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

Dit is de samenvatting van een rapport geschreven in opdracht van het Ministerie van Veiligheid en Justitie. Het rapport, B.J. Koops, R. Leenes, P. De Hert & S. Olislaegers (2012), *Misdaad en opsporing in de wolken. Knelpunten en kansen van* cloud computing *voor de Nederlandse opsporing*, Tilburg/The Hague: TILT/ WODC, oktober 2012, is beschikbaar op http://www.wodc.nl/publicaties/.

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.