, overheden en burgers denken na over de vraag of en zo ja hoe zij gebruik moeten maken van clouddiensten. Zoals eerder aangegeven is cloud computing op zichzelf weinig vernieuwend en lijkt het in zekere zin op het teruggrijpen op klassieke client-server-modellen in een nieuw jasje, met als belangrijkste verschil dat de cloud uit verschillende servers met gedistribueerde opslag bestaat. Een interessante vraag voor de onderhavige studie is of cloud computing een hype is die weer over gaat waaien of dat we ons op moeten maken voor radicale en grootschalige veranderingen in de IT-infrastructuur. Om een antwoord op die vraag te krijgen, hebben wij gekeken naar een aantal witboeken en nieuwsberichten over de ontwikkeling en verspreiding van cloud computing.

Aanbieders van clouddiensten houden vaak vlammende betogen over de voordelen van de cloud. Google presenteert zelfs een 100% webstrategie voor *Enterprise IT* waarbij alle IT-processen via het web verlopen.[28] Veelal worden voordelen geschetst langs de lijnen van kostenbesparingen, locatie-onafhankelijkheid, snelheid, betrouwbaarheid, schaalbaarheid en innovatie, die het zowel voor het MKB[29] als voor grote ondernemingen aantrekkelijk maken om gebruik te maken van clouddiensten.

Ook consultancybedrijven produceren rapportages en onderzoeken over de adoptie en toekomst van cloud computing. Daaruit komt geen eenduidig beeld naar voren; op basis van vergelijkbare cijfers komen sommigen zelfs tot tegenstrijdige conclusies. Information Age[30] rapporteert bijvoorbeeld over twee studies uitgevoerd in het najaar van 2011 door respectievelijk het informatiebeveiligingsbedrijf Symantec en KPMG onder honderden organisaties in verschillende geografische regio's en bedrijfstakken. Beide studies rapporteren een adoptiegraad van rond de 20%, terwijl 10-20% van de geraadpleegde bedrijven aangeeft geen interesse in de cloud te hebben. Symantec schrijft op basis van deze gegevens: 'with cloud, there is more talk than action', terwijl KPMG het houdt op 'cloud computing is set to "skyrocket"'. Volgens KPMG heeft 81% van de bedrijven plannen, is aan het experimenteren of is reeds volop in de cloud aan het opereren. 'Cloud adoption is quickly shifting from a competitive advantage to an operational necessity, enabling innovation that can create new business models and will impact the long-term growth opportunities and competitiveness of businesses.'[31]

Forbes voerde in 2010 een studie uit onder 235 IT-topfunctionarissen van bedrijven met een omzet groter dan $500 miljoen. Daaruit komt naar voren dat de ruime meerderheid van de ondervraagden cloudprojecten heeft lopen of overweegt. Slechts 16% van de respondenten is niet van plan private clouddiensten te gaan gebruiken, terwijl 35% aangeeft geen plannen te hebben richting publieke clouddiensten.[32] Veiligheid en verlies aan controle worden gezien als de grootste aandachtspunten bij een overstap naar een publieke cloud. Veiligheid, gebrek aan interne expertise en integratie met bestaande systemen zijn de grote aandachtspunten bij het ontwikkelen van private clouddiensten.

[26] https://blog.torproject.org/blog/bittorrent-over-tor-isnt-good-idea (geraadpleegd 3 juli 2012).
[27] Chaabane, Manils & Kaafar 2010.
[28] Google, *100% Web. Google's vision for the future of enterprise IT*, http://www.idgconnect.com/view_abstract/7137/100-web-google-s-vision-future-enterprise-it.
[29] Zie bijvoorbeeld het rapport van IDG Connect (in samenwerking met Google), *The small business guide to cloud computing*, http://www.idgconnect.com/view_abstract/7136/the-business-guide-cloud-computing.
[30] http://www.information-age.com/channels/the-cloud-and-virtualization/perspectives-and-trends/1659523/symantec-and-kpmg-spin-cloud-stats-in-opposite-directions.thtml Artikel gepubliceerd op 4 oktober 2011 (geraadpleegd 3 juli 2012).
[31] Ibid.
[32] Forbes 2010.

Deloitte meldt in een rapport uit 2009[33] dat SaaS voorbij de hype is en dat zowel PaaS en IaaS de komende jaren aan belang zullen winnen. Ook Gartner en Intel laten zien dat er verschillen zijn in ontwikkeling en adoptie van de verschillende cloudvormen. Hun 'Cloud computing hype cycle' laat zien dat veel vormen in 2011 rond de 'peak of inflated expectations' (op de top van de hype) zaten, terwijl een aantal SaaS-vormen zich inmiddels in de 'slope of enlightenment' bevindt, dat wil zeggen dat de fase waarin de hype en daaropvolgende desillusie voorbij zijn en deze applicaties op weg zijn naar een stevige verankering in de maatschappij.[34]

De Nederlandse overheid heeft begin 2011 een strategie opgesteld voor het gebruik van clouddiensten door de overheid.[35] Het kabinet kiest hierin voor een gesloten cloud (private cloud) waarbij de inzet is om hogere prestaties tegen lagere beheerkosten en een groter gebruikersgemak te realiseren. Het kabinet richt zich in eerste instantie op het Rijk en streeft naar de ontwikkeling van een gesloten Rijkscloud in eigen beheer, in te richten als een voorziening die generieke diensten levert binnen de Rijksdienst. Deze voorziening wordt ingericht binnen een eigen beveiligd netwerk en beheerd door een eigen, rijksbrede organisatie.

2.4. Conclusie

Aan de hand van de vijf kernkarakteristieken van cloud computing (*on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service*) kunnen online diensten worden onderscheiden in clouddiensten en 'gewone' online diensten. Het onderscheid is echter niet in absolute zin te maken en er zijn de nodige randgevallen. Vanuit de doelstelling van dit onderzoek – het in kaart brengen van de gevolgen van cloud computing voor opsporing en vervolging – leggen wij in dit rapport de nadruk op verschijningsvormen die de kern van cloud computing raken, aangezien deze de meest illustratieve waarde hebben om de gevolgen van de opkomst van de cloud in beeld te brengen. Daarmee krijgt de specificiteit van cloud computing ook reliëf ten opzichte van andere ontwikkelingen in ICT en cybercrime, zoals anonieme routering en peer-to-peer-netwerken (Freenet, Bittorrent), die een eigen problematiek met zich brengen en zelfstandig onderzoek behoeven.

Verschijningsvormen die 'typisch' cloud computing zijn, zijn emaildiensten als Gmail en Hotmail, diensten voor opslag of delen van bestanden (zoals DropBox of Box.net, Skydrive, Megaupload), applicatiediensten als Google Docs en ontwikkelplatforms als Amazon AWS. Deze vormen werden vaak genoemd door de geïnterviewde personen bij de vraag wat zij verstonden onder cloud computing. Zij omschrijven cloud computing bijvoorbeeld als 'je data of je processen ergens anders plaatsen (buiten je eigen beheer)' of het 'uitbesteden aan derden van opslag en computationele kracht'.[36] Wat cloud computing daarbij anders maakt dan standaard webgebaseerde diensten of sociale netwerksites als Facebook is dat het gaat om uitbesteden van (bedrijfs)processen[37] met decentrale opslag (niet op één plek maar op veel plaatsen, vaak dubbel en in stukjes verknipt)[38] waarbij je de regie over de locatie uit handen geeft.[39]

Wanneer we deze voorbeelden en elementen samenvatten kunnen we de volgende werkdefinitie geven die we zullen hanteren in dit rapport: cloud computing is het uitbesteden van gegevensbeheer of computerapplicaties aan een dienstverlener, met gedistribueerde opslag en in beginsel zonder regie over de locatie.

Over de mate waarin cloud computing wezenlijke veranderingen aanbrengt in de communicatie- en informatie-infrastructuur, kan verschillend worden gedacht. Enerzijds gaat het om graduele verschillen, waarbij de golfbeweging tussen centralisatie en decentralisatie van computercapaciteit weer wat teruggolft naar centralisatie. Anderzijds gaat het om een nieuw type grootschalige infrastructuur die, vanwege schaal- en andere voordelen, door veel bedrijven zal

[33] https://www.deloitte.com/assets/Dcom-Global/Local%20Assets/Documents/TMT/cloud_-_market_overview_and_perspective.pdf (geraadpleegd 3 juli 2012).
[34] Zie het plaatje van de Gartner Hype Cycle 2010, beschikbaar op http://www.gartner.com/it/page.jsp?id=1447613 (geraadpleegd 3 juli 2012).
[35] *Kamerstukken II* 2010/11, 26 643, nr. 179, Brief van de Minister van Binnenlandse Zaken en Koninkrijksrelaties, 20 april 2011.
[36] Interviews Fox-IT en KLPD.
[37] Interview Fox-IT.
[38] Interview Openbaar Ministerie.
[39] Interviews KLPD en politie Oost-Nederland.

worden omarmd waarbij gegevensverwerking op grote schaal buiten het bedrijf zal plaatsvinden. Ook op de consumentenmarkt betekent de adoptie van SaaS-applicaties een belangrijke verschuiving van gegevensverwerking. Deze verschuivingen in patronen van gegevensverwerking en gegevensopslag kunnen, of ze nu radicaal of gradueel zijn, belangrijke gevolgen hebben voor opsporing en vervolging van misdrijven waarin digitaal onderzoek een rol speelt.

3. Ervaringen van opsporingsinstanties met de cloud

In dit hoofdstuk schetsen we op basis van de interviews en vragenlijst onder buitenlandse deskundigen welke ervaringen er tot nu toe bestaan met misdaad en opsporing in de cloud. Aangezien de ervaringen vooralsnog relatief beperkt blijken te zijn, vullen we deze schets aan met een uitvoeriger weergave van twee zaken uit het buitenland die een goede illustratie bieden van de cloudproblematiek.

3.1. Nederland

De ervaringen in Nederland met cloud computing in opsporing en vervolging lijken tot nu toe gering. Cloud computing bevindt zich nog in een relatief vroeg stadium van ontwikkeling en gebruik; de sleutelpersonen die wij spraken bij politie en Openbaar Ministerie reageren aarzelend op de vraag welke ervaringen zij tot nu toe hebben met cloud computing en weten weinig concrete voorbeelden te geven. De kans bestaat natuurlijk dat er wel ervaringen zijn bij andere onderdelen van de opsporing en justitie, maar het lijkt onwaarschijnlijk dat er substantiële zaken zijn waarbij de cloud een significante rol heeft gespeeld, die niet ook bekend zouden zijn bij de specialisten in cybercrime bij het Landelijk Parket of het KLPD.

Er bestaat één duidelijke uitzondering op de weinige praktijkervaring met cloud computing. Webmaildiensten als Gmail en Hotmail komen wel veelvuldig voor in opsporingsonderzoeken.[40] In de jurisprudentie komt dat niet prominent naar voren, vermoedelijk omdat de inhoud veelal als sturingsinformatie en niet als bewijs wordt gebruikt. Voor zover er in uitspraken verwezen wordt naar webmaildiensten, gaat het veelal om emailadressen die door slachtoffers zijn gebruikt[41] of hotmail-accounts die bij afgetapte chatsessies zijn gebruikt.[42] Wij hebben één geval aangetroffen waarin het gebruik van email uit een Hotmailaccount als bewijsmateriaal werd bestreden. In deze zaak had de officier van justitie via een informant een hotmailadres en wachtwoord gekregen met een tip dat in de postbus informatie zou staan over een boottransport met cocaïnelevering. De officier had een machtiging gevraagd van de rechter-commissaris ex art. 126ng Sv om de inhoud van email op te vragen bij Microsoft in Redmond, VS, maar de dag na het verkrijgen van de machtiging gaf hij opdracht aan een opsporingsambtenaar om zelf in te loggen op het hotmailaccount, vanwege het spoedeisend belang om het transport te onderscheppen. De rechtbank oordeelde dit in strijd met de wet, maar liet het gebruik voor bewijs in stand op basis van de Schutznorm-leer (bewijsuitsluiting is alleen aangewezen als de verdachte in de door de norm beschermde belangen is geschaad[43]). Het hotmailaccount behoorde immers toe aan een medeverdachte, zodat de verdachte zelf niet in zijn privacybelang was geschaad.[44]

Webmaildiensten worden niet alleen gebruikt om berichten te versturen naar andere emailadressen, maar ook voor interne communicatie binnen misdadigergroepen, waarbij iemand een bericht in de map ‘concepten’ plaatst dat de beoogde ontvanger vervolgens via hetzelfde account leest, waarna het bericht kan worden verwijderd zonder dat het verstuurd is.[45] Ook diensten om bestanden op te slaan en te delen als Google Docs, Skydrive en Box.net komen voor in opsporingsonderzoeken.[46] Het verkrijgen van materiaal uit de cloud, in het bijzonder de inhoud van Gmail en Hotmail, levert meestal geen problemen op (als tenminste bekend is welke diensten een verdachte gebruikt). De grote aanbieders van dergelijke diensten werken mee aan vorderingen tot uitlevering van gegevens die via een rechtshulpverzoek aan de VS worden

[40] Interviews Openbaar Ministerie, KLPD en politie Oost-Nederland.
[41] Zie bijvoorbeeld Rb. Roermond 8 april 2009, LJN BI2037.
[42] Zie bijvoorbeeld HR 20 februari 2007, LJN AZ0213.
[43] Zie nader noot 215 en bijbehorende tekst.
[44] Rb. Rotterdam 26 april 2010, LJN BM2518. In hoger beroep accepteerde het Hof de email eveneens als bewijs vanwege de Schutznorm, waarbij in het midden gelaten werd of de handelwijze van de officier op zich onrechtmatig was geweest (“Indien en voor zover er in vorenstaand verband derhalve al sprake zou zijn geweest van enig vormverzuim (…)”); zie Hof ’s-Gravenhage 27 april 2011, LJN BR6836.
[45] Van der Hulst & Neve 2008, p. 46.
[46] Interviews Openbaar Ministerie en politie Oost-Nederland. Zie bijvoorbeeld Rb. Roermond 22 april 2011, LJN BQ3544 (gebruik Dropbox tussen twee verdachten).

uitgevaardigd, en de gegevens worden meestal binnen redelijke termijn geleverd.[47] Bestanden uit dataopslagdiensten zijn echter minder goed te verkrijgen, omdat die gedistribueerd zijn opgeslagen en – zo beweren sommige aanbieders – de aanbieder zelf niet altijd goed bij de data kan.[48] Sporadisch komt een rechtshulpverzoek binnen uit een ander land om materiaal opgeslagen in Nederland veilig te stellen; in het geval van een 'mini-cloud' in Nederland zijn bijvoorbeeld diverse servers in beslag genomen ten behoeve van een Amerikaans verzoek.[49]

Wat betreft criminaliteit in of via de cloud gepleegd zijn er geen concrete voorbeelden bekend van zaken die in Nederland tot vervolging hebben geleid. Het is wel bekend dat criminaliteit via de cloud wordt gepleegd of gefaciliteerd, zoals grootschalige auteursrechtschendingen via Megaupload of de verspreiding van kinderporno via documentdeeldiensten als Gigatribe.[50]

3.2. Buitenland

Het beeld dat op basis van onze enquête onder buitenlandse deskundigen ontstaat van ervaringen in het buitenland, wijkt niet af van dat van Nederland. Hierbij moeten we wel een grotere slag om de arm houden, aangezien we slechts uit een beperkt aantal landen reacties hebben en onze respondenten uit het wetenschappelijke netwerk ook niet altijd dicht op de praktijk in hun land zitten. Echter, ook de meest ervaren internationale deskundigen op het gebied van cybercriminaliteit, zoals Susan Brenner in de Verenigde Staten en Ian Walden in het Verenigd Koninkrijk, rapporteren dat zij weinig tot geen concrete gevallen kennen van criminaliteit gepleegd in of via de cloud of van concrete ervaringen met opsporing in de cloud (behoudens webmaildiensten). Dit suggereert dat het aannemelijk is dat de cloud tot nu toe geen bijzonder prominente plaats inneemt in de praktijk van cyberopsporing. Illustratief is het volgende citaat:

> experts and reports concerning the cloud computing/crime nexus have yet to report any real substantive case studies to focus on and instead focus on the obvious potential that exists with cloud computing for use in criminal activities.[51]

Wat criminaliteit betreft vermelden onze respondenten dat botnetaanvallen zijn gepleegd met gebruikmaking van cloudgebaseerde applicaties vanuit Amazon EC2.[52] Daarnaast wordt wanwaar (kwaadaardige programmatuur) gemaakt met gebruikmaking van Google Apps. Het gebruik van Amazon-clouddiensten voor uitwisseling van hulpmiddelen voor cybercriminaliteit is ook bekend in de Verenigde Staten. Ook wordt kinderporno opgeslagen in de cloud. Verder wordt nog gemeld dat cloudapplicaties zijn gebruikt om illegale boekhoudingen bij te houden.

Bij de opsporing komt het volgens diverse respondenten regelmatig voor dat webmail wordt opgevraagd bij cloudaanbieders. Dit is ook gebruikt als bewijs in strafzaken. Daarnaast worden ook bijvoorbeeld IP-adressen en logbestanden gevorderd bij cloudaanbieders. Over het vorderen van bestanden die in de cloud worden opgeslagen via diensten als Google Docs of Skydrive melden onze respondenten niets.

Google biedt sinds 2010 een overzicht van verzoeken of vorderingen die zij krijgt van overheden om in het kader van strafzaken inhoud van het web te verwijderen (bijvoorbeeld YouTube-filmpjes) of gegevens van of over gebruikers te overhandigen.[53] In de eerste helft van 2011 kreeg Google bijvoorbeeld 15.744 verzoeken, die in totaal ruim 25.000 gebruikers/accounts betroffen.[54] Daarvan kwamen er bijvoorbeeld 64 uit Nederland (waarvan 48% werd gehonoreerd),

[47] Interviews KLPD, Openbaar Ministerie en Fox-IT.
[48] Interview Openbaar Ministerie. Het valt moeilijk te achterhalen of dit daadwerkelijk zo is. Vgl. het voorbeeld dat Walden 2011, p. 9 geeft: 'In April 2011, for example, Dropbox was forced to change the wording used in a 'help' article to reflect an amendment made to its terms of service. It had stated that "Dropbox employees aren't able to access user files"; part of the security assurances made to its customers relating to its use of encryption. However, its terms incorporate a provision enabling it to hand over user data in compliance with a valid court order, which required it to clarify that its employees are 'prohibited' from accessing user files, rather than being unable to access them.'
[49] Interview KLPD.
[50] Interview Openbaar Ministerie.
[51] Ian Walden, reactie op enquête.
[52] Zie ook CNET News, 'Amazon EC2 cloud service hit by botnet, outage', 11 december 2009, http://news.cnet.com/8301-1009_3-10413951-83.html.
[53] Google Transparency Report, http://www.google.com/transparencyreport/.
[54] Het totaal ligt hoger, aangezien Google niet alles kan of mag vermelden en landen met minder dan 30 verzoeken weglaat; zie http://www.google.com/transparencyreport/faq/.

90 uit België (67% gehonoreerd), 1065 uit Duitsland (66% gehonoreerd), 1279 uit het VK (63% gehonoreerd), 5950 uit de VS (93% gehonoreerd), 1739 uit India (70% gehonoreerd) en 42 uit Rusland (0% gehonoreerd). Onduidelijk is echter hoeveel hiervan clouddiensten van Google als Gmail, Google Docs of Google Apps betreft; het kan ook gaan om gebruikers die materiaal via Google-diensten aan het publiek aanbieden, zoals YouTube-filmpjes.[55]

België kent een interessant alternatief voor het opvragen van gegevens bij aanbieders, dat in de praktijk wordt gebruikt: de politie kan zelfstandig gegevens verzamelen uit de cloud vanaf een Belgische computer (art. 88ter Belgisch Wetboek van Strafvordering).[56] In de meeste landen is een dergelijke grensoverschrijdende netwerkzoeking niet toegestaan (zie nader par. 5.1.1 over deze problematiek).

3.3. Casus 1: de Yahoo!-zaak

Op 29 november 2007 verzocht de procureur des Konings in België, vergelijkbaar met de officier van justitie in Nederland, Yahoo! Inc., een vennootschap naar Amerikaans recht (hierna: Yahoo!), om gegevens mee te delen over de houders van bepaalde e-mailaccounts. Deze gerechtelijke vordering gebeurde via e-mailadressen en websites, of zogenaamde “webloketten”, die Yahoo! op Belgisch grondgebied ter beschikking stelt om misbruiken, veiligheidsproblemen en/of inbreuken te melden.[57]

Op 10 december 2007 antwoordde Yahoo! Customer Care per e-mail dat een dergelijk verzoek schriftelijk diende te worden gericht aan Yahoo! Custodian of Records gevestigd in Sunnyvale in de VS. Op 29 februari 2008 verzond de procureur zijn origineel verzoek per gewone post en per fax naar dit adres.

Op 10 maart 2008 antwoordde Yahoo! niet in te willen gaan op de vordering omdat alle gevraagde informatie binnen de VS geregistreerde e-mailaccounts betrof en daarom op grond van de Amerikaanse Electronic Communications Privacy Act (ECPA) diende te worden gevorderd. Dit vereist ofwel een vordering van een VS-autoriteit, zodat de vraag van de Belgische procureur des Konings diende te worden gericht aan het Amerikaanse Ministerie van Justitie, ofwel het ondernemen van een civiel proces tegen onbekenden (een John Doe-zaak). Yahoo! wees ook op de mogelijkheid de daders bij Internet-toegangsaanbieders te identificeren op basis van IP-adressen in de mailheaders. Yahoo! argumenteerde met andere woorden dat artikel 46bis van het Belgisch Wetboek van Strafvordering (BSv) niet de rechtsgrond was waarop de procureur des Konings onderzoeksdaden kon vorderen. Na op 7 juli 2008 Yahoo! een laatste maal tevergeefs te hebben aangeschreven met hetzelfde verzoek, dagvaardde de procureur des Konings Yahoo! met succes voor de rechtbank van eerste aanleg te Dendermonde wegens weigering gegevens mee te delen op grond van artikel 46bis BSv, waarop volgens dit artikel bestraffing met geldboete van zesentwintig tot tienduizend euro staat. Naderhand volgden talrijke zaken in beroep en cassatie met terugverwijzing, waarop het openbaar ministerie wederom in cassatie is gegaan.[58]

Het geschil is nog steeds niet beslecht – het ligt momenteel weer bij het Hof van Cassatie (de hoogste rechter) – zodat er nog geen definitieve antwoorden zijn op de voorliggende rechtsvragen. Deze vragen betreffen zowel de definitie van een elektronische communicatiedienst als rechtsmacht (extraterritoriale procedurele jurisdictie) op grond waarvan de procureur des Konings het Wetboek van Strafvordering en meer bepaald artikel 46bis BSv mag toepassen om e-mailgebruikersgegevens te vragen aan een bedrijf zoals Yahoo!.

---

[55] Het betreft ‘any users or accounts used to store or provide information on our services’, aldus http://www.google.com/transparencyreport/faq/#datarequestsfaq.

[56] Philippe van Linthout, reactie op enquête.

[57] Zie http://help.yahoo.com/l/us/yahoo/privacy/general.html en http://help.yahoo.com/l/us/yahoo/abuse/abuse.html (geraadpleegd 3 juli 2012).

[58] Zie Rechtbank van eerste aanleg (Corr.) te Dendermonde 2 maart 2009, http://jure.juridat.just.fgov.be/view_decision?justel=N-20090302-14&idxc_id=235056&lang=nl, *T.Strafr.* 2009 (2), p. 116-124; Hof van beroep te Gent 30 juni 2010, http://jure.juridat.just.fgov.be/view_decision?justel=N-20100630-1&idxc_id=242315&lang=nl; *Computerrecht* 2010 (6), p. 351; *T.Strafr.* 2011 (2), p.132-136, m.nt. P.van Linthout; Hof van Cassatie (Cass.) 18 januari 2011, A.R. nr. P.10.1347.N, http://jure.juridat.just.fgov.be/view_decision?justel=N-20110118-1&idxc_id=249937&lang=nl; *T.Strafr.* 2011, afl. 2, 120-122, m.nt. P. van Linthout; Hof van beroep te Brussel 12 oktober 2011, *Computer Law & Security Review* 2012, p. 237-238.

In België regelt BSv de opsporingsbevoegdheden in een strafrechtelijk onderzoek. Artikel 46bis BSv bevat de wettelijke regeling ter identificatie van abonnees en gewoonlijke gebruikers van elektronische communicatiediensten en -middelen en het opvragen van gegevens met betrekking tot elektronische communicatiediensten. Zowel het hof van beroep te Brussel als het Hof van Cassatie lijken extraterritoriale procedurele jurisdictie te gronden op de definitie van elektronische communicatiedienst.

Het Hof van beroep te Gent sloot Yahoo! uit van het toepassingsgebeid van de Wet van 13 juni 2005 betreffende de elektronische communicatie, omdat het webmailsysteem van Yahoo!

> in essentie een software- of netwerkapplicatie is die toelaat om a.h.v. een Yahoo!-e-mailadres elektronische berichten te versturen en te ontvangen van op eender welke locatie m.b.v. (…) het globale (wereldwijde) netwerk, uitgebouwd en beheerd door – van Yahoo te onderscheiden – operatoren van netwerken en verstrekkers van elektronische communicatiediensten.[59]

Daarbij aansluitend beschouwde het hof van beroep te Gent een louter virtuele link met België niet voldoende om extraterritoriale procedurele jurisdictie vast te stellen; een zogenaamde technisch-virtuele link zou wel voldoende zijn, dat wil zeggen een fysieke doorgave van gegevens hetzij als een operator van een elektronisch communicatienetwerk dan wel als verstrekker van elektronische communicatiedienst, maar dat was hier niet het geval. Daarom is volgens het hof van beroep te Gent artikel 46bis BSv niet van toepassing op Yahoo!.

De Procureur-Generaal te Gent tekende beroep aan tegen dit arrest bij het Hof van Cassatie, vergelijkbaar met de Hoge Raad in Nederland. In tegenstelling tot het Hof van beroep gaf het Hof van Cassatie een bijzonder ruimere interpretatie aan het begrip elektronische communicatiedienst in artikel 46bis BSv, zodat een softwareapplicatie zoals Yahoo! onder dit begrip valt.[60] Meer bepaald kan volgens het Hof van Cassatie de 'persoon die een dienst aanbiedt die erin bestaat zijn klanten toe te laten via een elektronisch netwerk informatie te verkrijgen of te ontvangen of te verspreiden', ook een verstrekker van een elektronische communicatiedienst zijn.[61] De ruimere interpretatie van het begrip elektronische communicatiedienst door Cassatie zou het daarom mogelijk maken om extraterritoriale procedurele jurisdictie vast te stellen, nu Yahoo! wel onder de reikwijdte van art. 46bis BSv valt. Het Hof van Cassatie vernietigde bijgevolg het arrest van het hof van beroep te Gent en verwees de zaak naar het hof van beroep te Brussel.

Het Hof van beroep te Brussel[62] knipt vervolgens echter de band tussen extraterritoriale procedurele jurisdictie en de door Cassatie gegeven definitie van elektronische communicatiedienst door. Het Hof stelt dat het 'enkel gegeven dat het technisch mogelijk is, onder meer ook voor de procureur des Konings, om [Yahoo!] vanop Belgisch grondgebied te bereiken bij wege van elektronische of andere communicatiemiddelen' niet volstaat om binnen Belgisch grondgebied aan Yahoo! gegevens te vorderen in de zin van artikel 46bis BSv.

Het wordt zo duidelijk dat het hof van beroep te Brussel de interpretatie van elektronische communicatiedienst door het Hof van Cassatie niet aanvaardt om extraterritoriale procedurele jurisdictie op te gronden. Het is daarbij niet duidelijk of het Hof van beroep te Brussel de eerdere interpretatie van elektronische communicatiedienst door het Hof van beroep te Gent aanvaardt, omdat het Brusselse Hof van beroep geen enkele indicatie geeft over wanneer extraterritoriale procedurele jurisdictie wél mogelijk is. De volgende vraag zou dan zijn of het Hof van beroep te Brussel de link tussen de interpretatie van elektronische communicatiedienst door Het hof van beroep te Gent en jurisdictie aanvaardt. Mogelijk komen deze vragen aan de orde wanneer het Hof van Cassatie zich opnieuw uitspreekt over deze zaak.

[59] Hof van berroep te Gent 30 juni 2010, §15, 19 en 23.
[60] Cass. 18 januari 2011, A.R. nr. P.10.1347.N.
[61] Cass. 18 januari 2011, A.R. nr. P.10.1347.N, §6.
[62] Hof van berroep te Brussel 12 oktober 2011.

3.4. Casus 2: de Rackspace/Indymedia-zaak

Rackspace is een Amerikaanse aanbieder van cloudinfrastructuur (IaaS) met vestigingen in Groot-Brittannië. Een van de klanten van Rackspace is Indymedia, ofwel Independent Media Center, dat een online *open publishing* platform aanbiedt voor politiek nieuws waar iedereen nieuwsberichten (anoniem) kan publiceren. Op 7 oktober 2004 stond Rackspace een tweetal in Groot-Brittannië gebaseerde servers – genaamd de 'Ahimsa'-servers – die gebruikt werden door Indymedia, af aan de Amerikaanse FBI. Als gevolg daarvan waren meer dan twintig Indymedia-websites wereldwijd onbereikbaar; ook diverse andere webpagina's en organisaties werden hierdoor geraakt.[63]

De inbeslagneming werd uitgevoerd door de Amerikaanse overheid in opdracht van de Italiaanse overheid.[64] Italië had de Amerikaanse regering verzocht om, in het kader van strafrechtelijk onderzoek van een reeks aanvallen die uitgevoerd waren door een aantal pro-anarchistische / anti-Europa-groeperingenn op Romano Prodi, de Italiaanse voorzitter van de Europese Commissie op dat moment. De groeperingen werden onder meer beschuldigd van poging tot moord.[65] Volgens de Italiaanse autoriteiten hadden de verdachten een brief waarin zij hun verantwoordelijkheid opeisten op een webpagina van Indymedia geplaatst. Door middel van de inbeslagneming wilde de Italiaanse regering achterhalen welke persoon de brief had geplaatst op het Indymedia nieuws-platform.

De wettelijke grond voor het Italiaanse verzoek aan de Verenigde Staten was een rechtshulpverdrag (*Mutual Legal Assistance Treaty*, MLAT), meer in het bijzonder het Verdrag tussen de Verenigde Staten van Amerika en de Italiaanse Republiek betreffende de wederzijdse rechtshulp in strafzaken (1982).[66] Dit rechtshulpverdrag vereist in artikel 13 de 'verplichte productie van documenten en artikelen in dezelfde mate als vereist zou zijn voor criminele acties in de aangezochte staat'. Na het Italiaanse verzoek verkreeg de FBI een gerechtelijk bevel van het *United States District Court for the Western District* van Texas. Het gerechtelijk bevel was gericht aan Rackspace Managed Hosting in de Verenigde Staten en beval dat Rackspace VS voor de assistant-Procureur van Verenigde Staten van het westelijke district van Texas zou verschijnen, om logbestanden met betrekking tot het plaatsen en updaten van de websites die overeenkomen met bepaalde URL's in een bepaalde periode.

Wat interessant is aan deze zaak is dat de Britse regering niet betrokken was bij de inbeslagname van de server die plaatsvond in Londen.[67] Het is onduidelijk aan wie Rackspace feitelijk de hardware heeft overhandigd (de FBI en/of een overheidsfunctionaris van Groot-Brittannië, of anderszins) en op welke juridische grond het Amerikaanse gerechtelijk bevel is uitgevoerd in Groot-Brittannië . Hoewel er een MLAT tussen Groot-Brittannië en de Verenigde Staten bestaat[68] dat zou kunnen hebben gediend als juridische grondslag voor de inbeslagname, is de kans groter dat het Amerikaanse Rackspace haar Britse dochteronderneming heeft geïnstrueerd om samen te werken met de Amerikaanse regering om aansprakelijkheid in de VS te vermijden.[69] Aldus laat de Indymedia-zaak zien dat, in feite, de locatie van clouddata niet

[63] https://www.eff.org/cases/indymedia-server-takedown , onder "Indymedia".
[64] https://www.eff.org/cases/indymedia-server-takedown en http://indymedia.org/en/2004/10/112047.shtml. In de media werd beweerd dat er eveneens een verzoek aan de VS was gedaan tot Indymediagegevens vanuit de Zwitserse overheid. Dit blijkt echter niet uit de officiële Amerikaanse overheidsdocumenten die gerelateerd zijn aan de Ahimsa inbeslagname, die naar voren zijn gekomen naar aanleiding van een gerechtelijk verzoek tot openbaarmaking door de *Electronic Frontier Foundation*.
[65] https://www.eff.org/files/filenode/Indymedia/01.pdf, p. 6-11.
[66] Treaty between the United States of America and the Italian Republic on Mutual Assistance in Criminal Matters. Zie https://www.eff.org/files/filenode/Indymedia/01.pdf (geraadpleegd 3 juli 2012).
[67] Home Office Minister Caroline Flint reageerde in een officiele respons op de vraag of Groot-Brittannië betrokken was bij de Ahimsa inbeslagname als volgt: "*I can confirm that no UK law enforcement agencies were involved in the matter referred ...*" [Ik kan bevestigen dat geen Britse overeidsfunctionarissen betrokken waren bij deze zaak]. Zie https://www.eff.org/cases/indymedia-server-takedown (geraadpleegd 3 juli 2012), en Mueller, M.L. (2010) Networks and States: The Global Politics of Internet Governance. Massachusetts, The MIT Press, p. 19, noot 8.
[68] Verdrag tussen de regering van de Verenigde Staten van Amerika en de regering van het Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland betreffende de wederzijdse rechtshulp in strafzaken [Treaty between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Mutual Legal Assistance in Criminal Matters] (in werking getreden in 1996).
[69] In de Amerikaanse dagvaarding werd expliciet aangegeven dat, ingeval van niet-naleving door Rackspace, Rackspace VS zou worden "geacht schuldig te zijn aan minachting en onderworpen zou zijn aan rechtelijke

relevant is bij het bepalen welke wetgeving van toepassing is op die data. MLAT's vereisen van de lidstaten dat de strafprocesrechtelijke wetten van het verzoekende land (bijvoorbeeld Italië) hetzelfde effect hebben in het andere land (het verzochte land, bijvoorbeeld de VS), als waren deze wetten uitgevoerd in het verzoekende land. En, zoals de Indymedia-zaak illustreert, kunnen wetten, ook zonder een MLAT als juridische grond, extraterritoriale effecten hebben wanneer een bedrijf gevestigd is in een land en dochterondernemingen heeft in een ander land.

Opmerkelijk is dat de inbeslagname van de servers in Groot-Brittannië niet is gecontroleerd op geldigheid met het recht van Groot-Brittannië, zoals privacy- en gegevensbeschermingsrecht,[70], ondanks het feit dat veel mensen van over de hele wereld werden getroffen door de inbeslagname (de Amerikaanse dagvaarding vereiste de afgifte van vele gedetailleerde persoonlijke informatie van alle gebruikers of abonnees van Indymedia websites[71]).

Wat ook opvalt is dat, hoewel de Italiaanse regering verzocht om logbestanden, Rackspace volledige kopieën van Indymedia-servers heeft overhandigd, omdat het naar verluidt niet te voldoen was aan het gerechtelijk bevel binnen het opgelegde tijdsbestek.[72] Daarmee heeft Rackspace duidelijk meer informatie weggegeven dan geëist werd in de dagvaarding, hetgeen problematisch is omdat het kan leiden tot de onrechtmatig verkregen bewijs.[73] Een interessante vraag die rijst is of in dit geval de technologie, dat wil zeggen de (technische) organisatie van de clouddienst, de reden was waarom Rackspace niet in staat was de specifieke logbestanden te verstrekken binnen de gestelde periode.

3.5. Conclusie

De ervaringen met cloud computing in opsporing en vervolging lijken tot nu toe gering, zowel in Nederland als in het buitenland, met uitzondering van de al lang bestaande webmaildiensten.

Wat criminaliteit betreft is bekend dat cloudopslagdiensten worden gebruikt voor opslag en ook uitwisseling van kinderporno, auteursrechtelijk beschermd materiaal en hulpmiddelen voor cybercriminaliteit. Hierin verschilt de cloud niet direct van andere Internetgebaseerde diensten, die eveneens op grote schaal voor deze misdaadvormen worden gebruikt. Het plegen van botnetaanvallen of het ontwikkelen van wanwaar vanuit de cloud, waar diverse gevallen van gerapporteerd zijn, is evenmin erg specifiek voor de cloud. Er zijn geen gevallen bekend van vervolgingen van misdaad waarbij de cloud een substantiële rol heeft gespeeld.

Wat opsporing betreft komt het veel voor dat webmail bij cloudaanbieders als Google en Microsoft wordt gevorderd via een rechtshulpverzoek. Dergelijke grote aanbieders, die uit de hele wereld duizenden verzoeken per jaar krijgen, werken over het algemeen goed mee met vorderingen. In het buitenland is opgevraagde webmail ook als bewijs in de rechtszaal gebruikt; in Nederland zijn ons geen concrete voorbeelden bekend van bewijsvoering op basis van cloudmateriaal. Het vorderen van bestanden die via de cloud worden opgeslagen en gedeeld, die de politie ook tegenkomt in opsporingsonderzoeken, is mogelijk problematischer dan webmail vanwege de gedistribueerde opslag.

De twee zaken die we uitvoeriger ter illustratie hebben beschreven, tonen duidelijk aan dat de cloud noodzaakt tot internationale samenwerking en opsporing. In beide gevallen wordt materiaal gevorderd of in beslag genomen dat ligt opgeslagen in een ander land, waarbij men worstelt met de klassieke rechtshulpkaders. Mag een land rechtstreeks een beroep doen op een buitenlandse cloudaanbieder? Is het acceptabel dat een Amerikaanse cloudaanbieder (op vordering van de eigen overheid, die dat doet op basis van een Italiaans rechtshulpverzoek) servers uit de lucht haalt die in het Verenigd Koninkrijk staan? In de Rackspace-zaak kwam daar de problematiek bij van gedistribueerde opslag, waardoor het voor de aanbieder naar eigen zeggen niet mogelijk was om binnen de aangeven periode de gevorderde gegevens te achterhalen, zodat het paardenmiddel van hele servers in beslag nemen werd ingezet. In de Belgische zaak blijkt dat clouddiensten tot discussie leiden over de reikwijdte van het begrip communicatieaanbieder, zodat onduidelijk is welk juridisch regime van toepassing is.

---

sancties" ["deemed guilty of contempt and liable to penalties under the law"], zie https://www.eff.org/files/filenode/Indymedia/commissioners_subpoena.pdf (geraadpleegd 3 juli 2012).

[70] Vgl. Walden 2011, p. 12.

[71] https://www.eff.org/files/filenode/Indymedia/commissioners_subpoena.pdf.

[72] https://www.eff.org/cases/indymedia-server-takedown, onder "Questions Remaining from the Unsealed Documents"; zie ook Walden 2011, p. 11.

[73] Walden 2011, p. 12.

Dergelijke problemen komen in rechtszaken nog niet veel voor, maar worden wel in de literatuur en door onze respondenten gesignaleerd als belangrijke knelpunten bij opsporing in de cloud. In de volgende hoofdstukken gaan we dieper in op de uitdagingen die de cloud op conceptueel niveau biedt, eerst met betrekking tot criminaliteit (hfd. 4) en vervolgens met betrekking tot opsporing (hfd. 5) en vervolging (hfd. 6).

4. Misdaad in de cloud: materieel strafrecht

4.1. Inleiding

Een belangrijk deel van het criminele gebruik van de cloud is vergelijkbaar met reeds bekende Internetgerelateerde delicten. In dit hoofdstuk belichten we potentiële dadergroepen en specifieke manieren waarop de cloud kan worden misbruikt door misdadigers. Verder gaan we in op jurisdictie en de vraag of er lacunes in het materiële strafrecht bestaan of kunnen ontstaan als gevolg van cloudspecifieke delicten.

4.2. Dadergroepen

In een literatuuronderzoek naar 'High-tech crime, soorten criminaliteit en hun daders' uit 2008 wordt geconcludeerd dat er veel lacunes zijn in de kennis over daders van cybercriminaliteit,[74] waartoe ook criminaliteit in de cloud kan worden gerekend. Ten aanzien van hackers noemt het WODC-rapport op basis van de literatuur drie, mogelijk deels overlappende, dadertypen:[75]

- de jeugdige crimineel;
- de ideologische hacker;
- de financieel gemotiveerde hacker.

Hacken blijkt uit sommige onderzoeken vooral een aangelegenheid waarmee mannen tussen de 12 en 28 zich bezighouden. Er wordt dan ook wel gesproken over een vorm van jeugdcriminaliteit die vatbaar is voor dezelfde criminologische analyses als andere vormen van delinquentie onder jongeren. Uit het Hacker's Profiling Project blijkt volgens Van der Hulst en Neve dat hackers als intelligente mensen met een expliciete behoefte aan kennis, persoonlijke uitdaging en macht en een sterk gevoel voor burgervrijheid naar voren komen.

Uit de voor het onderhavige onderzoek gehouden interviews zien we de drie typen dadergroepen terug. Naast de jeugdige crimineel, waarvan de recent aangehouden 17-jarige 'KPN-hacker' een sprekend voorbeeld is,[76] wordt gesproken over programmeurs die onderzoeksmatig geïnteresseerd zijn in beveiligingslekken, die niet zozeer vanuit criminele intenties strafbare handelingen in de cloud verrichten, maar die eerder probeeraanvallen uitvoeren. Ze testen de grenzen van beveiligingen en zijn zelf vaak verrast over hun resultaten en de matige staat van de beveiliging van de systemen waar ze binnen weten te dringen. Vaak gaat het hier om zogenoemde ethische hackers of *white hat hackers*, dat wil zeggen ideologisch gemotiveerde hackers die beveiligingslekken blootleggen om het publiek en eigenaren van systemen meer bewust te maken van beveiligingsrisico's, en daarmee aan te sturen op verbetering van de beveiliging. Dergelijke hackers maken soms deel uit van gemeenschappen waarin ervaringen worden uitgewisseld en overwinningen worden gemeld. Binnen deze gemeenschap bestaan allerlei motivaties, niet alleen beveiligingsmissionarisme maar ook de kick en uitdaging om beveiligingspuzzels op te lossen en de technische vaardigheden te etaleren. Dit past bij de observatie dat hacken voor sommige jongeren een nieuwe vorm van entertainment is: 'een sociale activiteit waarbij digitale technologie het spelelement vormt.'[77]

Aan de andere kant staan de crimineel gedreven hackers. Zij worden ook wel *black hat hackers* genoemd. Hieronder bevinden zich ook de serieuze criminelen. Er is bij de geraadpleegde experts de nodige ervaring met georganiseerde criminelen uit Rusland en de Oekraïne.[78] Een voorbeeld van een netwerk met Russische wortels is het Russian Business

[74] Van der Hulst en Neve 2008.
[75] Ibid, p. 106.
[76] Deze jongen is via verschillende beveiligingslekken uiteindelijk bij honderden servers van KPN. Er bleek weinig kennis benodigd om de beveiligingen te doorbreken en de ouders van de jongen wisten van niets. Zie hierover http://www.nu.nl/internet/2773417/17-jarige-bekent-hacken-kpn.html, http://www.nu.nl/internet/2801094/kpn-hacker-komt-vrije-voeten.html (geraadpleegd 3 juli 2012).
[77] Van der Hulst en Neve 2008, p. 106.
[78] Zie bijvoorbeeld de aanhouding van drie hackers in Rusland en de Oekraïne die een virusaanval hebben uitgevoerd op klanten van ABN AMRO in 2008, http://www.om.nl/onderwerpen/@149040/internationale/ (geraadpleegd 3 juli 2012).

Network (RBN) dat betrokken was bij de verspreiding van malware, DDoS-aanvallen uitvoerde en zich bezig hield met hacken, kinderporno en spam.[79] De indruk lijkt te bestaan dat dergelijke bendes worden geleid door criminelen die zich ook met delicten als drugs en mensenhandel bezighouden en die groepen van programmeurs en hackers aansturen. Het gaat bij deze vorm van cybercrime duidelijk om financieel gewin of om politieke doeleinden. Volgens een van de geïnterviewde experts lijken de hackers die deel uitmaken van dergelijke netwerken niet principieel te verschillen van de eerder beschreven niet-crimineel georiënteerde hackers. Het gaat om nieuwsgierige jonge mannen (meestal) met geldingsdrang die voldoening krijgen uit het oplossen van puzzels (doorbreken van computerbeveiligingen). Ze kunnen daarbij mede gedreven worden door financiële motieven, maar ook door dezelfde motieven als wittehoedhackers.[80]

4.3. Vormen van misbruik van de cloud

Cloud computing heeft, net als het Internet in ruimere zin, een aantal kenmerken die het een potentieel interessant platform maken voor criminele handelingen. Verschijnselen zoals phishing, downtime (platleggen van apparatuur), datalekken en botnets bestonden al voordat de cloud populair werd.[81] Ze zijn mogelijk door zwakheden in de ICT-infrastructuur. De aandacht voor vraagstukken rond cloudbeveiliging en daarmee samenhangend rond cybercrime in de cloud wijkt vooralsnog niet veel af van die voor Internetveiligheid in het algemeen.[82] Cloud computing, en algemener het uitbesteden van ICT, kan echter bepaalde kwetsbaarheden versterken of nieuwe kwetsbaarheden introduceren, doordat data op afstand van de organisatie komen te staan en vanwege de schaalbaarheid van rekencapaciteit in de cloud.

4.3.1. Verlies/gijzeling van data in de cloud

Door cloud computing verdwijnt een deel van de controle over de data en IT-processen en ontstaat een afhankelijkheid van de beveiligingsmaatregelen van de cloudaanbieder. Het verdienmodel van veel cloudaanbieders is mede gebaseerd op het feit dat ze relatief minder overcapaciteit hoeven te hebben naarmate er meer gebruikers zijn (de gebruikers zullen immers niet allemaal tegelijkertijd hun maximale belasting vragen), waardoor de investeringskosten in apparatuur lager kunnen uitvallen. Cloudaanbieders hebben er daarom belang bij zo veel mogelijk klanten binnen te halen en concurrentie op prijs zal daarbij een belangrijke methode zijn. Dit kan gepaard gaan met onvoldoende investeringen in beveiliging,[83] met als gevolg dat de cloud een relatief interessant doelwit is voor kwaadwillenden. Daartegenover wordt gesteld dat de concentratie van data en dataverwerking bij een beperkt aantal cloudaanbieders juist kansen biedt om de beveiliging goed te organiseren.[84] Er is schaarste aan beveiligingsexperts en concentratie van de beschikbare kennis bij een kleiner aantal partijen kan derhalve efficiëntieverhogend werken.

Wanneer data buiten de eigen organisatie worden geplaatst, kan de beschikbaarheid, vertrouwelijkheid en integriteit van de data onder grotere druk komen te staan, hoewel ook het omgekeerde het geval kan zijn. Cloudaanbieders zullen namelijk de data doorgaans redundant opslaan en de beveiliging beter op orde hebben dan menig bedrijf waarvoor IT niet de kerntaak is. Of de migratie naar de cloud uiteindelijk beveiliging verhoogt of verlaagt, is moeilijk te zeggen. Centralisatie en decentralisatie van gegevensverwerking kennen verschillende typen risico's, die niet in alle opzichten goed vergelijkbaar zijn.[85] Duidelijk is in elk geval wel dat er bij centralisatie, ook als een cloudaanbieder een behoorlijke vorm van beveiliging biedt, bepaalde risico's bestaan door de uitplaatsing van de data.

De beschikbaarheid van data kan op verschillende manieren onder druk komen te staan. Toegang tot de data is in de eerste plaats afhankelijk van de toegankelijkheid van het platform.

---

[79] http://www.bizeul.org/files/RBN_study.pdf; http://www.networkworld.com/newsletters/sec/2011/032811sec1.html (geraadpleegd 3 juli 2012).
[80] Interview Fox-IT.
[81] Zie bronnen in Chen e.a. 2010.
[82] Ibid.
[83] Biggs & Vidalis 2010, p. 64.
[84] Chen e.a. 2010.
[85] 'The key conclusion of this paper is that the scale and flexibility are both a friend and a foe from a security point.' Catteddu & Hogben 2009, p.4.

Cloudaanbieders kunnen nooit volledige beschikbaarheid van hun voorzieningen garanderen, zelfs niet wanneer grootschalige redundantie in hun infrastructuur bestaat. Veel cloudaanbieders hebben te maken gehad met (tijdelijke) uitval van hun voorzieningen, waardoor grote groepen van gebruikers worden getroffen. Internationale voorbeelden zijn de uitval van een kritiek systeem bij Salesforce.com in 2009 waardoor 900.000 gebruikers niet bij hun data en applicaties konden en een uitval van voorzieningen bij Microsoft in 2009 waardoor 800.000 Sidekick gebruikers niet bij hun data konden.[86] Chen en anderen beschrijven een geval waarin een groot aantal Amazon EC2-machines door Spamhaus is geblokkeerd, waardoor gebruikers van deze machines gedurende enige tijd geen email meer konden versturen. De opname van de Amazon machines in de blacklist van Spamhouse volgde op misbruik door een spammer van een van de Amazon-machines.[87] Dit zijn weliswaar geen voorbeelden van beschikbaarheidsproblemen als gevolg van criminele handelingen, maar het is voorstelbaar dat criminelen zich richten op het verstoren van de beschikbaarheid van cloudsystemen als geheel. Het motief daarvoor kan zijn afpersing of (politieke) sabotage.

Een tweede mogelijke beperking van toegang tot data of voorzieningen bestaat op het niveau van individuele cloudgebruikers. Wanneer derden zich toegang tot de cloud kunnen verschaffen, wordt het mogelijk de toegang tot de data door de eigenaar te beletten door bijvoorbeeld de toegang tot de cloud te blokkeren (door verandering van het wachtwoord) of de data te versleutelen. De data van gebruikers kunnen op die manier worden gegijzeld en de cloudgebruiker worden afgeperst. Dit is een variant op de al bestaande gijzelwaar (*ransomware*).[88] Wanneer de betaling van het losgeld plaatsvindt via *premium-rate test messages* of via online voucherbetaalkanalen zoals Ukash of Paysafecard, is het achterhalen van de daders bovendien erg lastig.

Ook de vertrouwelijkheid van de data loopt risico's in de cloud. Evident is dat als derden zich toegang kunnen verschaffen tot dataopslag in de cloud, deze data ook kunnen worden gekopieerd. Bedrijfsspionage is een voorbeeld van een reden waarom criminelen zich toegang zouden willen verschaffen tot clouddiensten. Ook consumenten lopen risico's wanneer zij gegevens en documenten in de cloud opslaan; mede door het gebruik van verschillende (ook mobiele) apparaten waarmee de cloud kan worden benaderd, ontstaan extra risico's voor het misbruiken van toegangsgegevens. Identiteitsfraude kan hierdoor een nieuwe dynamiek krijgen.[89] Risico's bestaan niet alleen uit onrechtmatige toegang tot data door misdadigers; de vertrouwelijkheid van data is ook in het geding als opsporingsinstanties zonder geldige juridische basis gegevens uit de cloud opvragen.[90]

Een geavanceerde vorm van verkrijgen van data van cloudgebruikers bestaat uit het uitvoeren van *side channel attacks* in IaaS- en PaaS-diensten.[91] Cloudaanbieders zoals Microsoft (Azure) en Amazon (EC2) bieden de mogelijkheid aan om verschillende virtuele machines (VM's, dat wil zeggen een softwarematige nabootsing van een fysieke computer) te initiëren op hun gedeelde hardware. In theorie zijn de verschillende VM's volledig van elkaar gescheiden en kan er geen gegevensuitwisseling plaatsvinden tussen de verschillende virtuele machines. Ristenpart en collega's beschrijven hoe het mogelijk is om toch de virtuele machine van een beoogd slachtoffer te lokaliseren en vervolgens een eigen VM op dezelfde fysieke machine te creëren om vervolgens via een 'side-channel attack' te pogen data te ontvreemden uit de omgeving van het slachtoffer. In de experimenten die ze beschrijven blijkt het inderdaad mogelijk om een dergelijke aanval uit te voeren in een testomgeving.[92] Het spreekt voor zich dat als derden zich toegang kunnen verstrekken tot de cloudomgeving van een gebruiker, deze ook in staat zullen zijn om de integriteit van de data aan te tasten.

---

[86] Dabhur et al. 2011. Zie *Salesforce.com outage hits thousands of businesses,* DOI= http://news.cnet.com/8301-1001_3-10136540- 92.html en BBC, *The Sidekick Cloud Disaster,* DOI= http://www.bbc.co.uk/blogs/technology/2009/10/the_side kick_cloud_disaster.html (geraadpleegd 3 juli 2012).
[87] Chen e.a. 2010.
[88] Nationaal Cyber Security Centrum 2012, p. 27 en 45.
[89] Baiba Kaškina, reactie op enquête.
[90] Article 29 Working Party (2012), p. 5 ('There is a risk that personal data could be disclosed to (foreign) law enforcement agencies without a valid EU legal basis and thus a breach of EU data protection law would occur.')
[91] Ristenpart e.a. 2009.
[92] Ibid.

4.3.2. Delen van informatie

Een tweede vorm van crimineel gedrag in de cloud betreft het delen van informatie. Het gaat hier niet om een volstrekt nieuwe vorm van crimineel gedrag, delen van informatie kan immers vanuit iedere op het Internet beschikbare machine of applicatie (webpagina, email, chat, enzovoorts). De cloud faciliteert dergelijk gedrag wel, aangezien de kosten van het delen van informatie door de *resource sharing* drastisch omlaag zijn gegaan. Iedere cloud aanbieder biedt gratis voorzieningen aan voor bescheiden hoeveelheden data (bijvoorbeeld 5 Gb), waardoor de drempel om materiaal beschikbaar te stellen aan derden lager is dan wanneer de aanbieder webruimte moet huren bij de traditionele webruimteaanbieders. Ook wordt informatie gedeeld via gedeelde webmaildiensten waarbij berichten in de conceptenbox toegankelijk worden gesteld voor leden van een netwerk. Ook vindt delen van informatie plaats via diensten zoals Google Docs waarbij de accountgegevens binnen het netwerk worden gedeeld.

In de cloud vinden op grote schaal auteursrechtschendingen plaats. Voorbeelden van clouddiensten die ervan worden verdacht grote hoeveelheden auteursrechtelijk beschermde werken te netvesten zijn Megaupload,[93] Hotfile, RapidShare, MediaFire, MegaVideo en Dropbox. Gebruikers plaatsen op dergelijk 'cyberlockers' al dan niet versleutelde bestanden; de URL's van de bestanden (en eventueel gebruikersnaam en wachtwoord) worden vervolgens gedeeld binnen het netwerk van mensen die toegang tot de bestanden mogen krijgen. Ook kinderporno wordt op deze manier verspreid, zij het dat dit eerder zal gebeuren via private cloudachtige diensten via darknets en niet via publieke cloudaanbieders.

Aan de randen van de cloud bevinden zich p2p-netwerken die eveneens op kleine en grotere schaal worden gebruikt voor het delen van auteursrechtelijk en kinderpornografisch materiaal. Het gaat hier om geheel open netwerken gevoed vanuit bijvoorbeeld The Pirate Bay, maar ook om meer gesloten netwerken zoals Gigatribe.[94] Gigatribe is een soort p2p-netwerk opgebouwd rond het idee dat het netwerk een stam is, die redelijk gesloten is en buitenstaanders niet makkelijk toelaat. Dergelijke relatief gesloten platforms met cyberlockerdiensten zijn relatief populair onder kinderpornoverspreiders.[95]

4.3.3. Botnets en malware

Een derde vorm van crimineel gebruik van de cloud betreft het gebruik van de rekenkracht van de cloud om bijvoorbeeld wachtwoorden te kraken. Voor dit doel worden traditioneel botnets ingezet die bestaan uit gekaapte pc's van doorgaans onbewuste eigenaars. Deze pc's moeten eerst worden geïnfecteerd met malware om ze onder controle van het botnet te krijgen. De mogelijkheid om snel, eenvoudig en betrekkelijk goedkoop virtuele machines te huren in de cloud biedt voor (zwartehoed-)hackers een potentieel aantrekkelijk alternatief voor het opbouwen van botnets.[96] De kosten van het huren van virtuele machines liggen hoger dan die van 'klassieke' botnets.[97] Daartegenover staat echter dat de kwaliteit van gehuurde machines hoger is dan die van botnetmachines[98] en hackers zouden daarom de hogere prijs voor lief kunnen nemen. Botnets in de cloud zijn eenvoudiger te beëindigen, zowel door de gebruikers wanneer het hen te heet onder de voeten wordt, als door de cloudaanbieder wanneer dergelijk misbruik van hun systemen wordt ontdekt. Het is echter makkelijk om materiaal uit een virtuele machine snel naar een andere virtuele machine bij een andere aanbieder over te zetten; in dit opzicht maken cloudplatforms het moeilijker om phishing-pagina's effectief uit de lucht te halen, vanwege het gemak en de snelheid waarmee ze kunnen worden verplaatst.[99]

---

[93] Megaupload is in januari 2012 op last van de FBI uit de lucht gehaald, zie bijv. http://www.nrc.nl/nieuws/2012/01/19/een-van-de-grootste-filehosters-ter-wereld-uit-de-lucht-gehaald/

[94] 'GigaTribe is a peer-to-peer file sharing network. Originally developed in France, its American version was launched in November 2008. It offers free and paid versions; with the paid version users may restrict access to their encrypted files to a group of trusted friends.' http://en.wikipedia.org/wiki/GigaTribe (geraadpleegd 3 juli 2012).

[95] Interview Openbaar Ministerie.

[96] Chen e.a. 2010.

[97] Meer e.a. 2009.

[98] Herley 2009.

[99] Interview Rabobank Nederland.

Thomas Roth heeft als experiment laten zien dat virtuele machines van Amazon EC2 ook gebruikt kunnen worden om SHA-1 wachtwoordhashes te kraken.[100] Het experiment met Cuda-Multiforcer-software heeft hem $2 gekost voor de huur van een batterij krachtige grafische processoren.

Verder kan een IaaS-dienst worden gebruikt als platform om botnets te controleren gebaseerd op de Zeus 'crimeware kit'.[101] Dit softwarepakket wordt gebruikt door cybercriminelen om botnets te ontwikkelen. In 2009 is een Zeus-variant ontdekt die gebruik maakt van de Amazon EC2-infrastructuur (een IaaS).[102] Het gebruik van een cloudinfrastructuur voor een botnet kan voordelig zijn voor criminelen omdat detectie van het botnetverkeer wordt gemaskeerd doordat het deel uitmaakt van legitiem cloudverkeer. Bovendien is het lastig om de servers op een zwarte lijst te plaatsen omdat ze worden gedeeld met vele legitieme gebruikers.

4.4. Jurisdictie

Vanuit materieel strafrechtelijk oogpunt levert de cloud weinig bijzondere problemen op. Wel vragen diverse van onze geïnterviewde experts en buitenlandse respondenten aandacht voor materiële jurisdictievragen: welk land heeft of welke landen hebben rechtsmacht over een delict dat 'in' of via de cloud is gepleegd? Bijvoorbeeld: hoe bepalen we welk land moet vervolgen voor opslag van kinderpornografie als de bestanden zijn opgeslagen op servers in verschillende landen?[103] Bij deze vraag spelen drie aspecten een rol.

Het eerste aspect is of bepaalbaar is waar precies een bestand ligt opgeslagen als het 'in de cloud' ligt. De aanhangers van cyberspace als zelfstandige ruimte die los moet worden gezien van (statelijk) territoir zullen deze vraag negatief beantwoorden: het bestand staat primair 'in cyberspace' en men moet niet het bestand willen lokaliseren op de plaats van de server waar het toevallig opgeslagen ligt of voorbij komt.[104] Aanhangers van de fysieke benadering van cyberspace betogen dat cyberspace wordt geconstitueerd door computers en kabels en dat de plaats van servers daarom goede aanknopingspunten biedt voor bepaling van 'waar in cyberspace' iets plaatsvindt.[105] Deze laatste benadering, die dominant is bij wetgevers en rechters omdat zij nu eenmaal gewend zijn aan het koppelen van recht aan een fysieke plaats, wordt problematisch met de komst van de cloud.[106] Ten eerste worden bestanden vaak redundant opgeslagen, dus op meerdere plaatsen. Ten tweede worden bestanden meestal in stukjes verdeeld opgeslagen, zodat een individueel (kinderporno)plaatje heel wel opgeknipt kan liggen in de VS, Duitsland en IJsland. Ten derde is het voor cloudaanbieders zelf niet relevant om te weten waar een bestand opgeslagen ligt; de locatie wordt vaak automatisch berekend aan de hand van algoritmes die de meest efficiënte opslagplaats uitrekenen. Daarbij kunnen bestanden ook automatisch worden verplaatst afhankelijk van vraag en aanbod in het netwerk. Voor de cloudaanbieder en de klant gaat het om logische toegang tot een bestand (dat wil zeggen het te allen tijde kunnen opvragen), en niet om fysieke toegang (dat wil zeggen de server waar een bestand(deel) is opgeslagen, Voor de techniek en het bedrijfsmodel van cloud computing is de precieze fysieke locatie van een bepaald bestand simpelweg geen relevant aspect meer. In combinatie betekent dit dat wanneer een bestand uit de cloud wordt gehaald (door een gebruiker, politie of aanbieder), het moeilijk te bepalen zal zijn van welke server(s) het bestand op dat moment precies afkomstig is.[107] Uitgaan van de locatie van opslag op een server is dan ook geen goed aanknopingspunt voor het bepalen van rechtsmacht in de cloud.

Dat betekent echter niet als zodanig een probleem. Het tweede aspect van de jurisdictievraag is namelijk welke aanknopingspunten er zijn voor materiële jurisdictie. Rechtsmacht is niet

[100] Zie http://www.darknet.org.uk/2010/11/sha-1-password-hashes-cracked-using-amazon-ec2-gpu-cloud/ (geraadpleegd 3 juli 2012).
[101] Dabhur e.a. 2011.
[102] *Zeus crimeware using Amazon's EC2 as command and control server,* DOI= http://www.zdnet.com/blog/security/zeus-crimeare- using-amazons-ec2-as-command-and-control- server/5110.
[103] Yves Nicolet, reactie op enquête.
[104] Zie met name Johnson & Post 1996. Vergelijk Lodder 2012, p. 18: 'Informatie staat eerst en vooral op internet en pas op de tweede plaats is er een link met een plek op onze aarde. Soevereiniteit schiet zijn doel voorbij als deze wordt ingeroepen omdat informatie toevallig fysiek op een bepaalde computer te vinden is.'
[105] Zie met name Goldsmith 1998.
[106] Zie ook Velasco 2009, p. 6.
[107] Schwerha 2010, p. 8-9; Spoenle 2010.

beperkt tot de locatie waar een delict is gepleegd, maar strekt zich veelal ook uit over locaties waar effecten van het delict optreden, waar een instrument, de dader of het slachtoffer van het delict zich bevindt; ook kan rechtsmacht gegrond worden, voor bepaalde delicten, op nationaliteit van dader of slachtoffer. Al met al betekent dit bij cybercriminaliteit dat er bijna altijd wel een aanknopingspunt kan worden gevonden om rechtsmacht op te baseren.[108] In het voorbeeld van in de cloud opgeslagen kinderporno kan men jurisdictie bepalen aan de hand van de locatie van de computer vanwaaraf het bestand in de cloud is geplaatst of van de computer waarmee de cloudabonnee zich toegang verschaft tot het bestand in de cloud, en feitelijk ook de locatie van de dader op elk moment dat hij de kinderpornografie in zijn bezit heeft[109] of zich toegang verschaft tot het bestand. Voor Nederland is verder van belang dat het rechtsmacht heeft over alle cybercriminaliteit gepleegd door Nederlanders, of zij het feit nu hebben gepleegd in Nederland (art. 2a Sr) of buiten Nederland (art. 5 lid 1 onder 4° Sr). Voor de Nederlandse justitie zullen er daarom genoeg aanknopingspunten zijn om, waar zij dat opportuun vindt, misdrijven gepleegd in of via de cloud te vervolgen.

Dat roept wel de vraag op – het derde aspect van de jurisdictievraag – hoe omgegaan moet worden met positieve rechtsmachtconflicten, dat wil zeggen wanneer meerdere landen rechtsmacht kunnen of willen opeisen over een strafbaar feit. Dat is eigenlijk de belangrijkste vraag bij jurisdictie in relatie tot de cloud, aangezien vaak meerdere landen op basis van de aanknopingspunten (locatie van computer als instrument of waar het effect optreedt; nationaliteit) rechtsmacht zouden kunnen opeisen. Die vraag is wederom niet specifiek voor de cloud, maar zal mogelijk wel vaker aan de orde komen naarmate misdaad via de cloud toeneemt. Het Cybercrime-Verdrag biedt weinig houvast, aangezien het slechts bepaalt dat wanneer meerdere staten rechtsmacht opeisen, zij, 'waar dienstig', met elkaar overleggen 'met het oog op de vaststelling van de meest geschikte rechtsmacht om tot vervolging over te gaan' (art. 22 lid 5 Cybercrime-Verdrag). Factoren die bij het beslissen over prioriteit in vervolging van belang kunnen zijn, zijn onder andere waar de verdachte zich (in voorlopige hechtenis) bevindt, waar getuigen of bewijsmateriaal voorhanden is, waar de meeste schade is aangericht en in welk land vervolging het meest kansrijk is.[110]

4.5. Lacunes in strafbaarstelling?

De geïnterviewde experts en buitenlandse respondenten geven aan dat er weinig verschil lijkt te bestaan tussen de cloud en 'klassieke' Internetcriminaliteit. Dit betekent dat reeds gesignaleerde hiaten (zoals heling van gegevens) ook bij de cloud zullen spelen, maar niet specifiek zijn in relatie tot de cloud. Op basis van ons bronnenonderzoek lijken er geen bijzondere lacunes te bestaan in de materiële strafwetgeving die de bestrijding van cloudgerelateerde criminaliteit zouden bemoeilijken. Het enige aspect waarin de cloud relatief nieuw lijkt voor het materiële strafrecht, is het faciliteren van het kraken van wachtwoorden en versleutelde bestanden. Dat kan weliswaar ook met 'oude' applicaties (supercomputers of botnets) maar het zou door de rekenkracht van cloudinfrastructuur meer dan voorheen gefaciliteerd kunnen worden, waardoor bestaande kwetsbaarheden van datalekken en identiteitsfraude kunnen worden vergroot. De wetgever zou wellicht nader kunnen onderzoeken of het materiële strafrecht kan of moet worden ingeroepen tegen het (systematisch, grootschalig) kraken van wachtwoorden. Het valt niet onder (poging tot) oplichting of onder misbruik van hulpmiddelen (art. 139d lid 2 Sr) en zal als zodanig niet strafbaar zijn. De vraag is wel of de gevaarzetting van wachtwoordkraken dusdanig groot wordt door de cloud dat zelfstandige strafbaarstelling, vergelijkbaar met misbruik van hulpmiddelen, nodig is. Men zou ook kunnen volstaan met bestaande bepalingen die het misbruik van (al dan niet gekraakte) wachtwoorden strafbaar stelt (zoals hacken en oplichting).

Een vraag die belangrijker is voor het materiële strafrecht, is of de strafbepalingen die ter bescherming dienen van de beschikbaarheid, vertrouwelijkheid en deugdelijkheid van gegevens (zoals de strafbaarstelling van computersabotage, verstikkingsaanvallen en gegevensaantasting)

[108] Zie uitgebreid Brenner & Koops 2004.
[109] De rechtspraak zal moeten interpreteren of een bestand opgeslagen in de cloud in bezit is van de cloudabonnee. Mocht de rechter bepalen dat dat niet zo is, dan zal vervolging plaats kunnen vinden op basis van het ooit in bezit gehad hebben (namelijk op het moment dat de abonnee het bestand in de cloud plaatste) dan wel het zich toegang verschaffen tot het bestand op het moment dat de abonnee het bestand opvraagt uit de cloud.
[110] Zie Brenner 2006.

afdoende zijn voor de bescherming van data die burgers en bedrijven in de cloud opslaan. Een van onze respondenten noemt als mogelijke lacune de 'lack of legal instruments to guarantee the security of data stored by Cloud Providers '.[111] Dat zal echter vooral te maken hebben met de handhaving en handhaafbaarheid van de beveiligingseisen uit de Telecommunicatiewet (art. 11.3 Tw) en Wet bescherming persoonsgegevens (art. 13-14 Wbp), waar jurisdictiecomplicaties bijkomen als de cloudaanbieder in het buitenland is gevestigd, en niet zozeer met lacunes in de strafbaarstelling.

Art. 273d Sr is van toepassing op cloudaanbieders die een telecommunicatiedienst of -netwerk aanbieder (zowel openbaar als besloten), wat betekent dat cloud(communicatie)aanbieders niet wederrechtelijk[112] de inhoud van aan hen toevertrouwde gegevens mogen inzien, overnemen of verspreiden; dit geldt niet alleen voor communicatie (webmail) maar ook voor niet-communicatieve documenten, nu de bepaling in het algemeen spreekt van gegevens 'die door tussenkomst van [een telecommunicatienetwerk of -dienst] zijn opgeslagen, worden verwerkt of overgedragen en die niet voor hem zijn bestemd'. Wel zit hier een mogelijke lacune voorzover cloudaanbieders die opslagdiensten aanbieden niet onder de definitie van telecommunicatieaanbieder vallen (vgl. par. 5.2.1). Het valt te overwegen om de bescherming van de inhoud van aan de cloud toevertrouwde gegevens gelijk te trekken voor alle typen cloudaanbieders, bijvoorbeeld door in art. 273d in plaats van bij telecommunicatieaanbieders aan te sluiten bij het mogelijk ruimere begrip communicatieaanbieders (als bedoeld in art. 126la Sv), dan wel aanbieders van opslagdiensten zelfstandig toe te voegen aan art. 273d.

Verder kent de Nederlandse wetgeving ook enkele culpoze delicten die een prikkel zouden moeten kunnen bieden aan cloudaanbieders om hun diensten en infrastructuur te beschermen tegen misbruik. Wanneer een cloudaanbieder te weinig maatregelen neemt tegen DDoS-aanvallen die vanuit zijn netwerk of dienst worden gepleegd, kan hij mogelijk vervolgd worden wegens verwijtbare schuld aan computersabotage (art. 161septies Sr). Ook kan culpoze gegevensaantasting en culpoze virusverspreiding (art. 350b Sr) ingeroepen worden tegen cloudaanbieders die onvoldoende maatregelen nemen tegen het verspreiden van wanwaar via hun netwerk of dienst. Daarbij zij aangetekend dat een aanbieder het vermoedelijk wel bont moet maken met (niet-)beveiliging van zijn netwerk of dienst voordat hij op basis van een culpoos delict vervolgd zal worden. Het Openbaar Ministerie zou echter een beroep kunnen doen op de Garantenstellung-figuur, die aangeeft dat bepaalde posities in de maatschappij zwaardere verantwoordelijkheden met zich meebrengen, en kunnen betogen dat een cloudaanbieder naar maatschappelijke maatstaven een bijzondere verantwoordelijkheid heeft zijn diensten naar de stand van de techniek adequaat te beveiligen. Op die basis is een vervolging van een slecht beveiligde cloudaanbieder goed denkbaar. Een dergelijke vervolging zou een goede prikkel kunnen opleveren voor de branche om zich beter te beveiligen tegen misdadigers die hun diensten en netwerken willen exploiteren.

Aan de andere kant bestaat het gevaar dat een rem wordt gezet op de verdere ontwikkeling van cloud computing, wanneer cloudaanbieders in te hoge mate strafrechtelijk aansprakelijk zouden kunnen worden gehouden voor criminaliteit die via hun diensten worden gepleegd. De aansprakelijkheid van cloudaanbieders verdient daarom aandacht.[113] De bestaande aansprakelijkheidsuitsluitingsgrond voor Internetaanbieders van art. 54a Sr is in beginsel ook van toepassing op cloudaanbieders, voorzover zij telecommunicatieaanbieders zijn. Evenals bij art. 273d Sr kan de vraag worden gesteld of dit moet worden uitgebreid tot cloudaanbieders die geen (tele)communicatiedienst aanbieden maar enkel een opslagdienst. Nu ziet art. 54a Sr vooral op aanbieders die vervolgd zouden kunnen worden als medepleger of medeplichtige van uitingsdelicten; zij kunnen aan vervolging ontkomen door de onrechtmatige gegevens te ontoegankelijk te maken op vordering van de officier van justitie. Los van de bestaande onvolkomenheden van deze bepaling,[114] zien de meeste clouddiensten niet op publicatie van

[111] Lorenzo Picotti, reactie op enquête.
[112] Dus wel met toestemming van de gebruiker (wat mede kan omvatten situaties waarin volgens de Algemene Voorwaarden de dienstaanbieder zich het recht voorbehoudt om gegevens in te zien of te verstrekken aan derden) en bij een wettelijke plicht, zoals een justitiële vordering.
[113] Zie Micozzi 2011.
[114] Zie het Conceptwetsvoorstel versterking bestrijding computercriminaliteit en de toelichting daarbij uit 2010, http://www.internetconsultatie.nl/wetsvoorstel_versterking_bestrijding_computercriminaliteit.

uitingen, maar op besloten opslag en uitwisseling van gegevens. Uitingsdelicten die een component hebben van openbaarmaking of ruchtbaarheid geven zullen zich daarbij dan ook niet snel voordoen. Het bezit of de verspreiding van of toegang tot kinderpornografie kan echter wel in het geding zijn.

Zou art. 54 Sr van toepassing moeten zijn op opslagaanbieders die (zonder hun opzettelijke medewerking) kinderpornografie huisvesten? Vanuit de ratio van art. 54a Sr (dat voortkomt uit de Richtlijn elektronische handel)[115] is daar niet direct reden voor: art. 54a Sr (evenals de civiele aansprakelijkheidsuitsluitingen in art. 6:196 BW) beoogt zelfcensuur door met name hostingaanbieders te voorkomen, teneinde de vrije meningsuiting op Internet te waarborgen. Bij besloten opslag en uitwisseling van gegevens via de cloud is de vrije meningsuiting niet of nauwelijks.[116] Er valt daarom iets voor te zeggen om opslagaanbieders geen bijzondere aansprakelijkheidsuitsluiting te bieden gekoppeld aan een justitiële vordering, maar hun aansprakelijkheid over te laten aan de mate waarin zij volgens de gewone maatstaven medeplichtig kunnen worden gehouden voor bezit of verspreiding van kinderpornografie.

Aan de andere kant zijn er ook argumenten om art. 54a Sr wel uit te breiden tot opslag- en mogelijk ook tot infrastructuur- en platformaanbieders. Aangezien de cloud misbruikt kan worden om botnets en malware te faciliteren, lopen cloudaanbieders het risico vervolgd te worden voor medeplegen, medeplichtigheid of verwijtbare schuld aan computercriminaliteit. Aanbieders zouden daarom mogelijk strenge maatregelen kunnen gaan nemen om deze aansprakelijkheidsrisico's uit te sluiten. Dat zou een verkillend effect kunnen hebben op de ontwikkeling van clouddiensten en mogelijk ook, indien aanbieders tot vergaande monitoring van cloudverkeer zouden overgaan, afbreuk doen aan de privacybescherming van burgers en bedrijven in de cloud. Met dezelfde redenering als destijds de Richtlijn elektronische handel een aansprakelijkheidsuitsluiting invoerde, namelijk om de ontwikkeling van het Internet niet te belemmeren,[117] zou men nu kunnen overwegen om een generieke aansprakelijkheidsuitsluiting voor cloudaanbieders in te voeren voor via hun netwerk of dienst gepleegde computerdelicten, als zij alle maatregelen hebben getroffen om het desbetreffende misbruik te beëindigen zodra zij kennis hebben gekregen van het misbruik. Een dergelijke bepaling zou de innovatie en doorontwikkeling van cloud computing kunnen stimuleren. Wellicht zou het echter ook afbreuk kunnen doen aan de juridische prikkels voor aanbieders om hun netwerken en diensten goed te beveiligen. De aansprakelijkheidsuitsluiting is daarom een complex vraagstuk dat raakt aan de bredere beleidsvraag van sturingsinstrumenten om cyberbeveiliging in de cloud te stimuleren, die bijvoorbeeld opgepakt zou kunnen worden door de Nationale CyberSecurity Raad.

4.6. Conclusie

Voor het plegen van strafbare feiten biedt de cloud een nieuw instrument, maar het verschilt daarin niet fundamenteel van andere ICT-applicaties. Elke technische ontwikkeling brengt nieuwe kwetsbaarheden met zich mee. Op basis van onze bronnen kunnen we vaststellen dat er geen bijzondere aspecten lijken te zijn die cloudgerelateerde criminaliteit substantieel anders maken dan andere vormen van cybercriminaliteit. Potentiële daders zijn – voorzover dat op basis van schaarse literatuur kan worden gesteld – dezelfde als plegers van cybercriminaliteit, en de typen manieren waarop zij de cloud kunnen gebruiken – voor aanvallen op gegevens of systemen of voor het onderling delen van informatie – verschillen niet fundamenteel van 'klassieke' cybercriminaliteit. Hooguit zullen nuanceverschillen en verschuivingen optreden, afhankelijk van waar de zwakste schakels zitten in ICT-beveiliging; als de cloud relatief slecht wordt beveiligd, wordt het een aantrekkelijk doelwit, zeker als bedrijven en overheden overstappen naar clouddiensten. Dat roept wel beleidsvragen op, met name rond cyberbeveiliging in relatie tot de cloud, maar weinig (nieuwe) juridische vragen.

---

[115] Zie *Stb.* 2004, 210.

[116] Behoudens een zekere mate van garingsvrijheid die wordt gefaciliteerd door de uitwisseling van documenten.

[117] De Memorie van Toelichting bij de implementatiewet verwijst naar 'de algemene intermediaire functie die in het huidige en toekomstige, internationale maatschappelijke verkeer wordt vervuld door de tussenpersoon die een telecommunicatiedienst verleent bestaande in de doorgifte of opslag van gegevens. Het (…) belang van een onbelemmerde informatieuitwisseling alsmede het belang van een vrij verkeer van diensten waarop de onderhavige richtlijn in het bijzonder ziet, maken het wenselijk dat die functievervulling ongehinderd kan plaatsvinden.' *Kamerstukken II* 2001/02, 28 197, nr. 3, p. 63.

Het vaststellen van rechtsmacht zal, voor Nederland in elk geval, meestal geen probleem opleveren. Het Wetboek van Strafrecht lijkt vooralsnog voldoende geschikt te zijn om criminaliteit gepleegd in of via de cloud te kunnen vervolgen. Op enkele onderdelen kan worden bekeken of aanpassingen wenselijk zijn. Met name zou de wetgever nader kunnen onderzoeken of bepalingen betreffende telecommunicatieaanbieders, zoals art. 273d en 54a Sr, van toepassing zijn of zouden moeten zijn op cloudopslagaanbieders. Nu bedrijven en burgers niet alleen communiceren en publiceren via ISP's, maar ook hun bestanden langdurig toevertrouwen aan Internetdienstverleners, gaat het immers niet alleen om bescherming van communicatie maar ook om bescherming van aan dienstverleners toevertrouwde gegevens in het algemeen. Het ligt voor de hand om art. 273d Sr in dat licht uit te breiden tot opslagaanbieders, maar of de aansprakelijkheidsuitsluiting van art. 54a Sr ook van toepassing zou moeten zijn op cloudaanbieders, is een complexere vraag die betrokken moet worden bij de bredere beleidsvorming rond beveiliging van cloud computing.

5. Opsporing in de cloud: procedureel strafrecht

Door haar internationale, gedistribueerde karakter levert cloud computing evidente uitdagingen op voor de opsporing. In dit hoofdstuk gaan we eerst in op de internationale aspecten: hoe kunnen data uit de grensoverschrijdende cloud worden verkregen? Vervolgens behandelen we de, deels hiermee samenhangende, problematiek van de opsporingspraktijk, die meer dan ooit te maken zal krijgen met gegevens die niet ter plekke voorhanden zijn en die bovendien vaker versleuteld kunnen zijn. Daarna gaan we in op de toepassing van enkele specifieke opsporingsbevoegdheden waarbij de cloud vragen oproept, zoals het onderscheid tussen opgeslagen en getransporteerde gegevens. Naast deze mogelijke probleempunten levert de cloud ook enkele kansen op voor de opsporing, die we in tot slot behandelen.

5.1. Opsporing in een grensoverschrijdende context

Opsporing van strafbare feiten is nauw verbonden met nationale soevereiniteit: een staat is bevoegd op haar eigen territoir opsporingshandelingen te verrichten, maar niet op buitenlands grondgebied. Wanneer de Nederlandse politie bewijsmateriaal dat ligt opgeslagen in de cloud wil verzamelen, zal dit vrijwel altijd raken aan de grenzen van de strafvorderlijke rechtsmacht: cloudaanbieders opereren in een internationale context en het materiaal ligt opgeslagen op verschillende servers, waarbij het meestal niet goed aanwijsbaar is op welke locatie precies het materiaal (vaak in stukjes geknipt) ligt opgeslagen. Nu is dit geen nieuw probleem, aangezien opsporing in een Internetomgeving ook vaak in een grensoverschrijdende context moet opereren. Nog steeds wordt daarbij echter meestal aansluiting gezocht bij de plaats waar data opgeslagen zijn.[118] De versplinterdheid en onzichtbaarheid van dataopslag maakt het probleem voor cloud computing wel pregnanter. Zoals Jan Spoenle constateert:

> one could say that location as a constant applicable to all tangible objects and having been applied to intangible data objects ever since the Internet became popular as well, has ceased to function under the conditions of cloud computing.[119]

Er zijn globaal gesproken drie mogelijkheden om onderzoeksrelevante informatie of bewijs uit de cloud te verzamelen: aan de kant van de klant (via een netwerkzoeking), via de cloudaanbieder (via een vordering tot gegevensverstrekking) en ergens daartussenin (via interceptie van gegevens, bijvoorbeeld bij de toegangsaanbieder van de klant). We bespreken deze mogelijkheden in de achtereenvolgende paragrafen.

5.1.1. Grensoverschrijdende netwerkzoeking

De meest voorkomende situatie waarin de Nederlandse politie materiaal vanuit de cloud zal willen vergaren, is wanneer een Nederlandse ingezetene verdacht wordt van een strafbaar feit en men bewijsmateriaal rond die verdachte wil verzamelen. Naast de inzet van bijzondere opsporingsbevoegdheden als een tap of gegevensvordering (zie volgende paragrafen), is de doorzoeking bij de verdachte daarvoor een veelgebruikte methode. Bij die doorzoeking mogen computers onderzocht worden; computers kunnen ook (als dat proportioneel is) in beslag worden genomen en vervolgens op het bureau of door een forensisch instituut worden onderzocht.[120] Als gegevens echter niet op de computer of andere fysieke gegevensdragers ter plekke opgeslagen liggen, maar elders in een netwerk, heeft inbeslagname of onderzoek van de computer geen zin. Voor dat geval heeft de wetgever in 1993 de netwerkzoeking in het leven geroepen. Een doorzoeking kan vanaf de plaats waar deze plaatsvindt, worden voortgezet in een elders aanwezig computersysteem, mits de personen die op de plek van doorzoeking wonen, plegen te werken of te verblijven, met toestemming van de rechthebbende toegang tot een dergelijke computer hebben (art. 125j Sv).[121]

[118] Vgl. Brenner & Koops 2004, p. 44.
[119] Spoenle 2010, p. 5.
[120] Zie Koops & Buruma 2007, p. 91 e.v.
[121] Merk op dat de netwerkzoeking dus niet kan worden toegepast wanneer een computer, zoals een laptop, tablet of smartphone, in beslag wordt genomen buiten de situatie van een doorzoeking, bijvoorbeeld bij

De reikwijdte van de netwerkzoeking is echter beperkt tot de landsgrenzen. 'De Nederlandse wet kan immers geen grondslag bieden voor een onderzoek in een geautomatiseerd werk dat onder de jurisdictie van een ander land valt.'[122] Dat betekent dat een netwerkzoeking alleen mogelijk is als de computer waar gegevens opgeslagen liggen, zich kennelijk in Nederland bevindt, dan wel als er een uitdrukkelijke verdragsrechtelijke basis is voor een grensoverschrijdende netwerkzoeking.[123] Nu zou men kunnen stellen dat als je niet weet waar gegevens feitelijk opgeslagen liggen, deze 'kennelijk niet' in het buitenland liggen, maar dat is in het huidige netwerktijdperk geen houdbare stelling. Ook al heeft Nederland relatief veel servercapaciteit, er staan nog altijd meer servers in het buitenland – zeker van cloudaanbieders die veelal in het buitenland zijn gevestigd. Een opsporingsambtenaar die een netwerkzoeking doet, aanvaardt daarom de geenzins als denkbeeldig te verwaarlozen kans dat de data feitelijk in het buitenland liggen opgeslagen.

Een verdragsrechtelijke basis voor een grensoverschrijdende netwerkzoeking bestaat alleen in artikel 32 van het Cybercrime-Verdrag:

> Een Partij kan, zonder de toestemming van een andere Partij:
>
> a. zich toegang verschaffen tot opgeslagen publiekelijk toegankelijke (open bron) computergegevens, ongeacht waar deze zich in geografisch opzicht bevinden; of
>
> b. via een computersysteem dat zich op haar grondgebied bevindt, zich toegang verschaffen tot of de beschikking krijgen over opgeslagen computergegevens die zich bevinden in een andere Staat, indien de Partij de rechtmatige en vrijwillige instemming verkrijgt van de persoon die gerechtigd is de gegevens via dat computersysteem aan de Partij te verstrekken.[124]

Bij een netwerkzoeking naar cloudgegevens zal het geval onder a (op Internet voor het publiek beschikbare informatie) zich niet voordoen. Het geval onder b is wel mogelijk, maar dan moet de opsporingsambtenaar vrijwillige toestemming hebben van een rechthebbende. Dat kan zowel de cloudaanbieder als de verdachte zijn, mits deze vrijwillig meewerken. Dat ook cloudaanbieders rechthebbende kunnen zijn, blijkt uit de toelichting, die aangeeft dat een dienstaanbieder mag meewerken als zij daartoe bevoegd zijn;[125] die bevoegdheid wordt veelal geregeld in het contract met de klant, waarin veel aanbieders zich het recht voorbehouden om gegevens aan derden te verstrekken.[126]

In theorie is deze verdragsrechtelijke basis beperkt tot de momenteel 36 verdragspartijen,[127] en hoewel de Verenigde Staten (waar veel cloudaanbieders zijn gevestigd) verdragspartij zijn, kunnen data – ook van Amerikaanse aanbieders – opgeslagen liggen in landen die geen partij zijn bij het verdrag. Naar geldend recht mag, ook niet als de verdachte of de aanbieder vrijwillig toestemming geeft, door Nederlandse opsporingsambtenaren niet gezocht worden naar data die (kennelijk) op het grondgebied van niet-verdragsstaten liggen opgeslagen. In de praktijk zullen daar echter niet snel problemen ontstaan; behalve bij delicten met aanzienlijke internationale (cultuur)verschillen (zoals uitingsdelicten) of bij politiek gevoelige zaken (zoals internationale misdrijven), zal een ander land niet zo snel bezwaar maken als op hun grondgebied – incidenteel maar niet structureel – gegevens zijn verzameld met toestemming van de cloudgebruiker of -aanbieder ten behoeve van de opsporing van ernstige strafbare feiten.[128]

---

aanhouding. Naarmate meer gegevens niet meer op de computer maar in een cloud opgeslagen worden, zal er minder bewijs kunnen worden vergaard uit onderzoek van objecten die een verdachte bij aanhouding bij zich draagt.

[122] *Kamerstukken II* 1989/90, 21 551, nr. 3, p. 12.

[123] *Kamerstukken II* 1989/90, 21 551, nr. 3, p. 11.

[124] Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, *Trb.* 2002, 18.

[125] 'For example, a person's e-mail may be stored in another country by *a service provider*, or *a person* may intentionally store data in another country. *These persons* may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data, as provided in the Article' (cursivering toegevoegd). *Explanatory Report*, §294, beschikbaar op http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

[126] Zie onder, noot 145 en bijbehorende tekst.

[127] Stand van zaken juli 2012; zie http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.

[128] Niettemin ligt de toepassing van art. 32(b) Cybercrime-verdrag wel gevoelig. Landen als Rusland, Oekraïne en Slowakije vinden dat alleen de staat (in plaats van private partijen) toestemming kan geven voor een netwerkzoeking op haar grondgebied. Zie Koops 2012a, p. 43 (met verwijzingen).

Belangrijker echter dan de beperking tot verdragspartijen is dat in situaties waarin de verdachte niet meewerkt, en bij cloudaanbieders die normaliter alleen op basis van een gerechtelijk bevel maar niet van een verzoek van opsporingsautoriteiten meewerken,[129] art. 32 Cybercrime-Verdrag geen soelaas biedt. Een netwerkzoeking naar in de cloud opgeslagen gegevens zal daarom vaak op de grenzen van de territoriaal gebonden bevoegdheid stuiten.

De Raad van Europa is zich bewust van de grote beperkingen veroorzaakt door de territoriale benadering van toegang tot data, mede door de opkomst van de cloud. Op de Octopus-conferentie van juni 2012 werd vastgesteld:

> Transborder law enforcement access to data and electronic evidence is a major issue, in particular in the context of cloud computing. Many countries permit transborder access to data either directly or via service providers under limited circumstances. Common rules and safeguards are needed. The workshop will feed into the efforts of the Cybercrime Convention Committee that is preparing a proposal for an instrument to address this challenge.[130]

Het zal echter nog de nodige tijd duren voordat een dergelijk instrument voor grensoverschrijdende toegang tot data aangenomen en van kracht zal worden. Vanwege de gevoeligheid van het onderwerp en verschillende visies van landen, zal er een wisselwerking bestaan tussen de slagkracht en de breedte van het beoogde instrument: naarmate er scherpere voorstellen liggen om grensoverschrijdende toegang tot data toe te staan, valt te verwachten dat minder landen zullen tekenen, terwijl een instrument dat breed gedragen wordt concessies zal moeten doen aan de mate waarin grensoverschrijdende doorzoekingen worden toegestaan.

Intermezzo. De Belgische grensoverschrijdende netwerkzoeking

Een van de weinige landen die wel een verdergaande grenschoverschrijdende netwerkzoeking kennen, is België. Artikel 88ter BSv maakt het mogelijk voor de onderzoeksrechter, vergelijkbaar met de rechter-commissaris in Nederland, om een zoeking in een informaticasysteem of een deel daarvan uit te breiden ‘naar een informaticasysteem of een deel daarvan dat zich op een andere plaats bevindt dan daar waar de zoeking plaatsvindt’ (art. 88ter §1, 1e lid BSv). Belangrijk is het tweede lid:

> Wanneer blijkt dat deze gegevens zich niet op het grondgebied van het Rijk bevinden, worden ze enkel gekopieerd. In dat geval deelt de onderzoeksrechter dit, via het openbaar ministerie, onverwijld mee aan het ministerie van Justitie, dat de bevoegde overheid van de betrokken Staat hiervan op de hoogte brengt, indien deze redelijkerwijze kan worden bepaald. (art. 88ter §3 lid 2 BSv)

Artikel 88ter BSv laat dus toe om zonder formeel rechtshulpverzoek een netwerkzoeking te doen in een buitenlandse computer. De memorie van toelichting motiveert dit als volgt:

> De bevoegdheden waarover de overheid beschikt om onderzoekshandelingen te stellen in het kader van een strafprocedure kunnen immers in principe enkel worden uitgeoefend op het nationale territorium waarover die overheid gezag heeft. Dit houdt ongetwijfeld verband met het feit dat het strafrecht zeer sterk verbonden is met de notie van staatssoevereiniteit. Het hangt eveneens samen met het beginsel van de goede trouw in de interstatelijke betrekkingen. Tegelijk komt de klassieke invulling van het concept soevereiniteit in deze context onder druk te staan, enerzijds omwille van de toenemende internationalisering van de financieel-economische criminaliteit, en anderzijds door de enorme vlucht die de informatietechnologie heeft genomen. Men is er zich meer en meer van bewust dat de traditionele vormen van internationale gerechtelijke samenwerking, die juist in het leven werden geroepen om aan de beperkingen van de nationale opsporings- en onderzoeksbevoegdheden te remediëren, niet enkel moeten worden gemoderniseerd, maar op sommige punten moeten worden geïnnoveerd. (…)
>
> Een aantal punten zullen onmiskenbaar via internationale instrumenten of overleg met andere staten moeten worden behandeld. Dit neemt evenwel niet weg dat de problemen vandaag bestaan, en dat derhalve een juridisch houvast moet worden geboden aan de mensen die op het terrein naar aanleiding van een zoeking in een computersysteem met de problematiek van op internationale schaal verbonden informaticasystemen worden geconfronteerd. (…)
>
> Daarom wordt in dit ontwerp in deze materie een voorzichtige, maar pragmatische positie ingenomen. Het is duidelijk dat de grensoverschrijdende zoeking niet als regel kan worden gesteld. (…) Wanneer derhalve voldoende tijd en kennis voorhanden is, moet de weg van de klassieke

[129] Hetgeen bij grote cloudaanbieders het geval is, aldus Interview Openbaar Ministerie, Interview KLPD.
[130] Octopus 2012.

> internationale rogatoire commissies worden gevolgd, bij ontstentenis van juridisch adequate alternatieven op dit ogenblik sluiten. (….)
>
> Het belang van de waarheidsvinding in gevallen van ernstige criminaliteit kan een dergelijke grensoverschrijdende zoeking uitzonderlijk rechtvaardigen. In dergelijke gevallen is het evenwel onontbeerlijk om de betrokken andere staat te informeren teneinde deze toe te laten na te gaan of al dan niet een inbreuk op de rechtsorde werd gemaakt. Internationaalrechtelijk kan hierbij onder andere het element reciprociteit een rol spelen.[131]

De rechtbank van eerste aanleg te Brussel[132] vond de toepassing van deze bepaling terecht in een geval waarin bij een huiszoeking een document in beslag was met genomen met het wachtwoord tot twee Hotmailaccounts van verdachte, die weigerde zelf zijn wachtwoord te geven. Vervolgens doorzochten de verbalisanten de Hotmailaccounts. De rechtbank oordeelde dat in een dergelijk geval zonder bijkomende formaliteit de huiszoeking mag worden uitgebreid tot informaticasystemen die zich bevinden op een andere plaats dan de plaats waarvoor het huiszoekingsbevel is afgeleverd, mits de voorwaarden van art. 88ter, § 1 in fine en § 2 BSv worden nageleefd. Deze interpretatie van een 'verlengde huiszoeking' is overigens in de literatuur bekritiseerd omdat de wetgever bij art. 88ter §3 een sui generis-bevoegdheid zou hebben beoogd waarvoor de onderzoeksrechter vooraf toestemming voor zou moeten verlenen.[133]

Het Hof van beroep te Brussel merkte – in een obiter dictum – nog op dat wanneer België de buitenlandse staat in strijd met art. 88ter §3 lid 2 niet notificeert, dit niet tot bewijsuitsluiting hoeft te leiden aangezien het geen vormverzuim is dat gevolgen behoeft te hebben voor de rechten van de verdachte.[134]

Het model van de Belgische netwerkzoeking kent voor zover ons bekend (nog) geen navolging bij andere landen. De extraterritoriale bevoegdheid heeft evenmin tot substantiële protesten geleid van andere landen die hun soevereiniteit geschonden achten, maar wij weten niet of dat ligt aan onbekendheid, een laagfrequente toepassing of (stilzwijgende) instemming met dit model. Het biedt in elk geval een interessante denkrichting voor de aanpassing van art. 32 CCV.

5.1.2. Gegevens verkrijgen via de cloudaanbieder

In plaats van zelf gegevens veiligstellen via een netwerkzoeking, kan de opsporingsdienst ook gegevens opvragen bij een cloudaanbieder. Er bestaan de nodige bevoegdheden om gegevens te vorderen, afhankelijk van het type gegevens en het type aanbieder. Als een cloudaanbieder een aanbieder van een communicatiedienst is (dat is niet altijd duidelijk, zie par. 5.2.1), is het regime voor het vorderen van telecommunicatiegerelateerde gegevens van toepassing. Identificerende gegevens over gebruikers van communicatiediensten kunnen worden gevorderd op basis van art. 126na, 126ua of 126zi Sv, verkeersgegevens op basis van art. 126n, 126u of 126zh Sv.[135] De inhoud van communicatie en andere gegevens kunnen bij communicatieaanbieders worden gevorderd op basis van art. 126ng, 126ug of 126zo Sv. Voor cloudaanbieders die geen communicatieaanbieder zijn, geldt het algemene regime van vorderen van gegevens, dat onderscheid maakt tussen identificerende (art. 126nc/uc/zk Sv), gevoelige (art. 126nf/uf/zn Sv) en overige gegevens (art. 126nd/ud/zl Sv). De opsporingsdienst kan ook vorderen dat toekomstige gegevens worden doorgegeven, in dringende gevallen direct na de verwerking (in 'reële tijd') (art. 126ne/ue/zm Sv).

Ook bij deze bevoegdheden geldt echter een territoriale beperking: zij kunnen in principe alleen worden gebruikt tegenover cloudaanbieders die in Nederland gevestigd zijn. Dwangmiddelen mogen immers alleen worden ingezet binnen de eigen rechtsmacht van een staat. De meeste cloudaanbieders zijn echter buitenlandse aanbieders, veelal Amerikaans, zonder vestiging in Nederland. Gegevens moeten dan worden gevorderd via een rechtshulpverzoek. In de praktijk vordert de Nederlandse justitie gegevens bij cloudaanbieders ook altijd via een rechtshulpverzoek, hetgeen zich tot nu toe beperkt tot webmail; met het

[131] Wetsontwerp inzake informaticacriminaliteit, *Parl. St.* Kamer 1999-2000, nr. 2-392, 23-25.
[132] Corr. Brussel 10 januari 2008, *T.Strafr.* 2008, 149.
[133] Keustermans & De Maere 2010, p. 568.
[134] Hof van beroep te Brussel 26 juni 2008. Zie verder ook De Hert & Van Leeuw 2011, p. 922-926.
[135] Het Wetboek maakt bij bijzondere opsporingsbevoegdheden onderscheid tussen drie typen onderzoek: opsporing naar gepleegde strafbare feiten (art. 126 e.v.), onderzoek naar het beramen of plegen van georganiseerde misdaad (art. 126 o e.v.) en onderzoek naar terroristische misdrijven (art. 126za e.v.).

opvragen van documenten die in de cloud staan opgeslagen bestaat nog geen ervaring.[136] Bij aanbieders in de VS en Europa werken rechtshulpverzoeken vanuit Nederland meestal goed.[137] Vanuit andere landen is dat niet altijd het geval; in Letland bijvoorbeeld zijn een aantal rechtshulpverzoeken aan een ander land onbeantwoord gebleven – wellicht omdat het een klein land is en daarom rechtshulpverzoeken geen prioriteit krijgen.[138] In een Duitse zaak werd een rechter van het kastje naar de muur gestuurd toen hij, met kennelijke instemming van de verdachte, gegevens over verdachtes Facebookprofiel vorderde: Facebook Duitsland verwees hem door naar Facebook Ierland (waar de hoofdvestiging van Facebook in Europa is), die vervolgens niet reageerde op een rechtstreekse vordering, terwijl een daaropvolgend rechtshulpverzoek aan Ierland afketste omdat de data in de VS opgeslagen lagen en daarom het rechtshulpverzoek aan de VS zou moeten worden gericht.[139]

Het opvragen van gegevens bij cloudaanbieders is echter niet altijd vanzelfsprekend. De eerste vraag die politie en openbaar ministerie stellen als zij gegevens willen vorderen is: 'Bij wie moet je zijn?'[140] Bij een opsporingsonderzoek kan wel bekend zijn of vermoed worden dat een verdachte een clouddienst gebruikt voor communicatie of opslag van documenten, maar de identiteit van de aanbieder is lang niet altijd bekend (behoudens gevallen waarin een verdachte een herkenbare webdienst gebruikt, zoals bij huppeldepup@hotmail.com). Soms vergt het een doorzoeking bij de verdachte op het moment dat hij zijn computer gebruikt, waarbij voorkomen moet worden dat de verdachte de computer snel kan afsluiten, zodat op de openstaande verbindingen nagegaan kan worden welke clouddiensten in gebruik zijn; maar ook dat levert alleen de (min of meer toevallig) openstaande verbindingen op.

Ook als de aanbieder bekend is, hoeft deze niet altijd mee te werken. Er zijn bijvoorbeeld aanbieders actief die bewust zoveel mogelijk doen om gegevens uit handen van justitie te houden (zogeheten *bulletproof providers* oftewel 'kogelvrije aanbieders'); deze werken per definitie niet mee. Daarnaast is het voor het onderzoeksbelang soms beter om niet afhankelijk te zijn van medewerking van aanbieders, bijvoorbeeld als onbekend is hoe zij zullen omgaan met verzoeken. In Nederland heeft justitie er bij een recent rechtshulpverzoek uit de VS bijvoorbeeld voor gekozen om gegevens die in een 'mini-cloud' in Nederland waren opgeslagen, veilig te stellen door inbeslagneming van alle systemen in plaats van contact op te nemen met de aanbieder van de clouddienst.[141] Een aandachtspunt is ook of bij een vordering tot uitlevering van gegevens geheimhouding kan worden opgelegd; in Nederland is degene die een vordering krijgt, tot geheimhouding verplicht (art. 126bb lid 5 Sv), maar het is niet duidelijk of dat in het buitenland ook zo geregeld is.[142] Het rechtshulpverdrag tussen de EU en de VS bevat bijvoorbeeld alleen een inspanningsverplichting voor de aangezochte staat om een rechtshulpverzoek geheim te houden.[143]

Ook kunnen aanbieders gevestigd zijn in landen waarmee Nederland geen rechtshulpverdrag heeft of waarin de samenwerking moeilijk loopt. Momenteel levert dat nog geen problemen op (aangezien de meeste cloudaanbieders zijn gevestigd in de VS of Europa), maar wanneer

[136] Interview KLPD. Volgens het OM werkt Google wel mee bij vorderingen voor webmail, maar niet voor documenten uit Google Docs omdat die dienst volgens Google zodanig is ingericht dat zij niet bij de data kunnen (interview Openbaar Ministerie).
[137] Interview KLPD.
[138] Uldis Kinis, reactie op enquête.
[139] Gerrit Hornung, reactie op enquête, verwijzend naar 'Reutlinger Richter lädt Facebook-Lobbyistin als Zeugin. Update', 15 maart 2012, http://www.heise.de/-1472668.html.
[140] Interviews Openbaar Ministerie en KLPD.
[141] Interview KLPD.
[142] Het KLPD heeft wel eens meegemaakt dat een buitenlandse aanbieder als eerste zijn klant informeert over de vordering, hetgeen vanzelfsprekend het onderzoeksbelang ondergraaft. Interview KLPD. Vgl. Microsoft's bepaling dat zij in reactie op een justitiële vordering 'use commercially reasonable efforts to notify the enterprise customer in advance of any production unless legally prohibited' (geciteerd in Walden 2011, p. 9). Vgl. ook de aanbeveling voor cloudcontracten van de Article 29 Working Party (2012), p. 13-14: 'Notification of cloud client about any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.'
[143] Art. 10 Overeenkomst betreffende wederzijdse rechtshulp in strafzaken tussen de Europese Unie en de Verenigde Staten van Amerika, *PubEU* L181/34, 19.7.2003.

opkomende landen als China of India grootschalig internationale clouddiensten gaan aanbieden, zal dit een knelpunt worden.[144]

Aan de andere kant bestaat er wel enige ruimte om buiten de officiële weg van een rechtshulpverzoek gegevens op te vragen bij cloudaanbieders. Zoals hierboven geconstateerd werken sommige aanbieders, zoals Google, alleen mee op basis van een rechterlijk bevel uit de VS, maar andere aanbieders lijken ook te willen reageren op rechtstreekse verzoeken van buitenlandse opsporingsdiensten. Diverse aanbieders behouden zich in elk geval in hun Algemene Voorwaarden het recht voor om gegevens uit te leveren aan erkende buitenlandse opsporingsdiensten of in gevallen waarin er een duidelijk dringend publiek belang is (bijvoorbeeld levensgevaar).[145] Het rechtstreeks benaderen van buitenlandse aanbieders wordt echter ontmoedigd in de richtlijnen van de Raad van Europa over samenwerking tussen opsporingsdiensten en Internetaanbieders: 'For requests addressed to non-domestic Internet service providers, domestic law enforcement authorities should be encouraged not to direct requests directly to non-domestic Internet service providers but make use of procedures as described in international treaties (...).'[146] Evenzo dringt de Artikel 29 Werkgroep erop aan om in de nieuwe Dataprotectieverordening een bepaling op te nemen over 'the obligatory use of Mutual Legal Assistance Treaties (MLATs) in case of disclosures not authorised by Union or Member States law' om te voorkomen dat cloudaanbieders rechtstreeks gegevens verstrekken aan niet-EU-opsporingsdiensten zonder specifieke verdragsbasis of toestemming van een (Europese) toezichthouder.[147]

In welke mate cloudaanbieders mogen of kunnen reageren op rechtstreekse verzoeken of bevelen van buitenlandse opsporingsdiensten, zal zich in de praktijk verder moeten uitkristalliseren.

5.1.3. Gegevens onderscheppen

Gegevens onderscheppen (tussen klant en cloud in) komt neer op het aftappen van communicatie, geregeld in art. 126m/126t/126zg Sv. Aftappen is vooral relevant in twee situaties. Ten eerste in het geval van een cloudopslagdienst, wanneer de dienst zodanig is ingericht dat de gegevens versleuteld worden opgeslagen zonder dat de cloudaanbieder zelf in staat is te ontsleutelen.[148] Dat gebeurt (nog) niet veel, maar het is een interessant bedrijfsconcept omdat het een robuuste vorm van informatiebeveiliging biedt, die onder andere relevant kan zijn voor Europese bedrijven die hun data in de cloud willen opslaan zonder dat deze door bijvoorbeeld Amerikaanse overheidsdiensten op basis van de USA Patriot Act bij aanbieders kunnen worden gevorderd. De Nederlandse justitie kan de gegevens dan achterhalen door ze te onderscheppen voordat ze versleuteld in de cloud worden opgeslagen, bijvoorbeeld via een internettap bij de toegangsaanbieder van de verdachte in Nederland. (Een alternatief is het tappen bij de cloudaanbieder, maar dat is minder realistisch omdat die veelal in het buitenland zit en dan alleen via een rechtshulpverzoek gedwongen kan worden mee te werken, voor zover de wetgeving van het andere land dat toelaat. Ook druist het aftappen dan in tegen het bedrijfsconcept van versleutelde opslag zonder toegangsmogelijkheid door de aanbieder, zodat deze vermoedelijk niet snel zal meewerken aan een tap: zodra bekend wordt dat de aanbieder tapt ten behoeve van een (binnen- of buitenlandse) opsporingsdienst, wordt de basis onder dit bedrijfsconcept wankel. Bij dit bedrijfsconcept van opslagdiensten zal de dienst daarom vermoedelijk zodanig worden ingericht dat de aanbieder technisch niet in staat zal zijn om gegevensverkeer van klanten af te tappen.)

---

[144] Interview Openbaar Ministerie.

[145] Walden 2011, p. 9. Zie bijvoorbeeld de bepaling in Apple's *Privacy Policy* (versie 12 mei 2012): 'It may be necessary – by law, legal process, litigation, and/or *requests* from public and governmental authorities within *or outside your country of residence* – for Apple to disclose your personal information. We may also disclose information about you if we determine that for purposes of national security, law enforcement, or other issues of public importance, disclosure is necessary or appropriate' (cursivering toegevoegd). http://www.apple.com/privacy/ (geraadpleegd 3 juli 2012).

[146] Council of Europe 2008, guideline 36.

[147] Article 29 Working Party (2012), p. 23.

[148] 'Methods rendering data unreadable to CC [cloud computing] providers at any given time should be further explored.' International Working Group on Data Protection in Telecommunications 2012, p. 4. Cf. http://www.sealedcloud.de/grundgedanke.php (geraadpleegd 3 juli 2012).

De tweede situatie is die waarin de verdachte een cloudcommunicatiedienst gebruikt, zoals webmail. De communicatie via deze dienst kan dan wederom onderschept worden via een tap bij de toegangsaanbieder van de verdachte. Een tap bij de (buitenlandse) webmailaanbieder zal veelal niet eenvoudig zijn. Buitenlandse aanbieders die diensten in Nederland aanbieden vallen vermoedelijk niet direct onder de medewerkings- en aftapbaarheidsverplichtingen van hoofdstuk 13 Telecommunicatiewet, als zij geen vestiging in Nederland hebben;[149] in elk geval zijn de meeste aanbieders niet geregistreerd als openbare telecomaanbieder in Nederland.[150] Bovendien kan een tap alleen uitgevoerd worden via een rechtshulpverzoek aan het land waarin de server staat (dan wel het land waar de aanbieder is gevestigd), wat niet alleen vertraging oplevert maar ook complicaties door verschillen in rechtscultuur: in de VS moet zoveel mogelijk gefilterd worden om het tapmateriaal te beperken, terwijl in Nederland juist alles moet worden geleverd vanwege de volledigheid van het mogelijke (ook ontlastende) bewijsmateriaal.[151]

Zowel bij cloudopslag als bij cloudcommunicatie zal het aftappen dus vooral moeten gebeuren via een Internettap bij de (Nederlandse) toegangsaanbieder van de verdachte. In die zin is cloud computing niet een bijzondere factor (behalve voor zover cloudgebruik gepaard gaat met een toename van versleuteling, zie par. 5.2.3). Met het toenemend gebruik van (ook mobiele) Internettoepassingen, neemt het belang van de Internettap snel toe, en het maakt niet veel uit of het IP-verkeer een clouddienst of een andersoortige webdienst betreft. Toepassing van de Internettap zal naar verwachting flink toenemen in de nabije toekomst (onder andere door het groeiend aantal smartphones), maar kent wel de nodige knelpunten, zoals gebrek aan ervaring, benodigde capaciteit om grote hoeveelheden data uit te werken en de kennis om daarin effectief te zoeken, naast juridische vragen of knelpunten rond verbalisering, geheimhoudergegevens en selectie vooraf op basis van Deep Packet Inspection.[152]

In één opzicht maakt de cloud wel verschil: alle documenten die de verdachte niet (alleen) op zijn harde schijf maar (ook) in de cloud opslaat, komen langs de IP-tap. De opkomst van cloud computing biedt dan ook meer kansen om informatie te verzamelen via een tap in plaats van via een doorzoeking bij de verdachte (zie ook par. 5.3). Om die kansen te benutten, zal de overheid wel de genoemde juridische vragen moeten beantwoorden en de genoemde knelpunten moeten aanpakken rond de Internettap.

5.2. Juridische vragen en uitdagingen

Bij het verkrijgen van gegevens uit de cloud is het grensoverschrijdende aspect een van de belangrijkste aandachtspunten, zo blijkt uit het voorgaande. Daarnaast bestaan er echter ook binnen de Nederlandse context zelf enkele vragen en uitdagingen voor recht en praktijk, die we in deze paragraaf behandelen.

5.2.1. Kwalificatie als (tele)communicatieaanbieder

Een eerste juridische vraag is wanneer een cloudaanbieder als aanbieder van een communicatiedienst (kortweg: communicatieaanbieder) kwalificeert, wat relevant is voor de vraag welk juridisch regime van toepassing is (zie par. 5.1.2). Een aanbieder van een communicatiedienst is een

> natuurlijke persoon of rechtspersoon die in de uitoefening van een beroep of bedrijf aan de gebruikers van zijn dienst de mogelijkheid biedt te communiceren met behulp van een geautomatiseerd werk, of gegevens verwerkt of opslaat ten behoeve van een zodanige dienst of de gebruikers van die dienst (art. 126la Sv).

Duidelijk is dat een SaaS-aanbieder die specifieke communicatiesoftware aanbiedt, zoals webmail, hieronder valt. Bij andere softwarediensten ligt het minder voor de hand: een opslagdienst of een dienst die Office-achtige applicaties aanbiedt (zoals Google Docs) is in beginsel niet bedoeld voor communicatie maar voor gegevensopslag of gegevensverwerking. Een grammaticale lezing van art. 126la Sv suggereert dat diensten die alleen opslag of verwerkingscapaciteit aanbieden, los van een communicatiefunctionaliteit, niet onder de definitie

[149] Oerlemans 2012, p. 27, verwijzend naar *Kamerstukken II* 2007/08, 31 145, nr. 9, p. 6; zie ook Koops e.a. 2005, p. 38.
[150] Interview Openbaar Ministerie.
[151] Koops e.a. 2005, p. 38.
[152] Zie hierover uitgebreid Odinot e.a. 2012, p. 155-168.

vallen; het tweede gedeelte spreekt immers alleen van verwerking of opslag ten behoeve van een *zodanige* dienst (i.e., een dienst om te communiceren) en de gebruikers van *die* (i.e., communicatie)dienst. De wetsgeschiedenis kan echter een ruimere interpretatie opleveren. De toelichting bij art. 126la Sv geeft geen specificering van de tekst maar zegt dat nauw is aangesloten bij het Cybercrime-verdrag,[153] dat – in de Nederlandse vertaling – vrijwel dezelfde formulering hanteert.[154] De toelichting bij het Cybercrime-verdrag is wat dubbelzinnig:

> Under (ii) of the definition, it is made clear that the term "service provider" also extends to those entities that store or otherwise process data on behalf of the persons mentioned under (i). Further, the term includes those entities that store or otherwise process data on behalf of the users of the services of those mentioned under (i). For example, under this definition, a service provider includes both services that provide hosting and caching services as well as services that provide a connection to a network. However, a mere provider of content (such as a person who contracts with a web hosting company to host his web site) is not intended to be covered by this definition if such content provider does not also offer communication or related data processing services.[155]

Enerzijds staat hier, in de laatste zin, dat opslag- en verwerkingsdiensten alleen onder de definitie vallen als zij gerelateerd zijn aan communicatiefunctionaliteit. Anderzijds suggereert het voorbeeld van hosting- en cachingaanbieders dat het om een ruimer begrip gaat; dergelijke aanbieders bieden immers niet altijd ook functionaliteiten aan voor klanten om te communiceren. Men zou kunnen zeggen dat een cloudopslagdienst vergelijkbaar is met een hostingdienst in de zin dat beide opslagcapaciteit aanbieden.

Daar komt bij dat een strikte scheiding niet altijd valt aan te brengen; veel cloudopslagdiensten bieden tegelijk ook de mogelijkheid om bestanden te delen, zoals DropBox, en de clouddienst fungeert dan feitelijk als medium om bestanden tussen gebruikers heen en weer te sturen. Functioneel maakt het geen verschil of gebruiker A een document naar gebruiker B verzendt via de webmail van gebruiker B of via DropBox; in beide gevallen ligt het document opgeslagen bij de aanbieder en kan gebruiker B het document 'ontvangen' op het moment dat zij zelf kiest. Teleologisch redenerend ligt het dan voor de hand dat cloudopslagdiensten die (mede) als functionaliteit hebben om bestanden te delen tussen gebruikers, ook onder de definitie van communicatieaanbieder te laten vallen.

Vervolgens zijn er nog de PaaS- en IaaS-aanbieders. Deze bieden een platform (bijvoorbeeld Amazon AWS) of een complete infrastructuur waarop gebruikers zelf applicaties en diensten kunnen bouwen en gebruiken. Daarbij kunnen ook communicatiefunctionaliteiten zitten. De cloudaanbieder biedt dan een verwerkingsdienst die gerelateerd is aan een communicatiedienst. De vraag is of de cloudaanbieder in dat geval – indirect – ook als communicatieaanbieder kwalificeert. Enerzijds kan men zeggen dat dit type aanbieders verder weg staan van het type dienstverlening dat de makers van het Cybercrime-Verdrag en de Nederlandse wetgeving in 2006 voor ogen stond, en dat het gaat om een zeer indirecte manier van communicatie faciliteren. Anderzijds vervullen deze aanbieders een enigszins vergelijkbare rol met hostingaanbieders in de zin dat zij intermediair zijn voor eindgebruikers van het Internet, en dat bevoegdheden om gebruikers- en verkeersgegevens te vorderen potentieel even relevant zijn bij PaaS- en IaaS-aanbieders als bij toegangs- of SaaS-aanbieders.[156] Op dit vlak zal de toekomstige rechtsontwikkeling moeten uitwijzen welke zienswijze het meest plausibel is.

Al met al kan worden geconcludeerd dat webmailaanbieders duidelijk als communicatieaanbieder kwalificeren, maar dat onzekerheid bestaat over andere typen cloudaanbieders. In een ruime interpretatie van art. 126la Sv zullen ook opslag- en verwerkingsdiensten via de cloud onder de definitie vallen. Bij het aanbieden van platforms en infrastructuur in de cloud valt het moeilijk te zeggen; wellicht kan het beste per geval bekeken worden welk gebruik van deze dienstverlening wordt gemaakt en hoe dicht dat tegen communicatiedienstverlening aan zit.

---

[153] *Kamerstukken II* 2004/05, 26 671, nr. 7, p. 41.
[154] Zie art. 1 onder c van het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, Boedapest, 23 november 2001, Trb. 2004, 290.
[155] Convention on Cybercrime, CETS 185, Explanatory Report §27.
[156] Walden 2011, p. 16, stelt dat alle typen clouddienstaanbieders (evenals aanbieders van infrastructuur aan cloudaanbieders) onder de ruime definitie van het Verdrag ('"service provider" defined in the broadest possible terms') vallen, maar geeft daarvoor geen onderbouwing.

Een vervolgvraag is in welke mate cloudaanbieders openbare telecommunicatieaanbieders zijn, wat van belang is of zij vallen onder de bewaarplicht verkeersgegevens.[157] Dit hangt samen met de beheersvorm van de clouddienst (zie par. 2.1): een private cloud zal geen openbare dienst zijn, een publieke cloud wel. Of een hybride cloud openbaar is, zal waarschijnlijk afhangen van de omvang van het publieke deel. 'Openbaarheid' van telecomaanbieders is verder geen onproblematisch begrip, maar dat is niet specifiek voor clouddiensten; wij verwijzen daarom naar de literatuur hierover.[158]

Of het telecommunicatiediensten zijn als bedoeld in de Telecommunicatiewet, lijkt samen te hangen met de vraag of het communicatiediensten zijn als bedoeld in art. 126la Sv, maar deze begrippen lopen niet parallel. Voor de Telecommunicatiewet is niet de toelichting uit het Cybercrime-Verdrag relevant, maar de EU-regelgeving in de telecommunicatiesector, waar het begrip 'elektronische communicatiedienst' leidend is. Volgens Walden is de scheidslijn tussen 'elektronische communicatiedienst' en 'dienst van de informatiemaatschappij' vaag wanneer het wordt toegepast op clouddiensten; het gaat erom of de clouddienst 'geheel of hoofdzakelijk bestaat in het overbrengen van signalen via elektronische communicatienetwerken' (art. 1.1 onder f Tw), wat bij webmail vermoedelijk wel het geval is maar wat minder makkelijk is vast te stellen bij andere typen clouddiensten.[159] Volgens Hendriks e.a. vallen clouddiensten die primair betrekking hebben op opslag of bewerking van gegevens niet onder de definitie van telecommunicatiedienst.[160] Verder is van belang dat aanbieders die niet in Nederland gevestigd zijn maar wel diensten in Nederland aanbieden, niet onder de Telecommunicatiewet lijken te vallen[161] en dus niet bewaarplichtig zijn. Dat laat overigens onverlet dat zij in eigen land een bewaarplicht kunnen hebben en ook vanuit hun bedrijfsbelang vaak gegevens gedurende zekere periode bewaren.

5.2.2. Onderscheid opslag – transit

Een meer algemene juridische vraag die in het verlengde van deze discussie ligt, is of het onderscheid tussen opgeslagen data en data in transit goed toepasbaar is in een cloudomgeving. De opsporingswetgeving is gebaseerd op een fundamenteel onderscheid tussen data die ergens liggen opgeslagen (en die te verkrijgen zijn via doorzoeking of gegevensvordering) en data die onderweg zijn (en die te verkrijgen zijn via aftappen). Met de komst van email en voicemail werd dit onderscheid al enigszins onder druk gezet, aangezien daarbij het bericht tijdens de weg van zender naar ontvanger voor langere tijd opgeslagen kan liggen bij de aanbieder: het is dus zowel onderweg als (tijdelijk) opgeslagen. Deze informatie kan feitelijk niet worden getapt, maar wel worden gevorderd bij de aanbieder. De wetgever heeft daartoe een aparte bepaling ingevoerd om gegevens te vorderen 'die zijn opgeslagen in het geautomatiseerde werk van de aanbieder en niet voor deze bestemd of van deze afkomstig zijn', waarmee de inhoud van communicatie wordt bedoeld (art. 126ng/ug/zo Sv). Op zich is deze benadering goed toepasbaar op clouddiensten: de aanbieder kan hetzij bevolen worden mee te werken aan een tap (dat wil zeggen in- en uitkomend verkeer van de cloud in reële tijd door te leveren) dan wel om gegevens te leveren die bij hem zijn opgeslagen.

Daarbij doet zich wel de situatie voor dat als een opslagaanbieder *niet* kwalificeert als communicatieaanbieder (zie hierboven), bij hem opgeslagen gegevens moeten worden gevorderd via het algemene regime (zie par. 5.1.2) in plaats van de speciale bepaling van126ng Sv, terwijl de voorwaarden voor de toepassing van deze bevoegdheden sterk verschillen. Als een cloudopslagdienst niet valt onder de definitie van art. 126la Sv, kan de officier van justitie bij verdenking van voorlopigehechtenismisdrijven documenten vorderen die bij de dienstaanbieder zijn opgeslagen (aldus art. 126nd Sv); als de dienst echter wel onder art. 126la Sv valt, kan dit alleen met machtiging van de rechter-commissaris, bij voorlopigehechtenismisdrijven die een ernstige inbreuk op de rechtsorde opleveren, en voor zover de documenten een klaarblijkelijke relatie met de verdachte of het strafbare feit hebben (aldus art. 126ng lid 2 Sv). Vanuit het

[157] Art. 13.2a Tw, zoals gewijzigd bij Wet van 18 juli 2009, *Stb.* 2009, 333 en Wet van 6 juli 2011, Stb. 2011, 350.
[158] Dries, Gijrath & Knol 2003; Koops e.a. 2005, p. 33-36.
[159] 'The boundary is particularly blurred given the potential variety of approaches that could be adopted for interpreting the phrase "mainly in the conveyance of signals"' [een onderdeel van de definitie van elektronische communicatiedienst]. Walden 2011, p. 17.
[160] Hendriks e.a. 2012, p. 55.
[161] *Kamerstukken II* 2007/08, 31 145, nr. 9, p. 6 ('e-maildiensten, zoals vermeld in de vraagstelling [waaronder e-maildiensten als Hotmail en Yahoo], vallen niet onder de werking van Telecommunicatiewet').

oogpunt van rechtsbescherming en rechtszekerheid zou het merkwaardig zijn als documenten opgeslagen bij een cloudopslagaanbieder onder verschillende regimes vallen afhankelijk of de aanbieder naast de opslagfunctionaliteit al dan niet ook een communicatiefunctionaliteit biedt. Dit onderstreept het belang voor de wetgever of rechtspaak om helderheid te scheppen in de hiervoor behandelde kwalificatiekwestie.

Het gaat echter om een bredere vraag die hieruit voortvloeit. Art. 126ng lid 2 Sv is een specialis, die ingevoerd is omdat bij 'communicatie onderweg' de regimes van opgeslagen gegevens en gegevens-in-transit elkaar raken, waarbij vanwege het (tele)communicatiegeheim van art. 13 Gw gekozen is voor een zwaar beschermingsregime voor communicatie die bij de communicatieaanbieder ligt opgeslagen. Dit roept de vraag op of het terecht is om een onderscheid in rechtsbescherming te maken tussen communicatie en niet-communicatieve documenten die bij een cloudaanbieder liggen opgeslagen. Dat raakt aan de complexe vraag van de ratio van het (tele)communicatiegeheim, waarover de meningen uiteenlopen. Versimpeld gezegd vindt de ene stroming dat de ratio is gelegen in de noodzaak 'communicatie' als zelfstandige categorie te beschermen, terwijl de andere stroming de ratio ziet in de bescherming van het communicatiekanaal waarbij een derde partij – de aanbieder – beschikkingsmacht heeft over de communicatie.[162] Binnen het bestek van dit onderzoek kunnen we op deze vraag niet diep ingaan, maar wat ons betreft valt er wel het nodige te zeggen voor een kanaalbescherming. (Om één voorbeeld te geven: wij zien niet in waarom een emailbericht verstuurd naar een Gmail-adres intrinsiek meer bescherming verdient dan een dagboek dat in Google Docs wordt bijgehouden, als er gegevens bij Google worden gevorderd.) Wanneer men uitgaat van een kanaalbescherming, rijst de vraag of een cloudopslagdienst – waarbij feitelijk een document langdurig wordt opgeslagen onder beschikkingsmacht van een dienstaanbieder – ook aanspraak zou moeten kunnen maken op deze kanaalbescherming. Dat is een vraag die de grondwetgever bij de herziening van art. 13 Gw zal moeten beantwoorden.[163] Duidelijk is in elk geval dat de vraag of opslag-op-afstand in cloud onder het (tele)communicatiegeheim valt, ingrijpende consequenties heeft voor de strafvorderlijke regeling. Het zal lang duren voordat de grondwetgever zich definitief uitgesproken zal hebben over art. 13 Gw; in de tussentijd is het wenselijk dat de strafwetgever een uitspraak doet over de vraag welk wettelijk regime van toepassing is of zou moeten zijn op cloudopslagdiensten.

Daarbij zou ook nog de bredere vraag kunnen worden betrokken of de onderscheiden tussen opslag en transit en tussen communicatie en non-communicatie nog echt relevantie hebben in een informatie- en communicatielandschap waarin de cloud een belangrijke rol speelt. Bij diensten als DropBox vallen opslag van documenten en het uitwisselen van documenten (communicatie) feitelijk samen. Als gegevens in de cloud, op basis van algoritmes die de meest efficiënte opslag berekenen bij een continu veranderend vraag en aanbod, automatisch worden verplaatst van de ene server naar een andere, zijn ze dan onderweg of in opslag – en zou die vraag relevant moeten zijn voor het juridische regime van vorderen?[164] Gaat het bij dit alles niet eerder om de beschikkingsmacht van een dienstaanbieder over gegevens dan over de precieze vorm of status van die gegevens?

5.2.3. Toenemend gebruik van versleuteling

Versleuteling van communicatie en gegevensopslag neemt toe. Deels zit deze toename in Internettelefoniediensten (zoals Skype) die alle gesprekken versleutelen die via het IP-protocol worden getransporteerd. Dergelijke diensten die niet onder de Telecommunicatiewet vallen (omdat ze in het buitenland gevestigd zijn of omdat ze geen telecommunicatiedienst (maar software) aanbieden), kunnen niet worden gedwongen om klare tekst aan justitie te leveren.[165] Voor een ander deel zit de toename in encryptiegebruik door misdadigers zelf, waarbij – in tegenstelling tot enkele jaren geleden – een substantiële gebruikersgroep voldoende technisch onderlegd is om sterke versleuteling te gebruiken op een manier dat deze niet valt te kraken.[166] Dit is niet specifiek voor de cloud, maar levert wel een opsporingsprobleem op wanneer

[162] Zie bijvoorbeeld de verdeelde meningen binnen de Commissie-Thomassen, *Rapport Staatscommissie Grondwet* (2010).
[163] Zie *Kamerstukken II* 2011/12, 31 570, nrs. 20-21.
[164] Walden 2011, p. 11. Vgl. ook Vaciago 2012, p. 9; Koning 2012, p. 52.
[165] Odinot e.a. 2012, p. 165-166.
[166] Interview KLPD; Michelle Spoormaker, landelijk officier van justitie kinderporno, persoonlijke mededeling 16 april 2012.

gegevensopslag in de cloud ook in toenemende mate wordt versleuteld door eindgebruikers.[167] Belangrijk daarbij is dat grote cloudaanbieders die zelf niet standaard alle klantgegevens in hun dienstverlening versleutelen, de klant aanraden om zelf hun gevoelige data te versleutelen.[168]

Een mogelijkheid om dit aan te pakken is om de verdachte te vragen om encryptiesleutels, maar dat kent een aantal praktische en juridische bezwaren.[169] Naar deze problematiek loopt momenteel een ander WODC-onderzoek, zodat we dat in dit rapport verder niet analyseren.[170] Relevant is hier in elk geval dat het Openbaar Ministerie een voorkeur uitspreekt voor de oplossingsrichting van het zich toegang verschaffen tot computers op afstand (oftewel hacken) boven een ontsleutelplicht voor verdachten, met het argument dat het eerste breder toepasbaar en effectiever zal zijn.[171]

5.2.4. Hacken als opsporingsbevoegdheid

Dit leidt tot de vraag of het arsenaal aan opsporingsbevoegdheden nog toegerust is op onderzoek in het huidige Internetlandschap. De klassieke tap levert minder op naarmate communicatie meer via Internetapplicaties verloopt, terwijl de Internettap nog niet in alle opzichten goed is geregeld[172]; versleuteling van communicatie en gegevensopslag neemt toe, waarbij misdadigers in toenemende mate dusdanige sterke versleuteling gebruiken dat deze niet valt te kraken; en daar komt dan de cloud bij die betekent dat een doorzoeking van een computer – van oudsher een van de belangrijkste middelen om bewijsmateriaal te verzamelen over een verdachte – minder resultaten oplevert, waarvoor de netwerkzoeking en het opvragen van gegevens bij cloudaanbieders in een grensoverschrijdende context (zoals boven geconstateerd) niet direct een goed alternatief vormen. In dit complex van factoren lopen politie en justitie tegen de grenzen van de wet aan. Dat is op zich niets nieuws – het is inherent aan de opsporing om de grenzen van bevoegdheden op te zoeken[173] – maar in het afgelopen decennium is het informatie- en communicatielandschap dusdanig veranderd dat er wel degelijk reden is om te bezien of de huidige regeling van opsporingsbevoegdheden nog voldoet. Een illustratief voorbeeld van de grenzen en daarbijbehorende dilemma's waar justitie tegenaan loopt, is het volgende.

> Vorig jaar was er bijvoorbeeld een zaak rond verborgen websites via het Tor-netwerk (dat is geen cloud, maar een gewone applicatie), waarbij niet duidelijk was in welk land websites gehost werden; daar kon je achter komen als je in de webserver zat en achter het gordijn van de website kon kijken. We hebben toen met machtiging r-c de webservers betreden en in een aantal gevallen konden we vandaaruit verbinding naar buiten leggen en zien wat het echte IP-adres was en waar de machine zich bevond. Dan kom je er achter in een aantal gevallen dat die in het buitenland staat, waar we vooraf wel rekening mee hadden gehouden maar wat we niet vooraf konden weten. In dit geval hadden we vooraf wel aangekondigd aan de VS dat dit kon gebeuren. Eigenlijk moet je dan, zodra je ziet dat je in het buitenland zit, direct terugtreden en de VS vragen het over te nemen. Hier bleek er een grote hoeveelheid nieuwe kinderporno te staan, vermoedelijk dicht bij de bron. Daarom was er een kans dat bij een interventie van ons we mogelijk toekomstig misbruik zouden kunnen voorkomen, door alle materiaal veilig te stellen en vervolgens ontoegankelijk te maken (wissen en een waarschuwingspagina daarvoor in de plaats te zetten; en als onze toegang beperkt zou gaan worden, zouden we het systeem nog kunnen vervuilen met veel politielogoplaatjes). In dit soort gevallen kom je dus in een belangenconflict terecht: strak in de leer zijn en soevereiniteit beschermen, of een bepaald risico nemen ten behoeve van ingrijpen tegen zeer ernstige misdaad. We hebben hier voor laatste gekozen. Daarbij hebben we zowel vooraf contact gehad met de Amerikaanse autoriteiten en hen ook achteraf genotificeerd, en die zeiden dat ze het prima vonden. Dan is het geen punt meer.[174]

In dit voorbeeld komt het thema van grensoverschrijdende opsporing wederom pregnant naar voren,maar ook blijkt er de behoefte uit om in een server te kunnen kijken, dat wil zeggen toegang te verschaffen tot een computer op afstand, zonder toestemming van de rechthebbende. Er bestaat echter geen bevoegdheid om te hacken, wat justitie en politie als een van de meest

[167] Walden 2011, p. 3.
[168] Ruan e.a. 2011a, p. 11.
[169] Koops 2000.
[170] Koops 2012b.
[171] Interview Openbaar Ministerie.
[172] Zie noot 152 en bijbehorende tekst.
[173] Enschede 1988, p. 223-224.
[174] Interview Openbaar Ministerie. Dit geval is ook beschreven in Nationaal Cyber Security Centrum 2012, p. 52.

concrete knelpunten in de praktijk ervaren.[175] In het geschetste complex van factoren (Internetcommunicatie; versleuteling; cloud) zou het plaatsen van een afluisterprogrammaatje op de computer van de verdachte een geschikte methode kunnen zijn om het kernprobleem te ondervangen van het 'onder de radar' verdwijnen van informatie en communicatie. Indien een verdachte gebruik maakt van clouddiensten waarbij hij zelf zijn communicatie en bestanden met robuuste encryptie versleutelt, is een heimelijk geïnstalleerd afluisterprogrammaatje (dat wachtwoorden kan onderscheppen om de versleuteling ongedaan te maken) een van de weinige manieren om toch bij gegevens te kunnen komen. Tegelijkertijd is het hacken van computers een bijzonder ingrijpende bevoegdheid, die in elk geval alleen onder zware voorwaarden en met strikte waarborgen ingevoerd zou mogen worden.[176] Het is nu aan de wetgever om te beoordelen of invoering van een dergelijke bevoegdheid als 'noodzakelijk in een democratische samenleving' (art. 8 lid 2 EVRM) moet worden beschouwd.[177]

5.2.5. De opsporingspraktijk

Bij cloud computing verschuift de opslagplaats van gegevens van verdachtes harde schijf naar een server op afstand (al dan niet in het buitenland). Dat heeft consequenties voor de manier waarop politie en justitie gegevens kunnen verzamelen. Naast de hierboven gesignaleerde jurisdictie- en juridische vragen die deze verschuiving oplevert, vormt het ook een aandachtspunt voor de opsporingspraktijk.

> Mijn conclusie is dat de opsporing een stuk slimmer moet worden. Heel veel doen we nog op de manier van dertig jaar geleden. Je plugt een stekker bij de telecomoperator en gaat in de tapkamer zitten luisteren. Die mogelijkheden zijn al lang weg, er komt niets meer over die lijn. Maar een standaard-rechercheteam pakt het nog steeds op deze manier aan. Er moet gewoon verstandig gerechercheerd worden, daar valt heel veel winst te behalen.[178]

Naast de analoge tap is de opsporingspraktijk voor een belangrijk deel geënt op de klassieke vorm van doorzoeking en inbeslagneming. Inmiddels is het genoegzaam bekend bij opsporingsambtenaren dat computers waardevolle informatie kunnen bevatten die moet worden veiliggesteld, maar zijn zij ook bekend met de specifieke uitdagingen van cloud computing? Twee van onze buitenlandse respondenten noemden dit als een aandachtspunt dat cloud computing anders maakt dan traditioneel computeronderzoek. 'The traditional law enforcement approach based on data stored in a computer (search, seizure and analysis) is not always adequate in the cloud environment.'[179] In het bijzonder speelt daarbij het probleem van onzichtbaarheid: 'how does an officer know if a suspect is storing data on one or more cloud systems?'[180]

Mede vanwege het toenemend gebruik van versleuteling (zie par. 5.2.3) wordt het steeds belangrijker om bij een doorzoeking computers 'onder stroom' in beslag te nemen, dat wil zeggen de doorzoeking te doen plaatsvinden op het moment dat de computer aan staat, voorkomen dat de verdachte de computer uitzet en vervolgens de computer ter plekke te onderzoeken dan wel met speciale apparatuur de elektrische voeding van de computer aan te houden tijdens transport en onderzoek op het bureau of in het lab. Op die manier kunnen gegevens in het werkgeheugen van de computer – die verloren gaan op het moment dat de computer wordt uitgezet – worden verzameld, waaronder waardevolle informatie kan zitten als wachtwoorden of openstaande verbindingen, bijvoorbeeld met clouddiensten. Op de werkvloer is deze vorm van computeronderzoek echter nog geen gemeengoed. Naarmate meer data gaan verhuizen naar de cloud, zal deze vorm van veiligstellen van gegevens belangrijker worden voor de opsporingspraktijk. Dit vraagt om goede voorlichting en opleiding van opsporingsambtenaren. Bij implementatie van de aanbevelingen betreffende de organisatie van de opsporing van cybercrime in Nederland,[181] zou in de basisopleiding ook aandacht moeten worden besteed aan de opslag-op-afstand van cloud computing en het belang om openstaande verbindingen bij doorzoeking en inbeslagneming te onderzoeken.

---

[175] Interviews Openbaar Ministerie en KLPD; Odinot e.a. 2012, p. 166. Zie hierover uitgebreid Oerlemans 2011 en Koning 2012.
[176] Oerlemans 2011; Koning 2012. Zie ook Vaciago 2012, p. 9.
[177] Zie ook Odinot e.a. 2012, p. 166.
[178] Interview politie Oost-Nederland.
[179] Lorenzo Picotti, reactie op enquête.
[180] Susan Brenner, reactie op enquête.
[181] Struiksma, De Vey Mestdagh & Winter 2012.

5.3. Kansen van cloud computing voor opsporing en vervolging

Op basis van ons bronnenonderzoek kunnen we vaststellen dat cloud computer meer bedreigingen dan kansen oplevert voor misdaadbestrijding in Nederland. De literatuur en onze respondenten signaleren vooral uitdagingen voor opsporing en vervolging. Niettemin zijn er ook enkele kansen waar beleid en opsporingspraktijk op zouden kunnen inspelen. Grofweg worden drie typen kansen gesignaleerd.

Ten eerste wordt het mogelijk om heimelijk gegevens te vergaren die voorheen alleen onder de unieke beschikkingsmacht van verdachten zelf bleven, maar die nu makkelijker vergaard zouden kunnen worden doordat ze naar de cloud gaan.

> Als je iemand hebt die privé alles deelt met tien maten, kun je daar in de opsporing gebruik van maken. Als je een verdachte hebt, of een groep van verdachten, kun je in kaart brengen wat ze gebruiken, een Internettap plaatsen, email volgen, met een beetje geluk zitten daar accountgegevens van bijvoorbeeld SkyDrive of Box.net bij.[182] Voor de opsporing is dat een natte droom – als je bedenkt hoe duur een observatieteam is, en nu krijgen we plotseling de mogelijkheid om mensen te volgen die zelf hun data delen.[183]

In bredere zin kan worden verwacht dat een migratie naar cloudopslag het mogelijk maakt om gegevens te vergaren via een Internettap of vordering van gegevens bij de cloudaanbieder, zonder dat een doorzoeking bij de verdachte en inbeslagneming van diens computer nodig is. Hierdoor wordt het mogelijk om langer vooronderzoek te doen zonder dat de verdachte wordt gealerteerd dat een opsporingsonderzoek gaande is. Hierbij moet wel worden aangetekend dat deze kans alleen kan worden benut indien de knelpunten van grensoverschrijdende opsporing (par. 5.1.1 en 5.1.2), de Internettap (par. 5.1.3) en heimelijke toegang (hacken, par. 5.2.4), worden aangepakt.

Een tweede type kans die door enkele respondenten wordt genoemd, is dat de politie de rekencapaciteit van de cloud kan gebruiken voor gegevensanalyses die veel rekenkracht vergen (op dezelfde manier als misdadigers dat kunnen om botnetaanvallen uit te voeren, zie par. 4.3.3). Dit kan relevant zijn voor het kraken van zware encryptie of het geautomatiseerd zoeken in grote hoeveelheden data (*data mining*). Zo kan de cloud ook leiden tot 'Forensics-as-a-Service (…) to make use of the massive computing power to facilitate cyber criminal investigations on all levels.'[184] Er worden ook technieken ontwikkeld om cloudcapaciteit te gebruiken voor het traceren van anonieme communicatie via het Tor-netwerk (vgl. par. 2.2.5).[185]

Het derde type kans is gebruikmaken van de opslagcapaciteit van de cloud voor opslag van politiegegevens. Hierover lopen de meningen enigszins uiteen. Sommigen vinden dat opslag van politiegegevens beperkt moet blijven tot Nederlands grondgebied, waardoor de cloud weinig meerwaarde biedt.[186] Anderen vinden dat politiegegevens ook best in een buitenlandse cloud kunnen worden opgeslagen, mits ze robuust zijn versleuteld en de toegang tot (reserve)sleutels goed is geregeld. Voor de vele petabytes aan gegevens die de politie verwerkt, levert opslag in de cloud een dusdanige kostenbesparing op (het zou ongeveer een derde bedragen van de kosten die gemoeid zijn met opslag op eigen servers) dat deze optie serieus aandacht verdient.[187] Voorwaarde is wel dat de beveiliging en toegang tot de gegevens goed zijn geregeld, maar dat valt te organiseren; bovendien kan een professionele opslagaanbieder een veel hoger niveau van beveiliging en continuïteit waarborgen dan de politie op de werkvloer – 'intern heb je het risico dat iemand een keer iets verkeerds uit het rek trekt, dat gebeurt je bij een cloudprovider niet.'[188] Naast nationale opslag van politiegegevens valt zelfs nog te denken aan een internationale databank van politiegegevens in de cloud, in het kader van de toenemende uitwisseling van politiegegevens binnen Europa.[189]

---

[182] Diensten voor opslag en delen van documenten, zie http://windows.microsoft.com/nl-nl/skydrive/home en https://www.box.com/ (geraadpleegde 3 juli 2012). [noot toegevoegd door auteurs]
[183] Interview politie Oost-Nederland.
[184] Ruan e.a. 2011a, p. 14-15.
[185] Fu e.a. 2010.
[186] Interview KLPD.
[187] Interview politie Oost-Nederland.
[188] Ibid.
[189] Interview Openbaar Ministerie.

5.4. Conclusie

Cloud computing stelt de opsporing voor aanzienlijke uitdagingen. De meest gebruikte methoden om gegevens te verzamelen in een digitale context – doorzoeking en netwerkzoeking, vorderen van gegevens, onderscheppen van gegevens – hebben allemaal beperkingen wanneer ze worden toegepast op gegevens die in een cloud liggen opgeslagen of wanneer via de cloud worden gecommuniceerd. Het voornaamste knelpunt is de territoriale grenzen waaraan de Nederlandse opsporing nog steeds is gebonden. Aangezien een grensoverschrijdende netwerkzoeking niet is toegestaan (behalve in de weinig voorkomende gevallen van toestemming van de verdachte of vrijwillige medewerking van een buitenlandse aanbieder), moet justitie zich verlaten op wederzijdse rechtshulp met een vordering aan de buitenlandse cloudaanbieder om gegevens te leveren of een Internettap bij de Nederlandse toegangsaanbieder van de verdachte. Het eerste is mogelijk en werkt in de praktijk op zich goed bij grote Amerikaanse aanbieders, maar het werkt vertragend en is problematisch bij aanbieders die niet willen of kunnen meewerken. Het laatste is ook mogelijk en werkt ook tot op zekere hoogte, maar de IP-tap is nog niet goed uitgekristalliseerd in wetgeving en praktijk.

Ook binnen de Nederlandse juridische context zelf zijn er juridische vragen en knelpunten, zoals wanneer een cloudaanbieder als communicatieaanbieder (Sv) of openbare telecommunicatieaanbieder (Tw) moet worden gekwalificeerd; hoe het onderscheid in de strafvorderlijke regeling tussen opgeslagen en getransporteerde gegevens en het onderscheid tussen communicatie en niet-communicatie zich verhouden tot cloudopslag- en verwerkingsdiensten; en of door de opkomst van cloud computing in samenhang met toenemend gebruik van versleuteling het noodzakelijk wordt om een bevoegdheid in te voeren om op afstand heimelijk zich toegang te kunnen verschaffen tot computers van verdachten. Ook zal de opsporingspraktijk een omslag moeten maken om in te spelen op de verschuiving van gegevens van harde schijf naar cloud.

Wanneer deze knelpunten worden aangepakt, biedt de cloud uiteindelijk ook nieuwe kansen voor de opsporing, omdat er veel meer gegevens binnen bereik komen om heimelijk te onderzoeken, waardoor de voorfase van onderzoek langer kan doorlopen zonder de verdachte te alerteren op het onderzoek. Andere potentiële kansen van de cloud liggen in de reken- en opslagcapaciteit van de cloud die zou kunnen worden benut om politieprocessen efficiënter uit te voeren.

6. Vervolging in de cloud: bewijsaspecten

Wanneer de opsporing voldoende bewijs oplevert, kan justitie overgaan tot vervolging. Ook daar bestaan knelpunten. Deels hebben die te maken met dezelfde uitdagingen als bij cybercriminaliteit in het algemeen, waarbij bijvoorbeeld juridische vragen spelen rond toelaatbaarheid van digitaal bewijs en praktische of juridische problemen rond de vervolging wanneer de dader zich in het buitenland bevindt (al dan niet in een digitale vrijhaven). Ook zal aannemelijk moeten worden gemaakt dat digitaal bewijs, dat meestal afkomstig is van een gegevensdrager, aan de verdachte moet worden toegeschreven (en niet afkomstig is van andere computergebruikers). Voor dergelijke aspecten lijkt de cloud geen nieuwe dimensie toe te voegen. Wij beperken ons daarom in dit hoofdstuk tot die aspecten, met name in relatie tot bewijs, waarin de cloud voor extra problemen – of kansen – kan zorgen.

Dat bewijs een belangrijk aspect is, blijkt uit ons vraaggesprek met het KLPD:

> Het belangrijkste knelpunt is de bewijslast: als we fysiek ter plaatse een systeem veiligstellen, maken we een forensische kopie die aanvaardbaar is als bewijs in de rechtszaal. Bij clouddiensten kun je echter geen forensische kopie laten maken door de aanbieder, en dat kunnen we zelf al helemaal niet. Het is onduidelijk of het materiaal dan in de rechtszaal volledig gebruikt kan worden als bewijs. (…) Het belangrijkste probleem voor opsporing en vervolging veroorzaakt door cloud computing is de bewijslast: in hoeverre is materiaal dat je via rechtshulp uit de cloud krijgt een forensisch gewaarmerkte kopie?[190]

Forensisch digitaal bewijs in relatie tot de cloud krijgt ook relatief veel aandacht in de literatuur. Deels gaat deze literatuur in op forensisch onderzoek door eindgebruikers (denk aan bedrijven, accountants en verzekeraars) die huidige procedures voor 'audit trails' moeten omzetten naar een cloudomgeving. Bedrijven zullen hierover afspraken moeten maken met cloudaanbieders.[191] Bij forensisch onderzoek door strafvorderlijke opsporingsdiensten speelt dit aspect echter minder een rol – behalve voor zover opsporingsonderzoek gebruik maakt van de forensische procedures van bedrijven zelf, zoals bij bepaalde fraude- en witwaszaken.[192] Belangrijker voor deze studie is dat het verzamelen van bewijsmateriaal in de cloud door opsporingsinstanties in bepaalde opzichten gecompliceerd wordt. Vaciago stelt dat 'computer forensics (…) *experienced a fundamental change* due to the incredible expansion of cloud computing systems' in een verslag van een workshop getiteld – wellicht met enige overdrijving – 'The Death of Computer Forensics'.[193] Bij de complicaties rond forensisch bewijs kunnen technische en juridische aspecten worden onderscheiden.

6.1. Technische complicaties

Een overkoepelend knelpunt is een gebrek aan procedures en standaarden voor de forensisch betrouwbare vastlegging van bewijsmateriaal uit de cloud.[194] Voor zover er standaarden en richtlijnen bestaan voor digitaal bewijs – die in Nederland wel lijken te bestaan maar geen duidelijke formele status hebben – richten deze zich op het vastleggen van gegevens uit fysieke gegevensdragers. Bij de cloud komen problemen naar voren, die deels onderkend worden in het al wat langer bestaande gebied van *network forensics*. Het betreft onder andere de moeilijkheid om te bewijzen dat een kopie van gegevens die uit een netwerk worden opgehaald, één-op-één hetzelfde is als het 'origineel' (voor zover daarvan sprake kan zijn bij computergegevens), en de vraag of de computers die gebruikt zijn bij de vastlegging van de gegevens correct functioneerden. Deze vragen worden verder op scherp gesteld door de virtualisatie van de cloud,

[190] Interview KLPD.
[191] Ruan e.a. 2011a, p. 8; interview Rabobank Nederland.
[192] Taylor e.a. 2010, p. 307.
[193] Vaciago 2011, p. 1.
[194] Taylor e.a. 2010, p. 306; Ruan e.a. 2011b, die aangeeft dat in een enquête onder 80 experts op de vraag 'the most needed tools and procedures for cloud forensics' als belangrijkste behoefte naar voren kwam 'A procedure and a set of toolkits to preserve the soundness of digital evidence in the Cloud (89.55% think it is important or very important, 55.22% think it is very important)'.

waarbij gegevens decentraal en gedistribueerd worden opgeslagen.[195] Wanneer het om een publieke cloudaanbieder gaat (die aan meerdere klanten tegelijk dezelfde infrastructuur ter beschikking stelt, waarbij klantruimtes logisch maar niet fysiek zijn afgescheiden in 'virtuele machines'), komt daar nog het probleem bij van datascheiding: wanneer data van een bepaalde klant (denk aan een verdachte) worden opgevraagd uit de cloud, moeten deze data gescheiden worden van data van andere klanten die niets met het onderzoek te maken hebben; deze laatste gegevens moeten immers niet door justitie worden vergaard. De scheiding van data stelt echter de niet-manipuleerbaarheid van de wel verkregen gegevens ter discussie. Voor dit probleem van 'virtuele huisgenoten' (multitenancy) moeten nog adequate forensische procedures worden ontwikkeld.[196]

Een gebrek aan forensische procedures is ook zichtbaar aan de kant van cloudaanbieders, die in hun contracten over het algemeen niets zeggen over of, hoe en onder welke voorwaarden zij forensisch onderzoek – in opdracht van de klant zelf of in opdracht van justitie – zullen doen.[197] Daarbij kan het bedrijfsbelang van de cloudaanbieder – namelijk om de continuïteit van dienstverlening voor klanten te verzekeren – op gespannen voet komen te staan met een forensische procedure waarbij een integrale momentopname moet worden gemaakt van de situatie in de cloud.[198] Ook zal forensisch onderzoek op complexe (keten)afhankelijkheden tussen aanbieders stuiten, met name in gevallen waarbij een cloudinfrastructuuraanbieder (IaaS) netwerkcapaciteit ter beschikking stelt aan een clouddienstverlener (SaaS).[199] Een en ander betekent dat justitie en forensisch onderzoekers flink moeten investeren in samenwerking met cloudaanbieders, onder andere om forensische ontwerpprincipes in clouddiensten en -infrastructuren mee te laten nemen en om hulpmiddelen die voor forensische procedures noodzakelijke zijn (zoals logging, momentopnamen en auditing van toegang tot data) te laten installeren.[200]

Verder is nog van belang dat bepaalde data die bij onderzoek van een harde schijf naar boven komen, niet of moeilijker uit de cloud zijn te verkrijgen. Het gaat daarbij om metadata (zoals wanneer een bestand gemaakt en laatstelijk geraadpleegd is),[201] data in het werkgeheugen[202] en data die verwijderd zijn maar die met forensische programma's vaak nog weer zichtbaar gemaakt kunnen worden. Dit laatste levert bijvoorbeeld in kinderpornografiezaken vaak bewijs op dat tot een veroordeling kan leiden. Bij gegevens die in de cloud liggen opgeslagen, is het een complexe uitdaging om verwijderde gegevens te reconstrueren, vanwege de moeilijkheid om door de klant verwijderde gegevens (dat wil zeggen waarvan het logische adres is verwijderd maar die nog wel bestaan) in verband te brengen met de verdachte en ze in de cloud te lokaliseren.[203]

6.2. Juridische complicaties

Wat betreft juridische aspecten van bewijsmateriaal uit de cloud wordt in de literatuur jurisdictie als het belangrijkste knelpunt gesignaleerd. In een enquête onder 80 experts wordt jurisdictie als de top-uitdgaging genoemd: 'the top 5 challenges for cloud forensics are: (1) Jurisdiction (90.14% agree or strongly agree, 53.52% strongly agree) (…).'[204] De studie legt evenwel niet uit waar het jurisdictieprobleem precies zit; het is goed mogelijk dat de uitdaging vooral het

[195] Birk 2011, p. 1 ('the lack of physical access to servers constitutes a completely new and disruptive challenge for investigators'); Vaciago 2011, p. 2 ('the most difficult challenge is posed by the **loss of data control**: virtualization is one of the key elements in the implementation of cloud services, while in most cases investigators require evidence to be obtained from physical devices (…)even if it were possible to reconstruct the image, the investigator would never be able to validate it "beyond a reasonable doubt" in the same way as would be possible with a physical hard drive'); interview Rabobank Nederland ('De traditionele manier om een complete forensische image te maken zal een stuk moeilijker worden als je niet de beschikking hebt over de omgeving').
[196] Ruan e.a. 2011a, p. 11 ('it remains a challenge for the CSP and law enforcement to keep the same segregating in the whole process of investigation without breaching the confidentiality of other tenants sharing the same infrastructure and ensure the admissibility of the evidence'); interview Rabobank Nederland.
[197] Ruan e.a. 2011a.
[198] Ruan e.a. 2011a, p. 8.
[199] Ruan e.a. 2011b, p. 9, 12.
[200] Ruan e.a. 2011a, p. 5; Birk 2011; Vaciago 2011; interview Rabobank Nederland.
[201] Taylor e.a. 2010, p. 307.
[202] Vaciago 2011, p. 2.
[203] Ibid.; Ruan e.a. 2011a, p. 11.
[204] Ruan e.a. 2011b, p. 9.

grensoverschrijdend vastleggen van bewijsmateriaal is, wat meer te maken heeft met de juridische opsporingsproblemen (zie par. 5.1) dan met bewijsproblemen. Het kan evenwel ook te maken hebben met jurisdictievragen rond bewijs. Volgens Birk e.a. verschillen de eisen voor digitaal bewijs van land tot land, terwijl de vuistregel dat het recht van toepassing is van het land waar de gegevens opgeslagen zijn ('lex situs'), nu juist problematisch is in de cloud.[205] De auteurs hebben het echter vooral over privaatrecht; over strafrechtelijk toepasselijk recht merken zij slecht op dat het probleem tot nu toe niet opgelost is en dat er dringende behoefte bestaat aan een – idealiter internationaal afgestemde – wettelijke grondslag voor de bepaling welke eisen aan het bewijs worden gesteld.[206]

Of de soep zo heet gegeten wordt als hij in de literatuur hier wordt opgediend, is echter de vraag. Ten eerste kent Nederland een betrekkelijk open bewijsstelsel. Als wettige bewijsmiddelen gelden de eigen waarneming van de rechter, verklaringen van verdachte, getuigen en deskundigen, en schriftelijke bescheiden (art. 339 Sv). Van de schriftelijke bescheiden hebben processen-verbaal en andere door bevoegde instanties opgemaakte geschriften, alsook geschriften opgemaakt door buitenlandse ambtenaren zelfstandige rechtskracht; alle overige geschriften kunnen ook dienen als bewijsmateriaal, maar alleen in samenhang met andere bewijsmiddelen (art. 344 Sv). Geschriften hoeven niet op papier te staan, maar kunnen ook elektronisch zijn; het gaat erom dat zij voor voorlezing vatbaar zijn.[207] Aan digitaal bewijs worden verder geen formele eisen gesteld. Het komt vooral neer op de overtuigingskracht van het bewijs, dat de rechter de innerlijke overtuiging moet geven dat de verdachte het telastgelegde feit heeft begaan (art. 338 Sv). Die overtuigingskracht hangt bij digitaal bewijs vooral samen met de betrouwbaarheid ervan. Veelal zal materiaal dat uit de cloud is verkregen en als bewijsmateriaal wordt opgevoerd, de vorm hebben van processen-verbaal door opsporingsambtenaren dan wel rapporten van forensisch digitaal onderzoekers; de betrouwbaarheid daarvan hoeft over het algemeen geen bijzondere problemen op te leveren. Wel is het zo dat door de technische complicaties (par. 6.1) er nog weinig ervaring is met bewijsmateriaal uit de cloud, zodat de rechtsontwikkeling nog zal moeten uitwijzen of er problemen gaan ontstaan ten aanzien van de betrouwbaarheid van digitaal cloudbewijs.

Ten tweede is het gebruik van materiaal verkregen via een rechtshulpverzoek als bewijs in een Nederlandse strafzaak niet direct problematisch. Waar voorheen bij een rechtshulpverzoek in strafzaken het recht van het aangezochte land gold voor de uitvoering van bewijsverkrijging ('locus regit actum'), is in de Europese Unie sinds een jaar of tien het uitgangspunt dat bij de uitvoering van een rechtshulpverzoek de aangezochte staat zoveel mogelijk de procedures en vereisten van de verzoekende staat in acht neem ('forum regit actum').[208] De verzoekende staat kan bij een rechtshulpverzoek formaliteiten en procedures aangeven die bij de uitvoering in acht moeten worden genomen; de aangezochte staat moet deze vereisten in acht nemen, tenzij ze in strijd zijn met fundamentele rechtsbeginselen van de aangezochte staat.[209] Hierbij past wel de kanttekening dat het uitgangspunt van 'forum regit actum' binnen de EU bestaat, maar niet als zodanig is geregeld in het rechtshulpverdrag van de EU met de VS.[210] Het rechtshulpverdrag tussen Nederland en de VS in strafzaken bevat een hybride variant waarin beide uitgangspunten zijn opgenomen:

> Verzoeken worden uitgevoerd overeenkomstig de interne wet en de interne procedures van de aangezochte Staat, behalve voor zover dit Verdrag anders bepaalt. De in het verzoek aangegeven

[205] Birk, Heinson & Wegener 2011, p. 331.
[206] Ibid.
[207] A.L. Melai, M.S. Groenhuijsen e.a. (red.), *Wetboek van Strafvordering*, losbladig commentaar, aant. 2 op art. 344.
[208] Vermeulen 2011, p. 41.
[209] Zie art. 4 par. 1 van de Overeenkomst betreffende de wederzijdse rechtshulp in strafzaken tussen de lidstaten van de Europese Unie (2000); art. 8 van het Tweede aanvullende protocol bij het Europees Verdrag aangaande de wederzijdse rechtshulp in strafzaken (2001); art. 12 van het Kaderbesluit 2008/978/JBZ betreffende het bewijsverkrijgingsbevel; art. 8 par. 2 van het Richtlijnvoorstel betreffende het Europees onderzoeksbevel in strafzaken (2010/0817 (COD)).
[210] De Overeenkomst betreffende wederzijdse rechtshulp in strafzaken tussen de Europese Unie en de Verenigde Staten van Amerika, *PubEU* L181/34, 19.7.2003 (art. 9) bevat slechts bepalingen voor het stellen van voorwaarden door de aangezochte staat (dus niet de verzoekende staat) in verband met de bescherming van persoonsgegevens.

> procedures dienen te worden gevolgd, zelfs indien zij in de aangezochte Staat ongebruikelijk zijn, behalve voor zover zulks uitdrukkelijk is verboden in de wetten van de aangezochte Staat.[211]

Nederland kan dus bij rechtshulpverzoeken om gegevens van een buitenlandse cloudaanbieder te vorderen, voorwaarden aangeven die ertoe bijdragen dat het te verkrijgen materiaal als bewijs gebruikt kan worden in Nederland.

Of het vervolgens ook gebruikt *wordt* als bewijsmateriaal, is een andere kwestie. Het stellen van voorwaarden bij een rechtshulpverzoek impliceert een intentie om het verkregen materiaal als bewijs te gebruiken, maar biedt geen garantie voor de toelaatbaarheid van het bewijs.[212] Dat oordeel is immers aan de rechter ter zitting die over het bewijsmateriaal oordeelt. Over het algemeen aanvaardt deze bewijsmateriaal dat via rechtshulp is verkregen als rechtmatig en zal hij niet gaan toetsen of het aangezochte land een rechtsregel heeft geschonden bij de bewijsverkrijging. In sommige gevallen dient de rechter echter wel te onderzoeken of materiaal op rechtmatige wijze uit de andere staat is verkregen. In de zaak *Stojkovic t. Frankrijk en België* uit 2011 had België op verzoek van Frankrijk de heer Stojkovic als getuige verhoord, echter zonder aanwezigheid van een advocaat, ondanks een daartoe strekkend verzoek van de rechter van instructie in het rechtshulpverzoek en een uitdrukkelijk verzoek van Stojkovic zelf. Volgens het Hof had het Franse gerecht bij het gebruik van het verhoor als bewijs tegen Stojkovic moeten onderzoeken of de voorwaarde in het rechtshulpverzoek om het verhoor in aanwezigheid van een raadsman te doen plaatsvinden, was nageleefd in België, en of de activiteiten in België dusdanig in strijd waren geweest met de rechten van de verdachte dat het gebruik van de resultaten als bewijs in de Franse procedure een oneerlijk proces zou opleveren.[213]

Dat betekent dat wanneer de verdediging klaagt over gebruik van gegevens die uit de cloud zijn verkregen, omdat de vergaring in strijd met het recht zou zijn, de rechter moet onderzoeken of het bewijs wel rechtmatig is verkregen. Dat kan gecompliceerd zijn bij gebrek aan forensische procedures (zie par. 6.1), omdat niet altijd duidelijk zal zijn hoe het materiaal uit de cloud is verzameld. Het oproepen van forensisch onderzoekers (van de cloudaanbieder of van buitenlandse ambtenaren) als getuige zal ook niet altijd praktisch haalbaar zijn, zodat de gegevensvergaring in de rechtszaal niet goed kan worden betwist. Afhankelijk van waar het (volgens de verdediging) precies aan geschort heeft, kan dat betekenen dat het materiaal niet toelaatbaar is als bewijs of dat de betrouwbaarheid ervan is aangetast; in beide gevallen zal het dan niet gebruikt kunnen worden. Of dat vaak zal voorkomen, is de vraag. Digitaal bewijs wordt weinig aangevochten in de rechtszaal, en het is niet zeker of cloudbewijs daar verandering in zal brengen.

Daarbij komt dat de rechter kijkt naar het hele dossier en dat ook onrechtmatig verkregen bewijs in sommige gevallen toch kan meewegen in het rechterlijk oordeel. Het gaat immers om de procedure als geheel, waarbij onder andere gekeken wordt naar de mate waarin het omstreden materiaal betwistbaar is voor de verdediging in de rechtszaal en in welke mate het oordeel stoelt op ander bewijs dan het omstreden bewijs.[214] Indien het bestreden materiaal uit de cloud ondersteunend maar niet dragend bewijs is, zou het dus toch meegewogen kunnen worden.

Bovendien wordt de nodige ruimte geboden door het leerstuk van de Schutznorm, die bepaalt dat bewijsmateriaal niet hoeft te worden uitgesloten indien de norm die is geschonden (bij onrechtmatig verkregen bewijs) een ander belang dient dan dat van de verdachte:

---

[211] Art. 12 lid 2 Verdrag tussen het Koninkrijk der Nederlanden en de Verenigde Staten van Amerika aangaande wederzijdse rechtshulp in strafzaken.
[212] Vermeule 2011, p. 43.
[213] EHRM 27 oktober 2011, Stojkovic t. Frankrijk en België, app.nr. 25303/08, par. 41 ('Il revenait également aux autorités françaises d'apprécier *a posteriori* la portée du déroulement de la commission rogatoire sur la validité de la procédure en cours devant elles') en 55 ('Il incombait donc aux juridictions pénales françaises de s'assurer que les actes réalisés en Belgique n'avaient pas été accomplis en violation des droits de la défense et de veiller ainsi à l'équité de la procédure dont elles avaient la charge, l'équité s'appréciant en principe au regard de l'ensemble de la procédure').
[214] Zie EHRM 12 juli 1988, Schenk t. Frankrijk, app.nr. 10862/84.

> Opmerking verdient dat indien het niet de verdachte is die door de niet-naleving van het voorschrift is getroffen in het belang dat de overtreden norm beoogt te beschermen, in de te berechten zaak als regel geen rechtsgevolg zal behoeven te worden verbonden aan het verzuim.[215]

Dit is in het kader van dit rapport vooral relevant omdat een belangrijk deel van de problemen met de verkrijging van bewijs te maken heeft met nationale soevereiniteit en niet zozeer met het privacybelang van cloudgebruikers (zie par. 5.1). De Schutznorm opent daarom mogelijkheden voor de grensoverschrijdende netwerkzoeking, ook als daarvoor geen toestemming van de buitenlandse staat is verkregen waar de cloud genetvest is. Een dergelijke netwerkzoeking is weliswaar onrechtmatig, maar de norm die daarbij wordt geschonden is de soevereiniteit van andere staten en niet – zolang tenminste de netwerkzoeking voldoet aan de overige eisen van art. 125j Sv – het privacybelang van burgers. Het is daarom goed mogelijk dat extraterritoriale opsporingsactiviteiten door de rechter 'weggeschutznormd' worden.[216]

Al met al kunnen we concluderen dat er weliswaar problemen kunnen ontstaan bij het opvoeren van uit de cloud verkregen materiaal als bewijs, met name wanneer de verdediging aanvoert dat het bewijs in het buitenland onrechtmatig is verkregen of dat het onbetrouwbaar bewijs is vanwege gebrekkige forensische procedures bij de vastlegging, maar dat deze problemen niet onoverkomelijk hoeven te zijn. Belangrijk is dat zo goed mogelijk wordt gedocumenteerd hoe het materiaal uit de cloud is verkregen, dat het materiaal voldoende betwist kan worden in de rechtszaal, en dat het gebruik ervan als bewijs in samenhang met het overige voorhanden bewijs als geheel een eerlijk proces oplevert. Onvolkomenheden in de bewijsgaring hoeven daarbij niet altijd te leiden tot bewijsuitsluiting.

6.3. Forensische kansen

Of de cloud naast complicaties ook kansen biedt voor forensisch bewijs valt te betwijfelen. Onze geïnterviewden en respondenten noemen geen potentiële verbeteringen die de cloud zou kunnen opleveren. Ook de enquête onder 80 experts van Ruan e.a. ziet weinig kansen op het gebied van *cloud forensics*. Het is op zich mogelijk dat in de cloud meer data beschikbaar zijn dan op harde schijven van verdachten: in de cloud zwerven meer kopieën rond van hetzelfde bestand, die ook blijven bestaan wanneer de cloudgebruiker het bestand verwijdert:

> Data abundance generated in the Cloud is helpful to investigations as full data deletion cannot be guaranteed and investigators can take advantage of it to recover data as evidence. Scaled up to the Cloud, when a request to delete a cloud resource is made it actually technically can never result in true wiping of the data. (…) Thus pieces or segments of data that is crucial to investigation are very likely to remain somewhere in the Cloud for the investigators to discover.[217]

Het is echter complex om dergelijke sporen van verwijderde bestanden te achterhalen,[218] en van de experts uit Ruan's onderzoek is slechts een derde het eens met de stelling dat 'there are more chances to find critical evidence left in the Cloud due to data abundance.'[219] Het enige waar de experts zich wel in meerderheid in kunnen vinden is de stelling dat de cloud de kans biedt om een fundament van forensische standaarden en beleid te scheppen dat kan mee-evolueren met de technologie.[220] De cloud zou, met andere woorden, het momentum kunnen bieden om (in internationaal verband) nu eens goede standaarden te ontwikkelen voor het veiligstellen van digitaal bewijs in een netwerkomgeving, iets waar al langere tijd behoefte aan is.

6.4. Conclusie

Bij vervolging spelen rond de cloud vooral vragen rond technische en juridische aspecten van bewijs. Procedures en standaarden voor bewijsvergaring uit de cloud zijn nog in een vroeg

---

[215] Zie HR 30 maart 2004, LJN AM2533, par. 3.5. Zie ook de conclusie van A-G Jörg bij HR 6 juli 2004, LJN AO9785, die de Schutznorm iets eenvoudiger formuleert: 'De norm waarop een beroep wordt gedaan moet in abstracto strekken tot bescherming van de belangen van de verdachte, terwijl voorts in concreto de door die norm beschermde belangen moeten zijn geschaad.'
[216] Zie ook Rb. Rotterdam 26 april 2010, LJN BM2518, beschreven in noot 44 en bijbehorende tekst.
[217] Ruan e.a. 2011a, p. 13-14.
[218] Zie boven, noot 203.
[219] Ruan e.a. 2011b, p. 10.
[220] Ibid.

stadium van ontwikkeling. Technisch is het niet eenvoudig bewijsbaar dat een document dat uit de cloud wordt gehaald hetzelfde is als dat wat erin is gestopt, wanneer het gedistribueerd is opgeslagen en op basis van algoritmes op verschillende servers wordt bewaard. Het zal niet altijd duidelijk zijn welke forensische procedures er zijn gehanteerd om een document uit de cloud te verkrijgen. Er is behoefte aan de ontwikkeling van procedures en standaarden, alsook aan nauwe samenwerking met cloudaanbieders om basisvoorzieningen voor forensisch onderzoek in cloudinfrastructuren en -praktijken in te bouwen. De technische complicaties van cloudbewijs kunnen zich vertalen in juridische complicaties rond de betrouwbaarheid van bewijs, maar of dat substantiële problemen zal opleveren – meer dan bij andere vormen van digitaal bewijs – zal de rechtspraktijk moeten uitwijzen. Formeel-juridisch zijn er verder niet veel complicaties te verwachten bij cloudbewijs.

7. Conclusies

7.1. Knelpunten en kansen

Cloud computing is het uitbesteden van gegevensbeheer of computerapplicaties aan een dienstverlener, met gedistribueerde opslag en in beginsel zonder regie over de locatie. De opkomst van cloud computing leidt tot verschuivingen in patronen van gegevensverwerking en gegevensopslag. In essentie betekent dit dat gegevens niet meer in het bedrijf of bij mensen thuis opgeslagen liggen, maar elders. Dit kan tot kwetsbaarheden leiden, zowel bij bedrijven en burgers die de controle over gegevens uit handen geven, als bij opsporingdiensten die in de praktijk sterk leunen op locaal onderzoek van gegevens. Cloud computing kan dus potentieel belangrijke gevolgen hebben voor het plegen van gegevensgerelateerde criminaliteit en voor opsporing en vervolging van misdrijven waarin digitaal onderzoek een rol speelt.

Het gaat echter niet om een radicale verandering. Eerder is er sprake van een gradueel verschil met bestaande vormen van gegevensverwerking. Veel van onze geïnterviewden en respondenten vinden dat er in principe weinig nieuws onder de zon is bij cloud computing ten opzichte van bestaande cybercriminaliteit en -opsporing. De ervaringen met cloud computing in opsporing en vervolging tot nu toe lijken ook gering te zijn, zowel in Nederland als in het buitenland (met uitzondering van de al lang bestaande webmaildiensten). Het lijkt op het eerste gezicht, zoals bij veel innovaties in de ICT die kunnen worden misbruikt voor criminele doeleinden, op oude wijn in nieuwe zakken. Maar bij cybercriminaliteit gaat het wel om heel veel wijn in allerlei soorten zakken,[221] en de verschuivingen die cloud computing teweegbrengt zouden wel degelijk verschil kunnen maken voor misdaad en opsporing. Bij nadere beschouwing heeft de opkomst van de cloud dan ook wel degelijk belangrijke gevolgen, doordat de migratie van gegevensverwerking naar de cloud bepaalde ontwikkelingen en al langer bestaande problemen op scherp stelt. Dat heeft vooral te maken met het 'verlies van locatie'[222] dat de cloud met zich meebrengt en dat een fundamentele uitdaging vormt voor de territoriaal georiënteerde strafvordering.

7.1.1. Knelpunten in het materiële strafrecht bij cloudcriminaliteit

Uit ons onderzoek blijkt dat de gevolgen van cloud computing groter zijn voor de opsporing en vervolging dan voor het plegen van misdaad. Weliswaar wordt de cloud gebruikt voor het plegen van bepaalde typen aanvallen – momenteel vooral DDoS-aanvallen, het versturen van malware en het kraken van wachtwoorden – en voor het uitwisselen van gegevens binnen criminele groepen, maar de cloud verschilt hierin niet bijzonder van andere Internetapplicaties. In juridisch opzicht roept cloudmisdaad weinig specifieke vragen of uitdagingen op. Voor beleid en praktijk van misdaadbestrijding is het wel van belang om ontwikkelingen in de cloud nauw in de gaten te houden, maar dat is een logisch onderdeel van cyberopsporing, dat uit de aard der zaak nieuwe ICT-ontwikkelingen op de voet moet volgen. Het potentiële misbruik van de cloud moet daarbij in perspectief worden geplaatst in relatie tot andere vormen van ICT-misbruik. Bijvoorbeeld het gemak waarmee 'kogelvrije Internetdiensten' (die toegang door derden, waaronder opsporingsdiensten, maximaal proberen tegen te houden) kunnen worden opgezet, is op dit moment misschien zorgwekkender dan misbruik van bona fide clouddiensten.[223]

Het enige aspect waarin de cloud relatief nieuw lijkt voor het materiële strafrecht, is het faciliteren van het kraken van wachtwoorden en versleutelde bestanden. Dat kan weliswaar ook met 'oude' applicaties, maar het zou door de rekenkracht van cloudinfrastructuur meer dan voorheen gefaciliteerd kunnen worden en daardoor datalekken en identiteitsfraude in de hand werken. Dit is een aandachtspunt voor het beleid, waarbij afgewogen moet worden of de gevaarzetting dusdanig groot is dat het materiële strafrecht moet worden ingeroepen tegen het (systematisch, grootschalig) kraken van wachtwoorden (wat momenteel als zodanig niet strafbaar is), of dat kan worden volstaan met andere maatregelen (zoals zelfregulering door

[221] Jewkes & Yar 2010, p. 3.
[222] Spoenle 2010, p. 5 ('loss of location').
[223] Interviews KLPD en Rabobank Nederland.

cloudaanbieders), met als vangnet de reeds bestaande strafbepalingen die het misbruik van (al dan niet gekraakte) wachtwoorden strafbaar stellen (zoals hacken en oplichting).

7.1.2. Knelpunten bij opsporing en vervolging in de cloud

Hoewel de uitdagingen van de cloud voor opsporing en vervolging niet fundamenteel verschillen van bestaande uitdagingen rond cyberopsporing, voegt de verschuiving van gegevensverwerking naar de cloud wel een nieuwe dimensie toe aan bekende problemen. Waar cybercriminaliteit van oudsher al grensoverschrijdend en locatieonafhankelijk is en cyberopsporing dus ook van oudsher al te maken heeft met vragen rond grensoverschrijdende toegang tot gegevens, worden deze vragen op scherp gesteld door de 'loss of location'[224] die de cloud met zich meebrengt. Bestanden die in de cloud liggen opgeslagen, zijn veelal in meerdere kopieën en in stukjes opgeknipt opgeslagen op verschillende servers, waarbij het systeem zelf, op basis van vraag en aanbod, de meest efficiënte opslag berekent en bestanddelen verplaatst. Het is daarom op vrijwel elk moment moeilijk te bepalen, ook voor de cloudaanbieder zelf, op welk(e) plaats(en) een bestand ligt opgeslagen. De klassieke Internetvraag 'Is there a there there?'[225] moet met de opkomst van cloud computing vermoedelijk negatief worden beantwoord. De locatie waar gegevens 'zich bevinden' werkt niet meer als leidend aanknopingspunt bij de bepaling van rechten en plichten in relatie tot de cloud.[226]

Dit heeft implicaties voor zowel theorie als praktijk. Op het abstracte niveau van de theorievorming rond jurisdictie en soevereiniteit staan de 'cybernauten' tegenover de 'territorialisten'.[227] De laatsten, die cyberspace niet als zelfstandige ruimte benaderen maar de nadruk leggen op de fysieke plaats van servers en routerende computers, zullen terrein moeten prijsgeven aan de eersten wanneer cloud computing een vaste plaats verovert in het internationale Internetlandschap. 'Cloud' is in dit opzicht een treffende metafoor, die aangeeft dat gegevens niet aan de aarde verbonden zijn maar, in moeilijk te grijpen vorm, ergens boven de aarde zweven en zich verplaatsen door de grillen van hoge en lage druk in plaats van door menselijke aansturing.[228] Of de territorialisten daadwerkelijk zullen opschuiven in de richting van de cybernauten, zal nog moeten blijken. Wat ons betreft is er in elk geval wel het nodige te zeggen voor een verschuiving van nadruk van de plaats van servers waar gegevens zich bevinden naar de plaats van mensen die iets met die gegevens doen. Dit sluit aan bij literatuur over de cloud die, voor de bepaling van rechtsmacht, aanknopingspunten zoekt bij de plaats(en) van degenen die beschikkingsmacht hebben over gegevens (zoals de aanbieder en de klant) in plaats van bij de locatie van de server waar de gegevens opgeslagen liggen.[229]

Op het concrete niveau van de praktijk is het 'verlies van locatie' bijzonder relevant, in het bijzonder in de strafvorderlijke context waar territoriale soevereiniteit nog altijd een zeer bepalende rol speelt. Die bepalende rol blijkt bijvoorbeeld uit de moeizame onderhandelingen bij de totstandkoming van het Cybercrime-Verdrag, waarin men over grensoverschrijdende toegang tot gegevens (in art. 32 CCV) slechts een 'tandeloos compromis'[230] kon bereiken, en uit recente aanbevelingen binnen de Raad van Europa en de EU om opsporingsdiensten niet rechtstreeks buitenlandse Internetaanbieders te laten bevragen maar dit altijd via de weg van rechtshulp te doen.[231] Evenzo staat de Nederlandse opsporingswetgeving een netwerkzoeking slechts toe tot de landsgrens en moeten gegevens die via buitenlandse Internetaanbieders worden verwerkt, opgevraagd worden via een rechtshulpverzoek. Wanneer de gegevenshuishouding van misdadigers migreert naar de cloud, zal de Nederlandse opsporingspraktijk hard tegen deze territoriale beperkingen oplopen. Dit vraagt om aandacht van wetgeving en beleid, waarvoor we hieronder enkele aanbevelingen doen. Ondertussen zal de opsporingspraktijk een omslag

[224] Spoenle 2010, p. 5.
[225] Geist 2001.
[226] Spoenle 2010.
[227] Zie par. 4.4.
[228] Waarbij aangetekend zij dat de mens wel – vooralsnog niet bijzonder succesvolle – pogingen doet wolken aan te sturen, zoals bij de Olympische Spelen in Beijing in 2008; zie http://en.wikipedia.org/wiki/Beijing_Weather_Modification_Office (geraadpleegd 3 juli 2012).
[229] Zie bijvoorbeeld Spoenle 2010, p. 10-12 ('the power of disposal'), Lodder 2012, p. 18 (citerend uit eerder onderzoek uit 2000: 'doorslaggevend is (…) wie de mogelijkheid heeft de op de server vastgelegde informatie te benaderen').
[230] Interview Openbaar Ministerie.
[231] Zie par. 5.1.2.

moeten maken om in te spelen op de verschuiving van gegevens van harde schijf naar cloud. Bij doorzoekingen zal men zich, meer dan momenteel al gebeurt, moeten richten op onderzoek van geactiveerde computers, om het werkgeheugen en openstaande verbindingen (bijvoorbeeld met clouddiensten) veilig te stellen. De klassieke doorzoeking en de klassieke (spraaktelefonische) tap zullen geleidelijk aan plaats moeten maken voor meer Internettaps, waar praktijk en wetgeving momenteel nog niet goed op zijn ingespeeld.[232]

Naast knelpunten in de opsporing ontstaan mogelijk ook knelpunten in de vervolging, wanneer bewijs 'uit de cloud' afkomstig is waarvan de betrouwbaarheid betwist kan worden in de rechtszaal. Procedures en standaarden voor bewijsvergaring uit de cloud zijn nog in een vroeg stadium van ontwikkeling en nog niet getoetst in de rechtspraktijk. Materiaal dat op verzoek of vordering van buitenlandse cloudaanbieders wordt verkregen, kent technische en enigermate ook juridische risico's voor gebruik als bewijs. Technisch is het niet eenvoudig bewijsbaar, gezien de gedistribueerde en geautomatiseerd-dynamische opslag, dat een document dat uit de cloud wordt gehaald hetzelfde is als dat wat erin is gestopt. Het zal niet altijd duidelijk zijn welke forensische procedures de cloudaanbieder gehanteerd heeft om het document te verkrijgen; momenteel ontbreken vaak ook technische voorzieningen in de cloudinfrastructuur die voor forensisch onderzoek nodig zijn (zoals logs en *audit-trails*). Juridisch kan bewijs dat uit het buitenland wordt verkregen als zodanig worden gebruikt. , maar in sommige situaties – als de verdediging de toelaatbaarheid of betrouwbaarheid betwist – zal de officier van justitie de rechtmatigheid en betrouwbaarheid van cloudbewijs nader moeten motiveren.

7.1.3. Kansen voor opsporing en vervolging

Onze geïnterviewden en respondenten zien aanzienlijk meer bedreigingen voor opsporing en vervolging dan kansen. Op drie vlakken liggen er echter mogelijk kansen. De belangrijkste is dat door de migratie van gegevens van de harde schijf van verdachte naar de cloud er in potentie meer gegevens binnen bereik komen om heimelijk te onderzoeken, voordat de verdachte via een doorzoeking wordt gealerteerd op het feit dat er een opsporingsonderzoek loopt. Met een Internettap of gegevensbevraging (met oplegging van geheimhouding) bij de cloudaanbieder kunnen nu ook gegevens worden vergaard die vroeger alleen via een doorzoeking en onderzoek van de harde schijf in beeld kwamen. Hierdoor kan het vooronderzoek langer doorlopen, wat bij bepaalde onderzoeken tactische voordelen zal hebben. Dit biedt mogelijk compensatie voor het verlies aan onderzoek 'op locatie' en de moeilijkheden van grensoverschrijdende toegang tot gegevens die hierboven als knelpunten zijn geschetst. Maar deze kans kan alleen worden benut als de knelpunten ten aanzien van cloudopsporing, in elk geval rond de Internettap en de 'locatiegerichte' opsporingspraktijk, worden aangepakt.

De andere vlakken waarop potentiële kansen bestaan liggen in de rekencapaciteit van de cloud, die zou kunnen worden benut om bijvoorbeeld versleutelde bestanden te kraken, en in de opslagcapaciteit van de cloud, die een kostenefficiënte oplossing zou kunnen bieden voor de grote hoeveelheden data die de politie bewaart. Het gebruiken van rekencapaciteit betreft een relatief klein onderdeel van de politiepraktijk en zou zonder veel obstakels kunnen worden uitgevoerd, maar het benutten van cloudopslagcapaciteit voor politiegegevens is een complex vraagstuk dat nadere reflectie vergt. Voorstanders van cloudopslag, met kostenbesparing als belangrijkste argument, geven aan dat clouddiensten vanzelfsprekend alleen gebruikt mogen worden als zij adequaat beveiligd zijn. Ook als de cloudaanbieder zelf de beveiliging goed op orde heeft, blijven beveiligingsrisico's (met name rond omgang met wachtwoorden en sleutels) bestaan aan de kant van de politie. Het vergt daarom nader onderzoek en een complexe beleidsafweging of de mogelijke kostenbesparing opweegt tegen de (afbreuk)risico's van cloudopslag van politiegegevens.

7.2. Oplossingsrichtingen

Op basis van dit onderzoek kunnen diverse suggesties worden gedaan voor wetgeving, beleid en praktijk om de genoemde knelpunten aan te pakken. Voor de **wetgever** geeft de cloud aanleiding om nog eens goed de systematiek van het materiële en procedurele strafrecht te doordenken in relatie tot Internetaanbieders. Het Wetboek van Strafrecht en het Wetboek van Strafvordering hanteren veelal het begrip aanbieder van een communicatiedienst, maar daarnaast wordt ook het

[232] Zie par. 5.1.3.

begrip aanbieder van een telecommunicatiedienst gebruikt (in art. 54a, 273d, 371 Sr, art. 125la Sv). Men kan zich afvragen of in het huidige ICT-landschap een onderscheid in rechtsbescherming tussen deze twee typen diensten gerechtvaardigd is, maar vooral ook hoe de opkomst van cloudaanbieders moet worden geduid in deze termen. Zowel ten aanzien van cloudopslagaanbieders als ten aanzien van cloudplatform- en infrastructuuraanbieders zal de wetgever (of de rechter) de reikwijdte van het begrip (tele)communicatieaanbieder nader moeten duiden.

Daarbij moet een tweede aspect worden betrokken, namelijk het in de systematiek van strafvordering gemaakte onderscheid tussen opslag en overdracht van gegevens. Bij veel cloudtoepassingen lijkt er eerder sprake te zijn van een mengvorm van beide: communicatie via de cloud (dus overdracht) wordt veelal langdurig opgeslagen, terwijl gegevens die in de cloud worden opgeslagen voortdurend in beweging kunnen zijn en daarbij onder de definitie van communicatie zouden kunnen vallen. Dit roept vragen op over het regime dat justitie moet toepassen om gegevens uit de cloud te verkrijgen: een vordering tot gegevensverstrekking (voor opgeslagen gegevens) of een tap (voor stromende gegevens)? Het onderscheid tussen opslag en overdracht van gegevens hangt voorts samen met de reikwijdte van het grondwettelijke (tele)communicatiegeheim, waarbij de wetgever de inhoud van (tele)communicatie zwaarder beschermt dan andere typen gegevens. De opkomst van cloud computing roept de vraag op of opslag van gegevens in de cloud aanspraak moet kunnen maken op hetzelfde niveau van rechtsbescherming als communicatie; bij cloudopslag zal er niet altijd sprake zijn van communicatie, terwijl er wel vergelijkbare kwetsbaarheden bestaan doordat private gegevens aan Internet-intermediairs worden toevertrouwd. Tezamen met de definitievragen rond (tele)communicatieaanbieders levert dit voldoende aanleiding op om de systematiek van het materiële en procedurele strafrecht eens grondig onder de loep te nemen in relatie tot de nieuwe vormen van gegevensverkeer die de cloud met zich meebrengt. Ook zou de grondwetgever bij de herziening van art. 13 Gw de rol van clouddiensten moeten meenemen wanneer hij het object en de reikwijdte van het (tele)communicatiegeheim opnieuw inkadert.

Verder zou de wetgever zich moeten buigen over de adequaatheid van sommige opsporingsbevoegdheden om gegevens uit de cloud te vergaren. De netwerkzoeking (art. 125j Sv) is momenteel gekoppeld aan een doorzoeking. Met de opkomst van mobiel Internet kan de cloud worden benaderd van willekeurig welke plaats. Niet alleen gegevens van de computer thuis migreren naar de cloud, maar ook gegevens die de verdachte bij zich draagt (zoals een agenda of adresboekje). Dit roept de vraag op of de netwerkzoeking niet ook mogelijk zou moeten zijn in gevallen waarin de politie een computer (mobiele telefoon, draagbare computer, tablet) in beslag neemt buiten een doorzoeking om, bijvoorbeeld bij aanhouding. Tegelijkertijd kan men zich afvragen of het huidige onderscheid in rechtsbescherming tussen voertuigen, plaatsen en woningen (art. 96b, 96c, 97/110 Sv) nog terecht is wanneer gegevens vanaf elke plaats toegankelijk zijn. Is het te rechtvaardigen dat elke opsporingsambtenaar een netwerkzoeking kan doen in de cloud vanuit een in een auto aangetroffen Internettelefoon (op basis van art. 96b j^{o} 125j Sv), terwijl voor een netwerkzoeking vanuit een thuis-pc in dezelfde cloud toestemming nodig is van de rechter-commissaris (ex art. 97/110/125i j^{o} 125j Sv)? Wanneer de gegevenshuishouding van burgers (denk aan administratie, foto's, muziek) langzaamaan migreert van thuiscomputers naar de cloud, verdient het aanbeveling om de rechtsbescherming voor deze gegevens tegen kennisneming door de overheid mee te laten migreren naar het niveau dat geldt voor in de woning te vinden informatie.

Naast de netwerkzoeking – die van beperkte waarde zal zijn voor de cloud zolang de territoriale begrenzing blijft bestaan – is het ook belangrijk voor de wetgever om de juridische knelpunten rond de Internettap (betreffende onder andere verbalisering, geheimhoudergegevens en selectie vooraf)[233] aan te pakken, nu het belang van de Internettap zal toenemen door de opkomst van de cloud. Daarbij komt dat het vaker zal voorkomen dat een doorzoeking weinig oplevert als gegevens in de cloud liggen opgeslagen en de politie, om diverse redenen (zoals een niet-meewerkende cloudaanbieder of een stroperige rechtshulpgang), niet in staat is om de gegevens uit de cloud te verkrijgen. Daarmee maakt de cloud de reeds bestaande vraag prangender of, en zo ja onder welke voorwaarden, een bevoegdheid tot heimelijke toegang op afstand ('hacken' door plaatsing van een afluisterprogrammaatje) zou moeten worden ingevoerd.

[233] Odinot e.a. 2012.

Voor het **beleid** ligt er ten eerste de uitdaging om crimineel misbruik van de cloud vanuit Nederland tegen te gaan. Dat past in het bestaande beleid rond de aanpak van cybercrime, waarin verschuivingen in (cyber)criminaliteit worden gemonitord en waar mogelijk gepareerd. Idealiter vindt de bestrijding van cloudcriminaliteit op internationaal niveau plaats, maar vanwege nationale verschillen en beperkte supranationale bevoegdheden in criminaliteitsbestrijding zal Nederland ook zoveel mogelijk zelfstandig moeten doen. De doelstelling zou moeten zijn om barrières op te werpen die het plegen van cloudcriminaliteit in en vanuit Nederland moeilijker maken. Weliswaar treedt dan een waterbedeffect op waarbij de criminaliteit verplaatst naar andere landen, maar door – samen met landen als de VS, het VK en Duitsland – als voorloper op te treden, kan Nederland bewerkstelligen dat de criminaliteit niet alleen verplaatst maar uiteindelijk ook moeilijker wordt om te plegen.[234] Voor cybercriminaliteit, inclusief de mogelijkheden die de cloud daarvoor biedt, zou daarom een barrièremodel kunnen worden ontwikkeld, zoals dat reeds bestaat voor kinderpornografie en in ontwikkeling is voor diverse andere vormen van criminaliteit.[235] Een barrièremodel bestaat uit diverse stappen die misdadigers zetten voor het plegen van (cloudgerelateerde) cybercriminaliteit, met per stap interventiemogelijkheden gericht op de misdadiger, burgers en bedrijven, Internetaanbieders en overheid.[236] Een waardevolle strategie zou daarbij kunnen zijn om vooral in te zetten op het aanpakken van de computergenieën in plaats van de bazen binnen georganiseerde cybercriminaliteit, waarmee de georganiseerde cybermisdaad sneller vleugellam gemaakt zou kunnen worden.[237]

In de tweede plaats is het belangrijk dat er wordt geïnvesteerd in samenwerking, zowel met buitenlandse overheden als met cloudaanbieders. Het verkrijgen van gegevens uit de cloud is immers voor een belangrijk deel afhankelijk van supranationale of multilaterale rechtshulpverdragen en van medewerking van cloudaanbieders. Er vindt reeds in Europees verband overleg plaats met grote cloudaanbieders om een aanspreekpunt binnen de EU te hebben voor nationale autoriteiten van EU-lidstaten.[238] Dergelijk overleg en verdere stroomlijning van procedures rond (rechtshulp)verzoeken is van wezenlijk belang voor opsporing in de cloud.

De vraag daarbij is wel of het klassieke model om alles via rechtshulp te laten verlopen, nog goed werkt in een cloudomgeving. De cloud versterkt immers, zoals hierboven aangegeven, het theoretische perspectief van de ‘cybernauten’ boven dat van de ‘territorialisten’, wat tot nadere reflectie noopt op de rol van soevereiniteit bij de opsporing van strafbare feiten. Mede vanwege de moeilijke bepaalbaarheid van de locatie van gegevens in de cloud, alsook omdat opsporing in de cloud soms om snelle actie vraagt waarvoor rechtshulp – hoe gestroomlijnd ook – te traag kan zijn, zijn er goede argumenten om een grensoverschrijdende netwerkzoeking toe te staan. Het Belgische model, om onder bepaalde voorwaarde een doorzoeking uit te breiden tot netwerkverbindingen over de grens met aansluitend notificatie aan de desbetreffende staat, kan daarbij als inspiratie dienen. Vanzelfsprekend geldt daarbij het beginsel van reciprociteit: als Nederland grensoverschrijdend wil netwerkzoeken, zal het ook moeten toestaan dat andere landen in Nederlandse servers gaan zoeken.[239] Dat past bij een moderne invulling aan soevereiniteit in een genetwerkte wereld:

> ‘By becoming enrolled and enmeshed in global government networks, individual government institutions would affirm their judicial, legislative, or regulatory sovereignty. (…) If sovereignty were still understood as exclusive and impermeable rather than relational, strengthening the state would mean building higher walls to protect its domestic authority. But in a world in which sovereignty means the capacity to participate in cooperative regimes in the collective interest of all states, expanding the formal capacity of different state institutions to interact with their counterparts around the world means expanding state power.’[240]

---

[234] Interview KLPD.
[235] Zie *Kamerstukken II* 2011/12, 31 015, nr. 77 (bijlage) (kinderpornografie), 29 628 , nr. 318 (bijlage) (woninginbraken), 33 000 VI, nr. 103 (internationale misdrijven); *Justitiële Verkenningen* 2011 nr. 2 (preventie van georganiseerde misdaad).
[236] Vgl. Katyal 2001.
[237] Interview Fox-IT.
[238] Interview KLPD.
[239] Vgl. Seitz 2004.
[240] Slaughter 2004, p. 326-327. Vgl. AIV 2012, p. 11-12: ‘De soevereiniteitsdiscussie kan samengevat worden als een afweging tussen het vergroten van het handelingsvermogen en het behoud van de vrijheid van handelen. De AIV meent dat de moderne interpretatie van het begrip soevereiniteit gehanteerd moet worden’, aansluitend op

In het verlengde hiervan zou Nederland ook een standpunt moeten bepalen over het al dan niet rechtstreeks kunnen bevragen van cloudaanbieders. Dat gaat een stap verder dan samenwerking tussen autoriteiten en opsporingsdiensten onderling, waar het citaat over moderne soevereiniteit betrekking op heeft. Het beleid zou kunnen verkennen onder welke voorwaarden het ook toelaatbaar zou kunnen zijn voor justitie om zich rechtstreeks te wenden tot buitenlandse aanbieders in plaats van via de weg van rechtshulp (wederom op basis van reciprociteit). Daarbij zou Nederland ook een standpunt moeten bepalen ten aanzien van geheimhouding van gegevensopvraging bij cloudaanbieders: het ligt voor de hand dat de Nederlandse justitie de wettelijke basis van geheimhoudingsplicht (art. 126bb lid 5 Sv) ook ten aanzien van buitenlandse aanbieders wil handhaven in het kader van het opsporingsbelang, maar dat zou betekenen dat bevragingen van buitenlandse autoriteiten bij Nederlandse aanbieders ten aanzien van Nederlandse burgers en bedrijven dan ook geheim blijven, wat vanuit het oogpunt van rechtsbescherming misschien niet altijd wenselijk is.

Een derde veld waarop het beleid zich zou moeten richten is de verhoging van beveiliging van cloud computing. Kwetsbaarheden van de cloud die criminaliteit in de hand werken, zoals aanvallen op opgeslagen informatie en het kunnen plegen van botnetaanvallen, kunnen binnen de perken worden gehouden door adequate informatiebeveiligingspraktijken. Het stimuleren daarvan past binnen het bredere beleid rond cybersecurity, zeker wanneer de cloud meer het karakter krijgt van een vitale infrastructuur als burgers, bedrijven en overheidsinstanties belangrijke gegevensprocessen in substantiële mate zouden gaan verplaatsen naar de cloud. Beveiliging van de cloud zou dan ook op de agenda moeten staan van de Nationale Cyber Security Raad, zowel voor wat betreft het (op internationaal niveau) stimuleren van beveiligingsmaatregelen bij cloudaanbieders als voor wat betreft bewustzijn en beveiligingsmaatregelen aan de kant van Nederlandse cloudconsumenten.[241]

Ten vierde kan het beleid de opsporingspraktijk ondersteunen in het leren omgaan met cloudopsporing, door kennis en vaardigheden te stimuleren op de werkvloer rond onder andere het in beslag nemen en onderzoeken van computers in geactiveerde toestand en het omgaan met Internettaps.

Voor de **praktijk** ligt er, naast het beter leren omgaan met computerdoorzoekingen en Internettaps, vooral de uitdaging om een weg te vinden in de omgang met bestaande bevoegdheden en de beperkingen daarvan, zolang de juridische knelpunten – waaronder de territoriale begrenzing – niet zijn opgelost. Over het algemeen zal justitie de koninklijke weg van rechtshulp moeten blijven bewandelen, maar er zullen zich gevallen voordoen waarin dat een te lange, of zelfs een doodlopende, weg zal zijn. In die gevallen zou de praktijk kunnen experimenteren met niet-koninklijke maatregelen, zoals in het recente verleden bijvoorbeeld gebeurd is met de ontmanteling van het Bredolab-botnet[242] en het verwijderen van kinderporno van buitenlandse Tor-servers.[243] Wanneer dat gebeurt, is het belangrijk om daarover transparant te zijn en verantwoording af te leggen (zoals in beide genoemde zaken is gebeurd), zodat de activiteit in rechte getoetst kan worden. Een complicatie daarbij is wel dat dergelijke niet-koninklijke opsporingsactiviteiten niet altijd voor de rechter komen en dus niet feitelijk worden getoetst, wat vanuit het oogpunt van zowel rechtsbescherming als rechtsontwikkeling te betreuren valt. Het is daarom wenselijk dat, wanneer het Openbaar Ministerie in een dringende situatie besluit een grensoverschrijdende netwerkzoeking in de cloud toe te staan om gegevens veilig te stellen (met notificatie aan de buitenlandse staat achteraf), tot vervolging overgaat en de

---

Slaughter's interpretatie van nieuwe soevereiniteit die 'wordt bepaald door de capaciteit van een staat om effectief samen te werken in internationale fora en met gezag te participeren in internationale netwerken.' Vgl. ook onze buitenlandse respondenten: 'The impact of cloud computing on crimes and investigations will be devastating, especially in terms of investigations. We must change mentality in terms of digital forensics and try to encourage (maybe by updating the 2001 cybercrime convention) greater collaboration during cross-border investigations' (NN, reactie op enquête); 'Le type de criminalité qui se développe sur Internet, en particulier par le cloud computing, ne peut être combattu que par un renforcement de la coopération internationale en matière judiciaire. A cet égard, on ne peut que regretter que la Convention sur la Cybercriminalité du 23.11.2001 n'autorise pas la perquisition informatique à distance sans l'accord du prévenu' (Yves Nicolet, reactie op enquête).

[241] Vgl. Choo 2010, p. 4-5, die de noodzaak van een integraal beleid rond cloudbeveiliging benadrukt in de vorm van het stimuleren van een 'culture of security'.

[242] Zie Koning 2012, p. 47.

[243] Zie par. 5.2.4.

netwerkzoeking – ook als het alleen sturingsinformatie en niet direct bewijsmateriaal oplevert – in het dossier meldt. Dat levert mogelijk een zeker procesrisico op, maar dat lijkt een aanvaardbaar risico in het licht van de huidige jurisprudentie over de Schutznorm, die bepaalt dat bewijsmateriaal niet hoeft te worden uitgesloten indien de bepaling die is geschonden (bij onrechtmatig verkregen bewijs) een ander belang dient dan dat van de verdachte.[244] De beperking van de netwerkzoeking tot de landsgrens dient het belang van de soevereiniteit van andere staten en niet het privacybelang van burgers; het is daarom denkbaar dat een grensoverschrijdende netwerkzoeking, ook bij afwezigheid van toestemming door de desbetreffende buitenlandse staat, door de rechter 'weggeschutznormd' wordt. Hetgeen natuurlijk niet het belang wegneemt voor wetgever en beleidsmakers om in supranationaal verband te komen tot een betere regeling van de netwerkzoeking in het tijdperk van cloud computing.

Alles overziend kunnen we concluderen dat cloud computing vooralsnog meer knelpunten dan kansen oplevert voor de opsporing en vervolging van strafbare feiten. Als wetgeving, beleid en praktijk echter in staat zijn de handschoen op te pakken en een nieuwe, systematische en uitgebalanceerde regeling en praktijk te ontwerpen voor opsporing in de cloud, kan van deze nood een deugd worden gemaakt. Vroeg of laat zullen ook de strafrechtelijke rechtsleer en rechtspraktijk in een ICT-samenleving moeten leren leven met het verlies van locatie. Dat kan maar beter vroeg dan laat zijn.

[244] Zie par. 6.2.

Bijlagen

1. Lijst geïnterviewde personen en respondenten

Interviews

KLPD	Peter Zinn	adviseur Team High Tech Crime
	Frank Bernaards	beleidsmedewerker Team High Tech Crime
politie Oost-Nederland	Frans Kolkman	hoofd High Tech Crime Unit
Openbaar Ministerie	Lodewijk van Zwieten	landelijk officier van justitie cybercrime
Fox-IT	Ronald Prins	technisch directeur
Rabobank Nederland	Wim Hafkamp	hoofd strategie en beleid, afdeling Informatie Risico Management
	Hein Laan	adviseur informatiebeveiliging

Buitenlandse respondenten

België	Philippe van Linthout	onderzoeksrechter, Rechtbank van Eerste Aanleg te Mechelen
Duitsland	Gerrit Hornung	Professor of Public Law, IT Law and Legal Informatics, University of Passau
	Judge Buermeyer	Berlin High Court (Landgericht Berlin)
Italië	Lorenzo Picotti	Professor of Criminal Law, Business Criminal law and Criminal Information Law, University of Verona
	Ivan Salvadori	Research associate in Criminal Law and Criminal Information Law, University of Verona
	NN	advocaat[245]
Letland	Uldis Kinis	Associate professor of Law, Riga Stradins University
	Baiba Kaškina	Director of CERT.LV
Spanje	Fredesvinda Insa	Strategic Development Manager, CFLabs
Verenigd Koninkrijk	Stephen Mason	advocaat te Londen
	Ian Walden	Professor of Information and Communications Law, Centre for Commercial Law Studies, Queen Mary, University of London
Verenigde Staten	Susan W. Brenner	NCR Distinguished Professor of Law & Technology, University of Dayton School of Law
Zweden	Jonas Ekfeldt	Doctoral candidate in Law and ICT, Stockholm University
Zwitserland	Yves Nicolet	Procureur, Ministère public central, Division entraide, criminalité économique et informatique

[245] Deze respondent heeft verzocht naamsvermelding achterwege te laten aangezien informatie is verkregen uit (deels lopende) zaken waarvoor vertrouwelijkheid noodzakelijk is.

2. Samenstelling begeleidingscommissie

prof.mr. A.R. Lodder (voorzitter)	Vrije Universiteit Amsterdam
drs. R.C. Besemer	ministerie van Veiligheid en Justitie / DGRR
drs. F. Willemsen	ministerie van Veiligheid en Justitie / WODC

3. Literatuurlijst

AIV (Adviesraad Internationale Vraagstukken) (2012), *Europese defensiesamenwerking. Soevereiniteit en handelingsvermogen*, Advies nr. 78, januari 2012.

Article 29 Working Party (2012), *Opinion 05/2012 on Cloud Computing*, WP196, 1 July 2012.

Bergman, Michael K. (2001), 'The Deep Web: Surfacing Hidden Value', *The Journal of Electronic Publishing* 7 (1).

Biggs, S. & S. Vidalis (2010), 'Cloud Computing Storms', *International Journal of Intelligent Computing Research* 1 (1/2), p. 61-68.

Birk, Dominik (2011), 'Technical Challenges of Forensic Investigations in Cloud Computing Environments', Workshop on Cryptography and Security in Clouds, Zurich, 15-16 March 2011, http://www.zurich.ibm.com/~cca/csc2011/submissions/birk.pdf.

Birk, Dominik, Dennis Heinson & Christoph Wegener (2011), 'Virtuelle Spurensuche. Digitale Forensik in Cloud-Umgebungen', *Datenschutz und Datensicherheit* (5), p. 329-332.

Brenner, S. & B.J. Koops (2004), 'Approaches to Cybercrime Jurisdiction', *Journal of High-Technology Law* 4(1), p. 1-46.

Brenner, S.W. (2006), 'The Next Step: Prioritizing Jurisdiction', in: B.J. Koops & S.W. Brenner (eds.), *Cybercrime and Jurisdiction. A Global Survey*, The Hague: TMC Asser Press, p. 327-349.

Catteddu, D. & G. Hogben (2009), *Cloud computing: Benefits, risks and recommendation for information security*, European Network and Information Security Agency (ENISA).

Cavoukian, Ann (2008), 'Privacy in the Clouds', *Identity in the Information Society* 1, DOI 10.1007/s12394-008-0005-z.

Chaabane, A., P. Manils & M.A. Kaafar (2010), 'Digging into Anonymous Traffic: a deep analysis of the Tor anonymizing network', in: *NSS '10 Proceedings of the 2010 Fourth International Conference on Network and System Security,* IEEE Computer Society, Washington, DC.

Chen, Yanpei, Paxson, Vern & Katz, Randy H. (2010), *What's new about cloud computing security*, Technical report no. UCB/EECS-2010-5, University of California at Berkeley, 20 January 2010.

Choo, Kim-Kwang Raymond (2010), 'Cloud computing: challenges and future directions', *Trends & issues in crime and criminal justice* No. 400, Canberra: Australian Institute of Criminology, October 2010.

Clarke, Ian, Oskar Sandberg, Brandon Wiley & Theodore W. Hong (2001), 'Freenet: a distributed anonymous information storage and retrieval system', in: Hannes Federrath (ed.), *International workshop on Designing privacy enhancing technologies: design issues in anonymity and unobservability*, New York: Springer-Verlag , p. 46-66.

Clarke, Ian, Oskar Sandberg, Matthew Toseland, Vilhelm Verendel (2010), 'Private Communication Through a Network of Trusted Connections: The Dark Freenet', paper submitted to PET 2010, https://freenetproject.org/papers/freenet-0.7.5-paper.pdf.

Cohen, B. (2003), 'Incentives Build Robustness in BitTorrent', in: *Proc. 1st Workshop on Economics of Peer-to-Peer Systems (P2PECON),* 2003.

Council of Europe (2008), *Guidelines for the cooperation between law enforcement and internet service providers against cybercrime*, adopted by the global Conference Cooperation against Cybercrime, 1-2 April 2008, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/Reports-Presentations/567_prov-d-guidelines_provisional2_3April2008_en.pdf.

Cuijpers, C., R.E. Leenes, S. Olislaegers & C. Stuurman (2011), *De wolk in het onderwijs*, rapport voor SURF, Tilburg: TILT.

Dabhur, Kamal, Bassil Mohammad & Ahmad Bisher Tarakji (2011), 'A Survey of Risks, Threats and Vulnerabilities in Cloud Computing', in: *Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications,* ACM, article 12.

De Hert, P. & F. Van Leeuw (2011), 'Internet Crimes', in: E. Dirix & Y.-H. Leleu (eds), *The Belgian Reports at the Congress of Washington of the International Academy of Comparative Law*, Brussels: Éditions Bruylant.

Dries, H., S.J.H. Gijrath & P.C. Knol (2003), *Openbaarheid van netwerken en diensten in de Telecommunicatiewet*, ITeR-deel 60, Den Haag: Sdu uitgevers.
Enschedé, C.J. (1988), *De burger en het recht. Over macht, gezag en democratie*, Amsterdam: Meulenhoff.
Forbes (2010), *Seeding the Cloud – Enterprises Set Their Strategies for Cloud Computing*, http://www.emc.com/collateral/analyst-reports/emc-seeding-the-cloud-forbes-report.pdf.
Fu, Xinwen, Zhen Ling, Wei Yu & Junzhou Luo (2010), 'Cyber Crime Scene Investigations (C^2SI) through Cloud Computing', *Proceedings of the 2010 IEEE 30th International Conference on Distributed Computing Systems Workshops*, ACM, p. 26-31.
Geist, Michael A. (2001), 'Is There a There There? Toward Greater Certainty for Internet Jurisdiction', *Berkeley Technology Law Journal* 16, p. 1345ff.
Goldschlag, D., M. Reed & P. Syverson (1999), 'Onion Routing for Anonymous and Private Internet Connections', *Communications of the ACM* 42(2), p. 39-41.
Goldsmith, Jack L. (1998), 'The Internet and the Abiding Significance of Territorial Sovereignty', *Indiana Journal of Global Legal Studies* 5, p. 475-491.
He, Bin, Mitesh Patel, Zhen Zhang & Kevin Chen-Chuan Chang (2007), 'Accessing the deep web - Attempting to locate and quantify material on the Web that is hidden from typical search techniques', *Communications of the ACM* 50 (5), p. 94-101.
Hendriks, A., E.M. Meershoek, C. Stuurman, N. Robinson & J. Cave (2012), *Cloud computing. Fundament op orde*, versie 1.1, Verdonck, Klooster & Associates, 7 februari 2012.
Herley, C. (2009), 'Economics and the underground economy', Black Hat USA, Las Vegas, 25-30 July 2009.
International Working Group on Data Protection in Telecommunications (2012), *Working Paper on Cloud Computing - Privacy and data protection issues - "Sopot Memorandum"*, 23-24 April 2012, Sopot, http://www.datenschutz-berlin.de/attachments/873/Sopot_Memorandum_Cloud_Computing.pdf?1335513083.
Jewkes, Y. & Yar, M. (2010), 'Introduction: the Internet, cybercrime, and the challenges of the 21st century', in: Y. Jewkes & M. Yar (eds.), *Handbook of Internet Crime*, Cullompton: Willan Publishing, p. 1-8.
Johnson, David R. & David G. Post (1996), 'Law and Borders – The Rise of Law in Cyberspace', *Stanford Law Review* 48, p. 1367-1402.
Katyal, Neal Kumar (2001), 'Criminal Law in Cyberspace', *University of Pennsylvania Law Review* 149 (4), p. 1003-1114.
Keustermans, J. & T. De Maere (2010), 'Tien jaar wet informaticacriminaliteit', *Rechtskundig Weekblad* 2010-11 (14), p. 562-568.
Koning, M.E. (2012), 'Van teugelloos "terughacken" naar "digitale toegang op afstand"', *Privacy & Informatie* (2), p. 46-52.
Koops, B.J. (2012a), 'Politieonderzoek in open bronnen op internet. Strafvorderlijke aspecten', *Tijdschrift voor veiligheid* 11 (2), p. 30-46.
Koops, B.J. (2012b), *Het decryptiebevel en het nemo-teneturbeginsel. Nopen ontwikkelingen sinds 2000 tot invoering van een ontsleutelplicht voor verdachten?*, Tilburg/Den Haag: TILT/WODC.
Koops, Bert-Jaap (2000), *Verdachte en ontsleutelplicht: hoe ver reikt nemo tenetur?*, ITeR-reeks deel 31, Deventer: Kluwer.
Koops, Bert-Jaap, Rudi Bekkers, Frank Bongers & Marieke Fijnvandraat (2005), *Aftapbaarheid van telecommunicatie. Een evaluatie van hoofdstuk 13 Telecommunicatiewet*, Tilburg, november 2005.
Locher, Thomas, Patrick Moor, Stefan Schmid, Roger Wattenhofer (2006), 'Free Riding in BitTorrent is Cheap', *Fifth Workshop on Hot Topics in Networks: HotNets V*, Beckman Center, UC Irvine, 29-30 November 2006, p 85-90.
Lodder, Arno R. (2012), *Recht rond cyberwar, het internet van dingen en andere internet (on)gemakken: de tien geboden van het internetrecht*, oratie VU Amsterdam.
Mansfield-Devine, Steve (2009), 'Darknets', *Computer Fraud and Security Report* (12), p. 4–6.
Meer, H, N. Arvanitis & M. Slaviero (2009), *Clobbering the cloud*, Black Hat USA, Las Vegas, 25-30 July 2009.
Mell, P. & T. Grance, 'The NIST Definition of Cloud Computing', Version 15, 7 October 2009, http://csrc.nist.gov/groups/SNS/cloud-computing/cloud- def-v15.doc.

Micozzi, Francesco Paolo (2011), 'La responsabilità penale del Cloud Service Provider', E-Privacy conference 2011, Firenze, 3 juni 2011, http://e-privacy.winstonsmith.org/2011/atti/e-privacy-2011-06-responsabilita_penale_del_cloud_serv_prov-micozzi.pdf.
Nationaal Cyber Security Centrum (2012), *Cybersecuritybeeld Nederland. CSBN-2*, Den Haag: NCSC, juni 2012.
Octopus Conference (2012), *Octopus 2012 – Key messages*, 11 June 2012, http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_Octopus2012/2571_Octo_key_messages_V5.pdf.
Odinot, G., D. de Jong, J.B.J. van der Leij, C.J. de Poot & E.K. van Straalen (2012), *Het gebruik van de telefoon- en internettap in de opsporing*, Onderzoek en beleid nr. 304, Meppel/Den Haag: Boom Lemma/WODC.
Oerlemans, J.J. (2011), 'Hacken als opsporingsbevoegdheid', Delikt & Delinkwent 62 (8), p. 888-908.
Oerlemans, J.J. (2012), 'Mogelijkheden en beperkingen van de internettap', *Justitiële Verkenningen* jrg. 38, nr. 3, p. 20-39.
Ristenpart, Thomas, Eran Tromer, Hovav Shacham & Stefan Savage (2009), 'Hey, You, Get Off of My Cloud!: Exploring Information Leakage in Third-Party Compute Clouds', in: Somesh Jha & Keromytis, Angelos (eds.), *Proceedings of CCS 2009*, New York: ACM Press, p. 199-212.
Ruan, Keyun Ibrahim Baggili, Joe Carthy & Tahar Kechadi (2011b), *Survey on cloud forensics and critical criteria for cloud forensic capability: A preliminary analysis*, ADFSL Conference on Digital Forensics, Security and Law, Richmond, VA, 25-27 May 2011, http://cloudforensicsresearch.org/publication/Survey_on_Cloud_Forensics_and_Critical_Criteria_for_Cloud_Forensic_Capability_6th_ADFSL.pdf.
Ruan, Keyun, Joe Carthy, Tahar Kechadi & Mark Crosbie (2011a), 'Cloud forensics: An overview', 7th IFIP International Conference on Digital Forensics, *Advances in Digital Forensics* Vol. 7, Springer, http://cloudforensicsresearch.org/publication/Cloud_Forensics_An_Overview_7th_IFIP.pdf.
Schwerha IV, Joseph J. (2010), *Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers"*, Council of Europe Project on Cybercrime Discussion Paper (Draft), 15 January 2010, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/Reports-Presentations/2079_reps_IF10_reps_joeschwerha1a.pdf.
Seitz, Nicolai (2004), 'Transborder Search: A new perspective in law enforcement?', *International Journal of Communications Law & Policy* (9), p. 1-18.
Spoenle, J. (2010), *Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?*, Council of Europe Project on Cybercrime Discussion Paper, 31 August 2010, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf.
Struiksma, N., C.N.J. De Vey Mestdagh & H.B. Winter (2012), *De organisatie van de opsporing van cybercrime door de Nederlandse politie*, Apeldoorn/Groningen: Politie & Wetenschap / Pro Facto.
Taylor, M., J. Haggerty, D. Gresty & R. Hegarty (2010), 'Digital evidence cloud computing systems', *Computer Law & Security Review* 26, p. 304-308.
Vaciago, Giuseppe (2011), *The Death Of Computer Forensics: Digital Forensics After the Singularity. Summary of the Workshop*, 2 May 2011, http://www.techandlaw.net/wp-content/uploads/2012/03/2011_05_02_Cloud_Forensics.pdf.
Vaciago, Giuseppe (2012), 'Cloud Computing and Data Jurisdiction: A New Challenge for Digital Forensics', *Cloud Computing and Data Jurisdiction: A New Challenge for Digital Forensics*, IARIA, p. 7-12.
Van der Hulst, R.C. & R.J.M. Neve (2008), *High-tech crime, soorten criminaliteit en hun daders - Een literatuurinventarisatie*, Den Haag: WODC.
Velasco, Cristos (2009), 'Jurisdictional Aspects of Cloud Computing', Octopus Interface Conference 2009, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20cristos%20cloud.pdf.

Vermeulen, Gert (2011), *Free gathering and movement of evidence in criminal matters in the EU. Thinking beyond borders, striving for balance, in search of coherence*, oratie Maastricht, Antwerpen etc.: Maklu.

Walden, Ian (2011), *Accessing data in the Cloud: The long arm of the Law Enforcement Agent*, Queen Mary School of Law Legal Studies Research Paper No. 74/2011, http://ssrn.com/abstract=1781067.