Normering van digitale opsporingsmethoden

J.J. Oerlemans

Nederlandse Defensie Academie (NLDA)
Faculteit Militaire Wetenschappen (FMW)
Postbus 90002
4800 PA Breda

Vormgeving
Bureau Multimedia NLDA

Druk
Bureau Repro, FBD Breda

ISBN: 978-90-88920-69-1

Voorwoord

Het gebruik van digitale opsporingsmethoden is noodzakelijk voor het vergaren van bewijs in cybercrimezaken. Ook in steeds meer traditionele opsporingsonderzoeken speelt digitaal bewijs een belangrijke rol. Kennis over de toepassing van digitale opsporingsmethoden en normering daarvan is schaars. Deze studie heeft als doel om een deel van deze kennis te verschaffen aan studenten en professionals die binnen de strafrechtsketen te maken krijgen met digitaal bewijs. Ik ben de Nederlandse Defensie Academie en in het bijzonder bgen. prof. dr. Paul Ducheine dankbaar voor het geven van de mogelijkheid deze *research paper* uit te brengen.

Deze studie is grotendeels gebaseerd op hoofdstuk 5 tot en met hoofdstuk 8 van mijn proefschrift '*Investigating Cybercrime*'.[1] Een belangrijke toevoeging ten opzichte van mijn proefschrift betreft de analyse van het Nederlands juridisch kader omtrent de inbeslagname en onderzoek van gegevens in computers.

In de komende jaren zal het juridisch kader omtrent de digitale bewijsgaring zich verder ontwikkelen. Binnen het project 'Modernisering Strafvordering' wordt de inbeslagname en onderzoek van gegevens in computers meegenomen. Dat zal leiden tot nieuwe regels omtrent het digitaal forensisch onderzoek binnen de strafrechtsketen.[2] Daarnaast wordt als onderdeel van het project ook de structuur van het Wetboek van Strafvordering gewijzigd.[3] Toch blijft de inhoud van de regels voor de toepassing van bijzondere opsporingsbevoegdheden (straks 'heimelijke bevoegdheden' genoemd) grotendeels hetzelfde.[4] Het ligt in de verwachting dat er in de komende jaren ook een aantal uitspraken zullen komen met betrekking tot de toepassing van digitale opsporingsmethoden. Daarnaast is het mogelijk dat het Openbaar Ministerie een meer actieve rol dan voorheen op zich zal nemen en via Aanwijzingen meer sturing zal geven aan het proces van digitale bewijsgaring. Tenslotte zullen technologische ontwikkelingen blijven voort denderen en hun invloed uitoefenen op de maatschappij. Deze technologische ontwikkelingen hebben ook invloed op criminaliteit en op het daarop volgende opsporingsproces.

De digitale bewijsgaring en het juridisch kader daaromtrent moeten constant worden geüpdatet om opsporingsinstanties de instrumenten te geven hun werk goed te kunnen doen en tegelijkertijd burgers afdoende bescherming te geven tegen misbruik van overheidsmacht en willekeur. De resultaten van deze studie zullen slechts een aantal jaar actueel blijven, maar in de tussentijd hopelijk enige richting geven aan de interpretatie van het juridisch kader omtrent digitale opsporingsmethoden.

Jan-Jaap Oerlemans
Leiden, januari 2017

1 Zie Oerlemans 2017. De dissertatie is op https://openaccess.leidenuniv.nl/handle/1887/44879 publiekelijk toegankelijk gesteld (laatst geraadpleegd op 2 januari 2017).
2 Zie het discussiestuk 'Onderzoek ter plaatse, inbeslagneming en doorzoeking en onderzoek van gegevensdragers en in geautomatiseerde werken' van 6 juni 2014.
3 Zie de contourennota van het project Modernisering Strafvordering van 30 september 2015. Beschikbaar op: https://www.rijksoverheid.nl/documenten/kamerstukken/2015/09/30/brief-aan-de-tweede-kamer-modernisering-wetboek-van-strafvordering-plus-contourennota (laatst geraadpleegd op 2 januari 2017). De genoemde artikelnummers in deze studie zullen wijzigen als de voorstellen worden aangenomen.
4 Zie Ölçer 2015 voor een overzicht van de huidige plannen met betrekking tot bijzondere opsporingsbevoegdheden.

Inhoudsopgave

Voorwoord **5**

Lijst van afkortingen **9**

1 Introductie **11**
1.1 Beperkingen van de scope van het onderzoek 11
1.2 Methodologie 12
1.3 Structuur 12

2 Vergaren van publiekelijk toegankelijke online gegevens **15**
2.1 Definitie 15
2.2 Handmatig vergaren van online gegevens 15
2.2.1 Juridische basis voor de opsporingsmethode 18
2.2.2 De Wet politiegegevens 19
2.3 Automatisch vergaren van online gegevens 20
2.4 Observatie op internet 22
2.5 Slotbeschouwing 24

3 Online undercover opsporingsmethoden **27**
3.1 Achtergrond regulering undercover opsporingsmethoden 28
3.2 Online pseudokoop 30
3.3 Online undercover interacties met individuen 31
3.3.1 Juridische basis 31
3.3.2 De Context-zaak 31
3.3.3 De lokpuber 32
3.4 Online infiltratieoperaties 33
3.4.1 Juridische basis 34
3.4.2 Infiltreren in een online drugsforum 34
3.5 Slotbeschouwing 35

4 Inbeslagname en onderzoek van gegevens in computers **37**
4.1 Computers als voorwerp ter inbeslagname 37
4.1.1 Inbeslagname tijdens de doorzoeking 38
4.1.2 Gebrek aan een procedure voor onderzoek in computers 39
4.2 Bijzondere bescherming voor computers 39
4.3 De netwerkzoeking 40
4.3.1 Reikwijdte van de netwerkzoeking 41
4.3.2 Grensoverschrijdende netwerkzoeking 42
4.4 Slotbeschouwing 43

5 Vorderen van gegevens bij online serviceproviders 45
5.1 Het belang van gegevens bij online serviceproviders 45
5.1.1 Gegevens bij breedband internetproviders 45
5.1.2 Gegevens bij anonimiseringsdienstverleners 46
5.1.3 Gegevens bij andere online serviceproviders 48
5.2 Wetssystematiek vorderen van gegevens 48
5.3 Vorderen van gebruikersgegevens 49
5.4 Vorderen van verkeersgegevens 49
5.5 Vorderen van 'andere gegevens' 50
5.6 Vorderen van inhoudelijke gegevens 51
5.7 Slotbeschouwing 52

6 Hacken als opsporingsmethode 55
6.1 Aanleiding tot normering van hacken als opsporingsmethode 55
6.1.1 Beoogde oplossing voor problematiek binnen de opsporing 55
6.1.2 Inhoud van de nieuwe bevoegdheid 57
6.2 De doorzoeking op afstand 58
6.3 Het gebruik van policeware 59
6.4 Het ontoegankelijk maken van gegevens 60
6.5 Slotbeschouwing 61

Literatuurlijst 63

Over de auteur 69

Lijst van afkortingen

AmvB	-	Algemene Maatregel van Bestuur
BOB	-	Bijzondere opsporingsbevoegdheden
CBP	-	College Bescherming Persoonsgegevens (thans: Autoriteit Persoonsgegevens)
CTC	-	Centrale Toetsingscommissie
DDoS	-	Distributed Denial of Service
EHRM	-	Europees Hof voor de Rechten van de Mens
EVRM	-	Europees Verdrag voor de Rechten van de Mens
FBI	-	Federal Bureau of Investigation
HR	-	Hoge Raad
HvJ EU	-	Hof van Justitie van de Europese Unie
I2P	-	The Invisible Internet Project
IP	-	Internet Protocol
IRT	-	Interregionaal Recherche Team
MvT	-	Memorie van Toelichting
OSINT	-	Open source intelligence
Polw	-	Politiewet
Rb.	-	Rechtbank
Stb.	-	Staatsblad
Stcrt.	-	Staatscourant
Sr	-	Wetboek van Strafrecht
Sv	-	Wetboek van Strafvordering
Tor	-	The Onion Routing
Trb.	-	Tractatenblad
VoIP	-	Voice-over-IP
VPN	-	Virtual Private Network
Wpg	-	Wet politiegegevens

1 Introductie

Op 20 december 2016 is de Wet computercriminaliteit III door de Tweede Kamer aangenomen. De verwachting is dat de Wet computercriminaliteit III uiteindelijk ook door de Eerste Kamer wordt aangenomen en in 2017 wordt bekrachtigd. Het meest in het oog springende voorstel is om 'hacken als opsporingsmethode' in het Wetboek van Strafvordering te reguleren. De bijzondere opsporingsbevoegdheid zou noodzakelijk zijn om de problemen van anonimiteit, versleuteling en *cloud computing* binnen de opsporing het hoofd te bieden.[5]

De nieuwe bevoegdheid biedt in bepaalde omstandigheden inderdaad nieuwe opsporingsmogelijkheden. Wel gelden strenge voorwaarden voor de toepassing van de opsporingsbevoegdheid, waaronder een interne toetsing van de Centrale Toetsingscommissie (CTC) binnen het Openbaar Ministerie. Door deze strenge voorwaarden ligt het niet voor de hand dat de opsporingsmethode op grote schaal wordt toegepast. Bovendien vergt de toepassing van de opsporingsbevoegdheid schaars beschikbare technische expertise en zijn niet alle typen computers eenvoudig te hacken omdat ze bepaalde software en besturingssystemen hebben.

In deze studie wordt naast hacken als opsporingsmethode (hoofdstuk 6), ook de juridische basis voor andere digitale opsporingsmethoden besproken. Het gaat daarbij om het vergaren van publiekelijk toegankelijke online informatie (hoofdstuk 2), online undercover opsporingsmethoden (hoofdstuk 3), de inbeslagname en onderzoek van gegevens in computers (hoofdstuk 4) en het vorderen van gegevens van online serviceproviders (hoofdstuk 5). Niet alleen zijn deze opsporingsmethoden eenvoudiger en onder minder strenge voorwaarden toe te passen dan hacken als opsporingsmethode, zij vormen ook belangrijke instrumenten bij het vergaren van bewijs in een digitale context. Het doel van deze studie is om studenten en professionals binnen het werkveld van digitale opsporing kennis te verschaffen over de regulering van digitale opsporingsmethoden.

1.1 Beperkingen van de scope van het onderzoek

Deze studie beperkt zich tot een analyse van opsporingsmethoden die kunnen worden toegepast binnen een opsporingsonderzoek. Een opsporingsonderzoek vangt meestal aan bij een redelijk vermoeden van schuld bij een strafbaar feit.[6] Bij misdrijven die in georganiseerd verband worden gepleegd, is het mogelijk een opsporingsonderzoek te starten bij betrokkenheid van het plegen van misdrijven in georganiseerd verband.[7] Ten slotte is het ook mogelijk bij aanwijzingen van terroristische misdrijven een opsporingsonderzoek te starten en bijzondere opsporingsbevoegdheden in te zetten.[8] Telkens noem ik alleen de juridische basis van de genoemde opsporingsmethode onderzocht bij toepassing in klassieke opsporingsonderzoeken (bij een redelijk vermoeden van schuld).

5 Zie *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT Wet Computercriminaliteit III), p. 21-31.
6 Zie art. 27 Sv.
7 Zie Titel V van het Wetboek van Strafvordering.
8 Zie Titel VB van het Wetboek van Strafvordering.

Het gebruik van *datamining*, of daaraan gerelateerd *bigdata*-onderzoek, is een opsporingsmethode die sterk in opkomst is.[9] Tot nu toe wordt deze opsporingsmethode gereguleerd buiten het Wetboek van Strafvordering. Deze opsporingsmethode valt dan ook buiten de scope van het onderzoek. Het is echter wel een opsporingsmethode die in de nabije toekomst wellicht strenger zal worden gereguleerd.

De beperking tot het analyseren van de juridische basis van opsporingsmethoden binnen het Wetboek van Strafvordering brengt ook met zich mee dat slechts de toepassing van opsporingsmethoden door opsporingsambtenaren (meestal werkzaam bij de Nationale Politie) wordt behandeld. Regels met betrekking tot opsporingsmethoden die worden ingezet door ambtenaren van bestuursorganen (zoals gemeenten en toezichthouders) of private organisaties (zoals werknemers van beveiligingsafdelingen van grote bedrijven en particuliere recherchebureaus), vallen buiten deze studie.

1.2 Methodologie

De onderzoeksmethodologie in deze studie komt overeen met de gebruikte methodologie uit mijn proefschrift '*Investigating Cybercrime*'.[10] Voor het proefschrift is gebruikgemaakt van de volgende onderzoeksmethoden: (1) een literatuurstudie, (2) het afnemen van veertien semigestructureerde interviews met experts op het gebied van cybercrime en digitale opsporing en (3) een dossieronderzoek met betrekking tot tien cybercrimezaken.[11]

1.3 Structuur

In deze studie worden zes opsporingsmethoden elk in een apart hoofdstuk behandeld.

In hoofdstuk 2 wordt de normering van het vergaren van publiekelijke toegankelijke online gegevens onderzocht. Het gaat daarbij om respectievelijk het handmatig vergaren van online gegevens, het automatisch vergaren van online gegevens en de observatie van online gedragingen van individuen die betrokken zijn bij een opsporingsonderzoek.

In hoofdstuk 3 wordt de juridische basis voor de toepassing van online undercover opsporingsmethoden onderzocht. Eerst wordt de aanleiding tot de Wet bijzondere opsporingsbevoegdheden besproken voor de benodigde achtergrondinformatie. Daarna worden de opsporingsmethoden van de online pseudokoop, online undercover interacties met individuen en online infiltratieoperaties besproken.

In hoofdstuk 4 wordt ingegaan op het juridisch kader voor de inbeslagname en onderzoek van gegevens in computers. Het huidige stelsel voor de opsporingsmethode wordt eerst behandeld. De recente discussie omtrent de normering van de inbeslagname en onderzoek op computers wordt eveneens uitgebreid onderzocht. De juridische basis voor de zogenaamde 'netwerkzoeking' wordt ook toegelicht.

■

9 Lees hier over meer in bijvoorbeeld het WRR-rapport (2016) over bigdata-toepassingen door de overheid.

10 Oerlemans 2017.

11 Zie Oerlemans 2017, p. 11-17 voor meer informatie over de beperkingen van de reikwijdte van het onderzoek en de gebruikte onderzoeksmethodologie.

Hoofdstuk 5 onderzoekt de juridische basis voor het vorderen van gegevens bij online serviceproviders. Eerst wordt aangeven waarom juist deze opsporingsmethode van belang is voor opsporingsonderzoeken met betrekking tot cybercrime. Ook de recente discussie omtrent de Wet bewaarplicht wordt daarin meegenomen. De analyse blijft daarna beperkt tot het juridisch kader omtrent het vorderen van gebruikersgegevens, verkeersgegevens, 'andere gegevens' en inhoudelijke gegevens bij online serviceproviders.

In hoofdstuk 6 wordt hacken als opsporingsmethode behandeld. De nieuwe voorgestelde opsporingsbevoegdheid in artikel 126nba Sv wordt daarbij uiteraard uitgebreid besproken. Daarna wordt dieper ingegaan op de concrete toepassing en normering van de doorzoeking op afstand, het gebruik van 'policeware' en de ontoegankelijkheidsmaking van gegevens op afstand.

2 Vergaren van publiekelijk toegankelijke online gegevens

In dit hoofdstuk wordt het juridisch kader omtrent het vergaren van publiekelijk toegankelijke online gegevens binnen opsporingsonderzoeken toegelicht. Deze opsporingsmethode maakt het mogelijk om bijvoorbeeld op basis van de echte naam of een '*nickname*' (schuilnaam) van een verdachte informatie van internet te vergaren. In een tijd waar mensen vrijwillig een indrukkende hoeveelheid informatie over zichzelf via internet beschikbaar stellen en online drugshandel op publiekelijk toegankelijke websites plaatsvindt, kan deze opsporingsmethode essentiële informatie voor opsporingsonderzoeken opleveren.

In paragraaf 2.1 wordt de term 'publiekelijk toegankelijk online gegevens' toegelicht. In paragraaf 2.2 wordt het juridisch kader omtrent het handmatig vergaren van online gegevens uiteengezet. Paragraaf 2.3 onderzoekt het automatisch vergaren van online gegevens als opsporingsmethode. In paragraaf 2.4 wordt het juridisch kader omtrent online observatie onderzocht. Het hoofdstuk wordt in paragraaf 2.5 afgesloten met een slotbeschouwing.

2.1 Definitie

De term 'publiekelijk toegankelijke online gegevens' is afkomstig uit art. 32 sub a van het Cybercrimeverdrag.[12] Het betreft gegevens die voor een ieder via internet toegankelijk zijn. Het gaat daarbij ook om gegevens die door middel van observatie beschikbaar zijn, na registratie beschikbaar zijn of pas na betaling beschikbaar zijn.[13] Daarbij wordt de terminologie van Europol gevolgd. De aangehouden definitie staat los van de vraag of het *wenselijk* is dat opsporingsautoriteiten (vaak grote) gegevenssets kunnen kopen van commerciële exploitanten. Het antwoord op deze vraag valt buiten de kaders van dit onderzoek.

Ik prefereer 'publiekelijk toegankelijke online gegevens' boven het vaker gebruikte 'open bronnen onderzoek', ook wel '*OSINT*' genoemd.[14] Daar zijn twee redenen voor. Ten eerste wekt de term open bron verwarring onder juristen op. De vraag speelt bijvoorbeeld of een open bron louter gegevens betreft die via Google beschikbaar zijn of ook die na registratie bij een website beschikbaar zijn. Ten tweede brengt de term open bron de connotatie met zich mee dat deze gegevens 'vrijelijk toegankelijk' zijn. Met andere woorden, alsof het een onuitputtelijke bron is.[15] Dat het vergaren van gegevens *niet* onbegrensd is, wordt in de volgende paragraaf duidelijk gemaakt.

12 Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, Boedapest, Trb. 2002, 18. Zie Koops & Oerlemans 2015 in: Verrest & Paridaens 2015 voor een uitgebreid commentaar van het Verdrag.

13 Zie voor een gelijksoortige definitie Eijkman & Weggemans 2012, p. 287. Deze auteurs sluiten op hun beurt aan bij de definitie van National Open Source Enterprise, Intelligence Community Directive 301 (juli 2006). Zie voor een gelijksoortige definitie ook: art. 25 lid 4 van het Besluit van de Raad van 6 april 2009 tot oprichting van de Europese politiedienst (Europol) (2009/271/JHA), L 121/51.

14 De afkorting OSINT staat voor 'open source intelligence'. Deze term past nog slechter bij deze studie, aangezien het hier om opsporingsonderzoeken en niet over intelligence of het handhaven van de openbare orde.

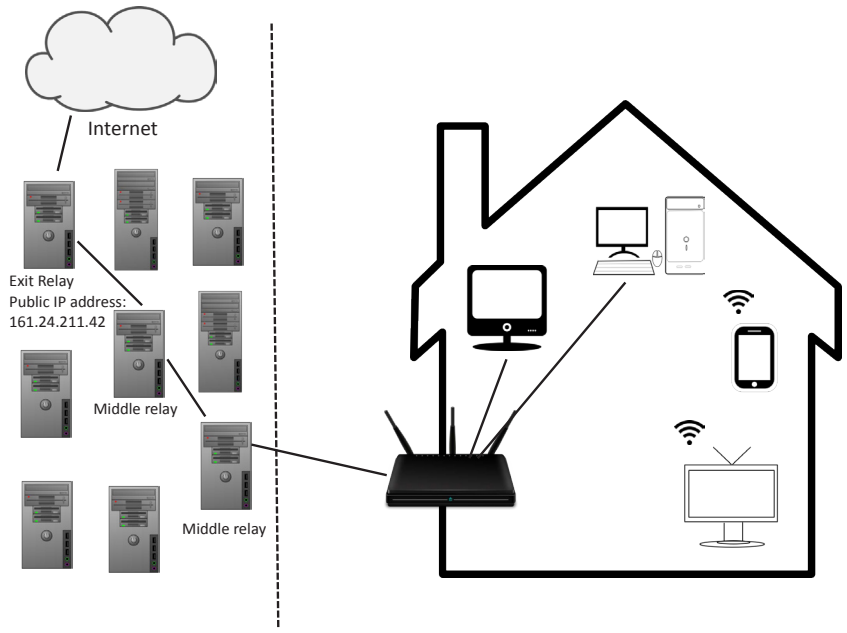
15 De titel 'Onuitputtelijk bron' van een artikel uit het politietijdschrift Blauw (M. Streefkerk) spreekt bijvoorbeeld boekdelen. Zie ook Harry Lensink & Gerard Janssen, 'Plaats delict: social media', Vrij Nederland, 18 april 2014. Beschikbaar op: http://www.vn.nl/Archief/Justitie/Artikel-Justitie/Plaats-delict-social-media.htm (laatst geraadpleegd op 25 november 2016).

2.2 Handmatig vergaren van online gegevens

Met het 'handmatig vergaren van online gegevens' wordt het proces van het vergaren van publiekelijk toegankelijke online gegevens door opsporingsambtenaren bedoeld. Daarbij wordt uiteraard gebruikgemaakt van computers en internet, maar niet van 'online monitoringssystemen' of geautomatiseerde systemen die gebruikmaken van '*spiders*' en '*crawlers*'. Wat met deze laatste termen wordt bedoeld, wordt in paragraaf 2.3 toegelicht.

Bij het handmatig vergaren van publiekelijk toegankelijke online gegevens moet worden gedacht aan het vergaren van gegevens die na het invoeren van zoektermen in een zoekmachine als Google beschikbaar zijn. Daarnaast kan worden gedacht aan het zoeken binnen online telefoongidsen, online discussieforums en sociale mediadiensten; ook als registratie is vereist.[16] In het verleden heeft het simpelweg invullen van een nickname in een zoekmachine in een cybercrimezaak al eens tot identificatie van de verdachte geleid.[17] Ook leverde het e-mailadres van de beruchte online drugsbaron Ross Ulbricht van handelsplatform '*Silk Road*' een belangrijk spoor op voor de FBI.[18] Met de groeiende populariteit van *social media* komt ook steeds meer informatie over mensen beschikbaar. In de meeste opsporingsonderzoeken zal de naam van de verdachte ook zeker 'even internet worden nagetrokken'.[19]

Publiekelijke toegankelijke online gegevens kunnen ook worden vergaard van het '*dark web*'. Met het dark web worden ook wel publiekelijk toegankelijke websites en diensten bedoeld, waarvan de IP-adressen van de servers verborgen zijn.[20] Deze diensten zijn in principe alleen bereikbaar via speciale servers in combinatie met software die het netwerkverkeer doorsturen. Het meest populair is op dit moment het gebruik van Tor.[21] Tor staat voor '*The Onion Routing*' en is een systeem om geanonimiseerd en op versleutelde wijze van internet gebruikt te maken.[22] Eenvoudig gesteld wordt het verkeer door minstens twee servers ('*relays*' genoemd) doorgeleid, waarbij elke relay alleen weet van welke laatste relay het netwerkverkeer vandaan komt en waar het verkeer naar toe moet. De servers onthouden niet het gehele pad dat het netwerkverkeer heeft gevolgd. Het Tor-systeem zorgt ervoor dat netwerkanalysetechnieken geen link kunnen maken tussen het beginpunt van het verkeer en eindpunt van het verkeer.[23] De werking van het Tor-systeem wordt in Figuur 2.1 geïllustreerd.



Figuur 2.1: Visualisatie van het Tor-systeem.

Het vergaren van gegevens op het dark web kan relevante informatie voor opsporingsambtenaren opleveren. Cybercrime[24] is oververtegenwoordigd[25] op het dark web en kan daarmee een interessante bron van bewijs opleveren.[26] Het is bijvoorbeeld mogelijk berichten die in het verleden op een handelsplatform of

16 Uiteraard worden daarbij niet de echte gegevens van de desbetreffende opsporingsambtenaar ingevuld, ook al wordt een 'real name policy' door de website vereist. Mijn overtuiging is dat het vergaren van deze gegevens onderdeel uitmaakt van de taakstelling van opsporingsambtenaren en de benodigde registratie geen materiële schade veroorzaakt dat eventueel op hen kan worden verhaald. Ook ligt het voor de hand om op een manier van internet gebruik te maken die niet herleidbaar is tot de politieorganisatie, bijvoorbeeld met behulp van een speciale infrastructuur voor internetrechercheren. In Nederland wordt daarvoor gebruikgemaakt van het IRN-netwerk en iColumbo-systeem. Zie uitgebreid: Koops e.a. 2012a.

17 Gary Cutlack, 'Police Caught an Anonymous Hacker by Googling his IRC Name', Gizmodo, 12 december 2012. Beschikbaar op: http://gizmodo.com/5968402/police-caught-an-anonymous-hacker-by-googling-his-irc-name (laatst geraadpleegd op 25 november 2016).

18 Zie Nate Anderson and Cyrus Farivar, 'How the feds took down the Dread Pirate Roberts', Ars Technica, 3 oktober 2013. Beschikbaar op: http://arstechnica.com/tech-policy/2013/10/how-the-feds-took-down-the-dread-pirate-roberts/, Kim Zetter, 'How the Feds Took Down the Silk Road Drug Wonderland', Wired, 18 november 2015. Beschikbaar op: http://www.wired.com/2013/11/silk-road/ en Joshuah Bearman, 'Silk Road: The Untold Story', Wired, 23 May 2015. Beschikbaar op: http://www.wired.com/2015/05/silk-road-untold-story/ (laatst geraadpleegd op 25 november 2016).

19 Zie ook Harry Lensink & Gerard Janssen, 'Plaats delict: social media', *Vrij Nederland*, 18 april 2014. Beschikbaar op: http://www.vn.nl/Archief/Justitie/Artikel-Justitie/Plaats-delict-social-media.htm (laatst geraadpleegd op 25 november 2016).

20 Andy Greenberg, 'Hacker Lexicon: What Is the Dark Web?', *Wired*, 19 november 2014. Beschikbaar op: http://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/ (laatst geraadpleegd op 25 november 2014).

21 Er bestaan ook andere anonimiseringssystemen, zoals *Freenet* en *I2P*. Freenet is publiekelijk beschikbare software die internetgebruikers de mogelijkheid geeft met elkaar bestanden te delen en websites te bezoeken die alleen via Freenet beschikbaar zijn (zie Clarke e.a. 2001, en Clarke e.a. 2010). Het Invisible Internet Project ('I2P') is nog ontwikkeling, maar zou populairder kunnen worden in de toekomst (cf. Ciancaglini e.a. 2013, p. 18). Op dit moment is Tor verreweg het meest populair. Zie ook Patrick Howell O'Neill, 'Tor and the rise of anonymity networks', 24 oktober 2013. Beschikbaar op: http://www.dailydot.com/debug/tor-freenet-i2p-anonymous-network/ (laatst geraadpleegd op 25 november 2016).

22 Tor is een afkorting voor 'The Onion Routing'.

23 Zie ook: Electronic Frontier Foundation. 'What is Tor' en 'Tor: overview'. Beschikbaar op: https://www.eff.org/torchallenge/what-is-tor.html en https://www.torproject.org/about/overview.html.en (laatst geraadpleegd op 25 november 2016). Zie ook Dingledine, Mathewson & Syverson 2004 voor een meer technische beschrijving. Af en toe verschijnt onderzoek waarbij wordt aangetoond dat gebruikers van anonimiseringsdiensten ontmaskerd kunnen worden. Ontwikkelaars maken deze lekken vaak weer dicht. Zie bijvoorbeeld: Larry Hardesty, 'Shoring up Tor. Researchers mount successful attacks against popular anonymity network - and show how to prevent them', 28 juni 2015. Beschikbaar op: https://news.mit.edu/2015/tor-vulnerability-0729 (laatst geraadpleegd op 2 januari 2017).

24 Met cybercrime bedoel ik: "*"misdrijven gepleegd door gebruikmaking van elektronische communicatienetwerken en informatiesystemen of tegen dergelijke netwerken en systemen*" (Mededeling van de Commissie aan het Europees Parlement, de Raad en het Europees Comité van de Regio's, 'Naar een algemeen beleid voor de bestrijding van cybercriminaliteit', COM(2007)267 definitief, 22 mei 2007).

25 Zie bijvoorbeeld Moore & Rid 2016.

26 Tegelijkertijd wordt het systeem ook gebruikt door bijvoorbeeld onderzoeksjournalisten, dissidenten en door mensen die simpelweg anoniem willen internetnetten.

discussieforum zijn gepubliceerd na te lopen en profielinformatie (voor zover publiekelijk beschikbaar) van de verdachte te verzamelen. Het gaat daarbij niet alleen om informatie die de verdachte zelf heeft gepubliceerd. Het is bijvoorbeeld ook denkbaar dat de echte naam van een verdachte in combinatie met zijn schuilnaam door anderen op het web wordt gepubliceerd.[27] Uit openbare interacties met anderen op internet kunnen bovendien interessante gegevens over het netwerk rondom een verdachte worden vergaard. Kortom, het handmatig vergaren van publiekelijk toegankelijke online gegevens kan informatie over de verdachte en diens omgeving opleveren. Allebei kunnen relevant zijn in een opsporingsonderzoek.

2.2.1 Juridische basis voor de opsporingsmethode

De vraag die voor ons ligt is op welke juridische basis deze gegevens verzameld mogen worden. Die vraag is niet eenvoudig te beantwoorden, omdat uniform nationaal beleid voor toepassing van de opsporingsmethode niet beschikbaar is.[28]

De wetsgeschiedenis maakt in ieder geval duidelijk dat opsporingsambtenaren (1) 'op internet kunnen rondkijken', (2) de gevonden informatie kunnen downloaden van verschillende bronnen op internet en (3) deze informatie kunnen opslaan in hun politiesysteem op basis van art. 3 van de Politiewet (Polw).[29] De opsporingsactiviteit is in dat geval onderdeel van de taakstelling van de politie om bewijs te verzamelen in opsporingsonderzoeken.[30] De toepassing van de opsporingsmethode vergt dan geen bevel van een officier van justitie en de opsporingsmethode kan worden toegepast in opsporingsonderzoeken naar elk type misdrijf.

Art. 3 Polw biedt slechts een voldoende juridische basis voor zover de opsporingsactiviteit (1) een geringe inmenging op de rechten en vrijheden van de betrokken individuen met zich meebrengt en (2) de integriteit van het opsporingsonderzoek niet in gevaar wordt gebracht. Deze norm wordt afgeleid uit de memorie van toelichting van de Wet bijzondere opsporingsbevoegdheden (Wet BOB) en uit jurisprudentie over de inzet van opsporingsmethoden.[31] Het handmatig vergaren van persoonsgegevens brengt mijns inziens slechts een geringe inmenging op de rechten en vrijheden van betrokkenen met zich mee.[32] De belangrijkste reden daarvoor is dat de informatie voor eenieder toegankelijk is. Mensen moeten er daarom rekening mee houden dat deze informatie door anderen, ook door de politie, kan worden vergaard. Een vergelijkbare redenering wordt door het Europees Hof voor de Rechten van de Mens (EHRM) aangehouden inzake het vergaren van informatie uit open bronnen en het gebruik van camera's ter observatie in het openbare leven.[33]

In slechts één (gepubliceerde) zaak bevestigen rechters van de Rechtbank Den Haag dat opsporingsambtenaren voor bewijsgaringsdoeleinden gebruik mogen maken van Google Earth op grond van art. 3 Polw.[34] In casu ging het om een persoon die verdacht werd van fraude. De rechercheurs konden met behulp van Google Earth vaststellen dat de betrokkene de designerstoelen van het type '*Bubble Club*' had aangeschaft, omdat Google Earth het mogelijk maakt tot in tuinen van mensen in te zoomen. Het verweer van de advocaat dat deze opsporingsmethode een meer dan geringe privacyinmenging met zich meebrengt, slaagde niet. De rechter merkte echter wel op dat het niet de bedoeling is dat 'stelselmatig gegevens van internet worden gedownload' op basis van de algemene taakstelling in art. 3 Polw.

In de memorie van toelichting van de Wet BOB wordt eveneens aangegeven dat het niet de bedoeling is dat 'stelselmatig gegevens van internet worden gedownload en in politiesystemen worden opgeslagen'.[35] Mijn inziens wordt daarmee niet bedoeld dat in dat geval een bijzondere opsporingsbevoegdheid van toepassing is. Een dergelijke bijzondere opsporingsbevoegdheid is namelijk niet voorhanden. In plaats daarvan moeten opsporingsambtenaren zich ervan bewust zijn dat de *Wet politiegegevens* van toepassing is.[36] Bovendien moeten opsporingsambtenaren – net zoals voor alle opsporingshandelingen die mogelijk relevant kunnen zijn tijdens het uiteindelijke proces tegen de verdachte – in principe een proces-verbaal opmaken van hun opsporingsactiviteiten op internet.[37]

2.2.2 De Wet politiegegevens

De Wet politiegegevens beperkt het handmatig verzamelen van publiekelijk toegankelijke gegevens op internet.[38] Deze wet schrijft bijvoorbeeld voor dat 'niet meer dan een noodzakelijke hoeveelheid' gegevens mag worden verzameld met een bepaald doel. Dat doel is in de context van deze studie natuurlijk het verzamelen van bewijs binnen een opsporingsonderzoek. Opsporingsambtenaren moeten zich er ook van bewust zijn dat het vergaren van 'gevoelige gegevens' slechts mogen worden verwerkt voor zover dat *onvermijdelijk* is voor het bereiken van het beoogde doel. Gevoelige gegevens zijn gegevens over ras, geloofsovertuiging, seksuele voorkeur en een eventueel lidmaatschap van een vakbond.[39] Foto's die worden gedeeld

27 Ook wel '*doxing*' genoemd. Zie https://en.wikipedia.org/wiki/Doxing (laatst geraadpleegd op 25 november 2016).
28 Zie ook Oosterhoff 2016.
29 Zie *Kamerstukken II* 1998/99, 26 671, nr. 3 (MvT Wet computercriminaliteit II), p. 35-36.
30 Zie *Kamerstukken II* 1998/99, 26 671, nr. 3 (MvT Wet computercriminaliteit II), p. 35. Voor de juridische basis ook wel verwezen naar artikel 141 en 142 van het Wetboek van Strafvordering (Sv). In zijn volledigheid is de juridische grondslag voor de opsporingshandeling dan ook art. 3 Polw jo art. 141-142 Sv.
31 Zie Fokkens & Kirkels-Vrijman 2009 en Borgers 2015. Deze standaard werd voor het eerst vastgesteld in de Zwolsman-zaak in 1995 (HR 19 december 1995, ECLI:NL:HR:1995:ZD0328, *NJ* 1996, 249 m. nt. Schalken). In deze zaak maakte de Hoge Raad duidelijk dat het doorzoeken van vuilniszakken op straat niet een zodanig ernstige privacyingemening met zich meebrengt dat een bijzondere opsporingsbevoegdheid voor de opsporingsmethoden voorhanden moet zijn. De standaard is later bevestigd in wetsgeschiedenis en andere arresten van de Hoge Raad. Zie bijvoorbeeld *Kamerstukken II* 1996/97, 25 403, nr. 3 (MvT Wet BOB), p. 110 en 115 en HR 20 januari 2009, ECLI:NL:HR:2009:BF5603, *NJ* 2009, 225, m.nt. Borgers, HR 13 november 2012, ECLI:NL:HR:2012:BW9338, *NJ* 2013, 413, m.nt. Borgers en HR 1 juli 2014, ECLI:NL:HR:2014:1562, *NJ* 2015/115, m.nt. P.H.P.H.M.C. van Kempen.
32 Zie Oerlemans 2017, p. 159-161. Anders: Oerlemans & Koops 2012. In tegenstelling tot wat ik in het artikel in 2012 heb betoogd, geloof ik niet dat van stelselmatige observatie sprake is indien gegevens uit publiekelijk toegankelijke bronnen worden verzameld. Bij observatie gaat het immers om het waarnemen van gedrag van mensen, terwijl het hier gaat om het verzamelen van gegevens, die *in het verleden* door de betrokkene zelf of anderen zijn gepubliceerd op internet.
33 Zie EHRM 25 september 2001, *P.G. en J.H. t. Verenigd Koninkrijk*, nr. 44787/98, § 57 en EHRM 17 juli 2003, *Perry t. Verenigd Koninkrijk*, nr. 63737/00, § 38.
34 Rb. Den Haag, 23 december 2011, ECLI:NL:RBSGR:2011:BU9409.
35 *Kamerstukken II* 1998/99, 26 671, nr. 3 (MvT Wet computercriminaliteit II), p. 36.
36 Zie ook *Kamerstukken II* 1998/99, 26 671, nr. 3 (MvT Wet computercriminaliteit II), p. 36.
37 Zie art. 152 Sv. De verbaliseringsplicht stelt de officier van justitie in de gelegenheid controle uit te oefenen over het opsporingsonderzoek en een verantwoorde vervolgingsbeslissing te nemen. Daarnaast stelt het ook de rechter én de verdediging op de terechtzitting in staat om de rechtmatigheid van het onderzoek te beoordelen. In HR 19 december 1995, *NJ* 1996, 249 geeft de Hoge Raad aan dat een redelijke uitleg van art. 152 Sv met zich meebrengt dat het opsporingsambtenaren slechts vrij staat het opmaken van een proces-verbaal achterwege te laten als het niet van belang kan zijn voor een door de rechter in het eindonderzoek te nemen beslissing.
38 Zie bijvoorbeeld ook Koops 2012, p. 32, Van der Bel, van Hoorn & Pieters 2013, p. 325 en Lodder e.a. 2014, p. 73.
39 Zie art. 5 Wet politiegegevens.

op sociale media of een foto van een persoon bij een online profiel zijn bijvoorbeeld gevoelige gegevens.[40] Ten slotte gelden nog andere vereisten voor de verwerken van politiegegevens, zoals een beperking van de bewaartermijn, een goed autorisatiebeleid en uiteraard een voldoende beveiliging van gegevens. Het is overigens een misvatting dat de Wet politiegegevens slechts van toepassing is bij het *opslaan* van gegevens in een politiedossier. De Wet politiegegevens is al van toepassing bij het *verwerken* van gegevens. Het verwerken van persoonsgegevens is al van toepassing wanneer de gegevens via een politiecomputer worden verzameld of door de systemen van een politie IT-infrastructuur stroomt.

De Wet politiegegevens vormt een complex juridisch kader op zichzelf, naast het Wetboek van Strafvordering dat in deze studie wordt behandeld.[41] Het valt buiten het bestek van deze studie om deze wet uitvoerig te analyseren. Wel wil ik erop wijzen dat uit deze korte analyse blijkt dat *het idee dat publiekelijk toegankelijke gegevens onbeperkt kunnen worden verzameld volstrekt onjuist is.* Op zijn minst moet een afweging worden gemaakt of het verzamelen van de gegevens noodzakelijk is. Dat vereiste wordt ingegeven door het recht op bescherming van persoonsgegevens, zoals onder andere in onze Grondwet is vastgelegd.[42] Gezien de verontrustende berichtgeving over de naleving van de Wet politiegegevens door de politie in Nederland, stel ik mijn vraagtekens bij de naleving van deze wet, ook in de context van het vergaren van publiekelijk toegankelijke online gegevens.[43] Ook vind ik het van belang erop te wijzen dat een proces-verbaal over het verzamelen van deze gegevens een relevant bewijsstuk tijdens de zitting oplevert. Op het moment van schrijven (januari 2017) ontbreekt het nog aan een procedure of landelijk beleid waarin op een concrete wijze wordt uitgelegd hoe de wetgeving van toepassing is.[44] Daar ligt wat mij betreft nog een taak voor de wetgever of het Openbaar Ministerie. Mogelijk kan inspiratie worden gevonden in de procedure voor 'internetrechercheren' die is gemaakt is voor ambtenaren binnen Nederlandse gemeenten.[45] Deze ambtenaren opereren binnen een ander juridisch kader, maar het is interessant om te zien hoe een concreet beleid is opgesteld voor het vergaren van gegevens uit publiekelijk toegankelijke bronnen door opsporingsambtenaren die werken voor Nederlandse gemeentes.

2.3 Automatisch vergaren van online gegevens

Het 'automatisch vergaren van publiekelijk toegankelijke online gegevens' onderscheidt zich van het handmatig vergaren in de zin dat daarbij gebruik wordt gemaakt van geautomatiseerde systemen. Deze systemen kunnen gebruikmaken van software, ook wel crawlers en spiders genoemd, die automatisch naar relevante informatie zoekt, bijvoorbeeld op basis van zoektermen of afbeeldingen.[46] '*Scraper*'-software download alle gevonden informatie meteen op de computerservers. Met behulp van deze geautomatiseerde verzamelsystemen kan publiekelijk toegankelijke informatie meer efficiënt en effectief worden gevonden en gepresenteerd aan opsporingsambtenaren. Koops (2013, p. 655) geeft daarnaast aan dat met behulp van plug-ins de zoek- en analysecapaciteiten vergroot kunnen worden, bijvoorbeeld met behulp van automatische herkenning of vertaalmogelijkheden. Potentieel kan in één muisklik een sociaal netwerk rondom een verdachte worden gevisualiseerd. In Nederland is het de ambitie van het iColumbo-systeem *'an 'intelligent, automated, "near" real-time Internet monitoring service' for governmental investigators'* te maken.[47] Om dat te bewerkstelligen zal zeer waarschijnlijk ook gebruik worden gemaakt van crawlers en scrapers om de informatie van te voren vast te leggen en te bewerken teneinde de beste resultaten aan de gebruikers van het systeem te kunnen tonen.

Juridische basis

Het automatisch vergaren van publiekelijk toegankelijke online informatie is ook aan wetgeving gebonden, omdat het een serieuze inmenging met het recht op privacy met zich meebrengt. Net als het handmatig vergaren van publiekelijk toegankelijke informatie wordt de opsporingsmethode nu nog op de algemene taakstelling van art. 3 Polw gebaseerd.[48] De Wet politiegegevens is eveneens van toepassing. Volgens minister Opstelten (destijds minister van Veiligheid en Justitie) kan gebruikmaking van iColumbo-systeem worden gebaseerd op art. 11 Wpg.[49] Toch blijkt uit een 'privacyscan' van Koops e.a. (2012a, p. 41-43) *niet* dat het systeem voldoet aan de Wpg. Een belangrijke vraag is hoe het iColumbo-systeem de Wpg op een *concrete* manier kan naleven.[50] Daarbij moeten vragen worden beantwoord, zoals voor welke delicten het systeem kan worden ingezet en wat de bewaartermijn is van de gegevens.

Een ander belangrijk punt is dat deze systemen preventief gegevens verzamelen en een grote en diverse set aan gegevens wordt verzameld. Dat betekent dat ook gegevens van mensen worden vastgelegd die in eerste instantie helemaal niet in het vizier van de opsporingsambtenaren liggen. Vanwege de serieuze inbreuk op de rechten en vrijheden van de betrokkenen heb ik betoogd dat aanvullende regelgeving noodzakelijk is.[51] Voor dit standpunt kan ondersteuning worden gevonden in de zogenaamde dataretentiezaken, waarbij het Hof van Justitie de Europese richtlijn voor de bewaarplicht van telecommunicatiegegevens ongeldig heeft verklaard.[52] Het Hof van Justitie kwam tot de conclusie dat de bewaarplicht van telecommunicatiegegevens op zichzelf een inmenging vormt op het recht op privacy en het recht op bescherming van persoonsgege-

40 Zie ook Koops e.a. 2012b, p. 42.
41 Zie Van der Bel, van Hoorn & Pieters 2013 voor een uitgebreide analyse.
42 Zie artikel 10 lid 2 Grondwet.
43 Zie bijvoorbeeld de volgende berichtgeving van de Autoriteit Persoonsgegevens: 'Regionale politiekorpsen niet toegerust op nieuwe eisen gegevensbescherming. CBP zal vervolgonderzoek doen bij individuele korpsen', 14 oktober 2008, 'Verwerking persoonsgegevens door regionale politiekorpsen Vervolgonderzoek CBP naar functioneren politie infodesks', 16 juli 2009, 'Politie en opsporingsdiensten verzuimen privacyaudit uit te voeren', 19 juli 2011 en Bart de Koning, 'Nieuws: de politie blijkt op grote schaal de wet te overtreden', *De Correspondent*, 8 december 2015. Beschikbaar op: https://decorrespondent.nl/3734/Nieuws-de-politie-blijkt-op-grote-schaal-de-wet-te-overtreden/44620296300 8-90777447 (laatst geraadpleegd op 25 november 2016).
44 Zie ook Lodder & Schuilenburg 2016, p. 152.
45 Zie het 'protocol internetonderzoek door gemeenten'. Beschikbaar op: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/protocol_internetonderzoek_door_gemeenten.pdf (laatst geraadpleegd op 25 november 2016).
46 Zie ook Lodder e a. 2014, p. 70 en de Kamerbrief van Minister van der Steur van 7 januari 2016 (*Kamerstukken II* 2015/16, 31 849, nr. 500) over het gebruik van een webcrawler om advertenties van loverboys te detecteren en de plaatsers van deze advertenties te identificeren.
47 Zie 'Deelprojectvoorstel, Ontwikkeling Real Time Analyse Framework voor het iRN Open Internet Monitor Network', 'iColumbo'. Beschikbaar op: http://www.nctv.nl/Images/deel-projectvoorstel-ontwikkeling-icolumbo-alternatief_tcm126-444133.pdf (laatst geraadpleegd op 29 november 2016).
48 Zie ook Brinkhoff 2016, p. 1402.
49 Zie de Kamerbrief van 13 december 2013 'Vrijheid en veiligheid in de digitale samenleving', *Kamerstukken II* 2013/14, 26 643, nr. 298.
50 Zie ook Lodder & Schuilenburg 2016, p. 152.
51 Zie Oerlemans 2017, p. 161-163.
52 HvJ EU 8 april 2014, C-293/12 (*Digital Rights Ierland t. Ierland*) en C-594/12 (*Seitlinger, Tschohl e.a.. t. Kärtner Landsregierung*). Zie ook Lodder & Schuilenburg 2016, p. 152.

vens.[53] Ook nam het Hof van Justitie in overweging dat gegevens van onschuldige mensen worden vastgelegd.[54] Het Hof van Justitie geeft in haar uitspraak aan dat het bij het vooraf opslaan van telecommunicatiegegevens nationale wetgeving omtrent de bescherming van persoonsgegevens moet bestaan, die op zijn minst misbruik en ongeautoriseerd gebruik van de gegevens moet tegengaan.[55] De hoeveelheid data die wordt vastgelegd, het type data dat wordt opgeslagen en het risico op misbruik moeten als factoren worden meegenomen om de legitimiteit van de maatregel te bepalen.[56] Ook wordt gewaarschuwd dat dergelijke waarborgen belangrijker zijn indien de gegevens op geautomatiseerde wijze verder worden verwerkt.[57] De uitspraak versterkt mijn idee dat de grootschalige preventieve opslag voor opsporingsdoeleinden een dermate grote privacyinmenging met zich meebrengt dat gedetailleerde wetgeving daarvoor noodzakelijk is.[58] In mijn proefschrift heb ik daarom beargumenteerd dat meer gedetailleerde regelgeving, vergelijkbaar met de regeling van cameratoezicht, noodzakelijk is.[59] In deze regelgeving kan bijvoorbeeld worden uitgelegd (1) waarom de privacyinmenging noodzakelijk wordt geacht, (2) voor welke delicten het middel kan worden ingezet, (3) welke gegevens worden opgeslagen, (4) wie toegang hebben tot het systeem en (5) welke bewaartermijn van de gegevens wordt aangehouden.

2.4 Observatie op internet

Observatie op internet is als opsporingsmethode in essentie hetzelfde als observatie in het openbare leven; het gaat om het waarnemen van gedrag van een persoon. Een persoon kan op internet bijvoorbeeld actief zijn op sociale media, discussieforums of chatkanalen. Het online gedrag van een persoon uit zich in die gevallen met het plaatsen van statusupdates of het delen van berichten op sociale media, het deelnemen aan of starten van discussies op forums, of het communiceren met anderen in chatkanalen.[60]

Vanaf het moment dat een opsporingsambtenaar het online gedrag van die persoon binnen een opsporingsonderzoek waarneemt, wordt de opsporingsmethode van observatie toegepast. Deze opsporingsmethode wordt onder de categorie van het 'vergaren van publiekelijk toegankelijke informatie' geplaatst, omdat het hier gaat om het passief waarnemen van de gedragingen van een persoon (eventueel na registratie bij een online dienst). Als de opsporingsambtenaar onder dekmantel gaat interacteren met de verdachte om achter deze informatie te komen, is er sprake van undercoveronderzoek en zijn mogelijk andere bijzondere opsporingsbevoegdheden mogelijk van toepassing. Observatie op internet onderscheidt zich van het handmatig vergaren van publiekelijk toegankelijke online gegevens in de zin dat de observatie op een enig moment in de tijd begint, terwijl bij het vergaren van publiekelijke toegankelijke online gegevens het gaat om gegevens die in het verleden zijn gepubliceerd.[61]

Juridische basis

Net als observatie als opsporingsmethode in de fysieke wereld is art. 3 Polw de juridische basis voor observatie (in het publieke domein), voor zover de opsporingsmethode niet stelselmatig wordt toegepast. Anders moet de bijzondere opsporingsbevoegdheid van *stelselmatige observatie* uit art. 126g Sv worden toegepast.[62] De wetgever heeft aangegeven dat bijzondere opsporingsbevoegdheden ook in de digitale wereld kunnen worden toegepast.[63] Daarom gaan we ervan uit dat voor het stelselmatig observeren van de gedragingen van personen in een online context ook de bijzondere opsporingsbevoegdheid van stelselmatige observatie moet worden ingezet.[64]

In de memorie van toelichting van de wet BOB geeft de wetgever aan dat van stelselmatigheid sprake is wanneer een 'min of meer volledig beeld van bepaalde aspecten van iemands privéleven' wordt verkregen. Om dat te bepalen geeft de wetgever de volgende factoren mee: de duur, plaats, intensiteit, frequentie, en het gebruik van een technisch hulpmiddel.[65] Tot op zekere hoogte kunnen de factoren naar een online context wordt vertaald.[66] De duur van de observatie van online waarnemingen spreekt vanzelf. Met betrekking tot de frequentie kan gedacht worden aan het verschil tussen het vijf keer per dag waarnemen van de gedragingen of één keer per week. De intensiteit als factor laat zich iets moeilijker vertalen. Mogelijk kan worden gedacht aan het waarnemen van gedrag uit verschillende online bronnen, de hoeveelheid vergaarde informatie en de gevoelige context van een bron.[67] Zo kan het waarnemen van een gedrag in een chatkanaal voor erotisch getinte gesprekken gevoeliger worden geacht dan gesprekken in een chatkanaal over het maken van opnames met drones.[68] Het is onduidelijk hoe het gebruik van een technisch hulpmiddel als factor voor online observatie kan worden vertaald. Het gebruik van computers en internet lijkt in ieder geval niet hieronder te vallen.[69]

Helaas wordt met de bovenstaande opsomming van factoren nog steeds weinig richting gegeven als het gaat om de vraag wanneer observatie in een online context de toepassing van de bijzondere opsporingsbevoegdheid van stelselmatige observatie vereist. Een eventuele interne richtlijn over 'internetrechercheren' is vooralsnog niet publiekelijk beschikbaar. Jurisprudentie laat zien dat ook in de fysieke wereld zeer

53 Zie HvJ EU 8 april 2014, C-293/12 (*Digital Rights Ierland t. Ierland*) en C-594/12 (*Seitlinger, Tschohl e.a.. t. Kärtner Landsregierung*), § 39 met verwijzing naar 26 maart 1987, *Leander t. Sweden*, nr. 9248/81, § 48, EHRM 4 mei 2000, *Rotaru t. Roemenië*, nr. 28341/95, § 46 en EHRM 29 juni 2006, *Weber en Saravia t. Duitsland*, nr. 54934/00, § 79.

54 HvJ EU 8 april 2014, C-293/12 (*Digital Rights Ierland t. Ierland*) en C-594/12 (*Seitlinger, Tschohl e.a.. t. Kärtner Landsregierung*), § 57-59. Zie ook Boehm & Cole 2014, p. 35-38. Interessant is dat de Advocaat-Generaal in zijn conclusie ook waarschuwt dat een dergelijk systeem de vrijheid van meningsuiting van mensen kan beperken door het '*chilling effect*' dat het met zich meebrengt (zie AG Opinion HvJ EU 8 april 2014, C-293/12 (*Digital Rights Ierland t. Ierland*) en C-594/12 (*Seitlinger, Tschohl e.a.. t. Kärtner Landsregierung*), § 53). Het Hof van Justitie nam deze overweging in haar uitspraak niet mee, omdat werd volstaan met een toets aan het recht op privacy en het recht op bescherming van persoonsgegevens en niet aan de vrijheid van meningsuiting.

55 HvJ EU 8 april 2014, C-293/12 (*Digital Rights Ierland t. Ierland*) en C-594/12 (*Seitlinger, Tschohl e.a.. t. Kärtner Landsregierung*), § 54.

56 HvJ EU 8 april 2014, C-293/12 (*Digital Rights Ierland t. Ierland*) en C-594/12 (*Seitlinger, Tschohl e.a.. t. Kärtner Landsregierung*), § 66.

57 HvJ EU 8 april 2014, C-293/12 (*Digital Rights Ierland t. Ierland*) en C-594/12 (*Seitlinger, Tschohl e.a.. t. Kärtner Landsregierung*), § 55.

58 Zie verglijkbaar: Lodder & Schuilenburg 2016, p. 152.

59 Zie Oerlemans 2017, p. 167.

60 Ik ben het dus niet eens met o.a. Oosterhoff (2016, p. 48-50), die in zijn scriptie betoogd dat stelselmatige observatie op internet niet van toepassing is.

61 Zie voor een soortgelijke redenering het CTIVD rapport over sociale media (2014, p. 9 en p. 42) in de context van open source intelligence (OSINT).

62 Zie *Kamerstukken II* 1998/99, 26 671, nr. 3 (MvT Wet computercriminaliteit II), p. 36 en *Kamerstukken II* 1996/97, 25 403, nr. 3 (MvT Wet BOB), p. 26-27.

63 Zie *Kamerstukken II* 1996/97, 25 403, nr. 3 (MvT Wet BOB), 29 en p. 55 en *Kamerstukken II* 1998/99, 26 671, nr. 3 (MvT Wet computercriminaliteit II), p. 36.

64 Zie ook antwoord op Kamervragen door staatssecretaris Klijnsma (Sociale Zaken en Werkgelegenheid) mede namens de Minister van Veiligheid en Justitie over internetopsporing (J.J. Oerlemans, 'Gebruik van open bronnen op internet en stelselmatige observatie', *Computerrecht* 2013/149.

65 Zie *Kamerstukken II* 1996/97, 25 403, nr. 3 (MvT Wet BOB), p. 26-27 en *Kamerstukken II* 1998/99, 26 671, nr. 7, p. 46. Zie ook HR 12 februari 2002, *NJ* 2002, 301, ECLI:NL:HR:2002:AD7804, par. 3.4.

66 Zie uitgebreid Koops 2012, p. 42 en Koops 2013, p. 663-664.

67 Zie ook Oerlemans & Koops 2012, p. 45.

68 Vergelijk met: *Kamerstukken II* 1997/98, 25 403, nr. 7, p. 47.

69 Zie ook Koops 2012, p. 42 en Koops 2013, p. 663-664.

verschillend wordt gedacht of observatie stelselmatig is.[70] Het 60 maal waarnemen van het gedrag van een verdachte binnen 27 maanden wil immers nog niet zeggen dat toepassing van de bijzondere opsporingsbevoegdheid is vereist.[71] Wat deze zaken wel met elkaar gemeen hebben, is dat vaak een proces-verbaal over de toepassing van de opsporingsbevoegdheid en duidelijkheid over de gebruikte juridische grondslag voorhanden is tijdens het proces. Het maken van een proces-verbaal, met daarbij vermelding van de juridische basis voor toepassing van de opsporingsmethoden, is daardoor belangrijk voor de beoordeling van de legitimiteit van het opsporingsmiddel. Dit zal niet anders zijn voor toepassing van observatie in een online context. Oosterhoff (2016) signaleert dat in de praktijk vaak wordt volstaan met zinnen als: "*Uit onderzoek op social media is gebleken dat …*". Dat is niet voldoende. Op zijn minst zouden de gemaakte zoekslagen en bezochte online bronnen moeten worden gemeld, alsmede de duur en frequentie van de observatie.

Helaas zijn er verder geen publieke bronnen beschikbaar die een procedure voorschrijven met betrekking tot observatie op internet. Het verdient aanbeveling aan de wetgever en het Openbaar Ministerie deze duidelijkheid wel te verschaffen. Dat is van belang voor alle actoren in het strafrechtsysteem. Zowel burgers als opsporingsambtenaren weten dan beter waar ze aan toe zijn en het beschermt burgers bovendien tegen willekeur van de overheid. Advocaten en de zittingsrechter kunnen vervolgens naleving van een procedure controleren.

2.5 Slotbeschouwing

Op basis van de analyse van de opsporingsmethode is Tabel 2.1 gemaakt. Deze tabel verschaft een overzicht van de juridische basis en voorwaarden voor het vergaren van publiekelijk toegankelijke online gegevens.

Opsporingsmethode	Grondslag	Voorwaarden	Voorbeelden toepassing
Handmatig vergaren van publiekelijk toegankelijke gegevens	Art. 3 Polw jo 141-142 Sv + Wet politiegegevens	Beperkingen op basis van Wet politiegegevens. Maken van proces-verbaal.	Gebruik van Google, sociale mediawebsites en online registers.
Automatisch vergaren van publiekelijk toegankelijke gegevens	Art. 3 Polw jo 141-142 Sv + Wet politiegegevens	Beperkingen op basis van Wet politiegegevens. Maken van proces-verbaal.	Gebruik monitoring software en crawlers en scrapers.
Observatie op internet	Art. 3 Polw jo 141-142 Sv of 126g Sv bij stelselmatige observatie	Bij stelselmatige observatie: bevel officier van justitie, slechts in opsporingsonderzoeken naar misdrijven in art. 67 Sv. Maken van proces-verbaal.	Betreft de observatie van gedragingen van individuen op sociale mediadiensten, online forums, chatkanalen, et cetera.

Tabel 2.1: Overzicht van de juridische grondslag voor het vergaren van publiekelijk toegankelijke online gegevens.

70 Zie Beijer e.a. 2004, p. 36 en 59.

71 Zie Oerlemans & Koops 2012, p. 44 met verwijzing naar HR 18 mei 1999, *NJ* 2000, 104, m. nt. Sch. (4M-zaak).

Uit Tabel 2.1 wordt duidelijk dat een juridische basis beschikbaar is voor de opsporingsmethode. Toch ligt er mogelijk een belangrijke taak voor de wetgever en het Openbaar Ministerie in het nader normeren van deze opsporingsmethode. Zeker in het licht van de voortschrijdende technologie zal wetgeving regelmatig moeten worden geüpdatet.[72] Nu ligt het niet direct voor de hand om een nieuwe bijzondere opsporingsbevoegdheid voor het handmatig vergaren van publiekelijk toegankelijke gegevens in het Wetboek van Strafvordering te creëren.[73] Het vergaren van gegevens uit publiekelijk toegankelijke bronnen moet mijns inziens worden gezien als de uitoefening van 'normaal politiewerk' en brengt slechts een geringe inmenging op het recht op privacy met zich mee. Het kan om die reden worden gebaseerd op art. 3 Politiewet. Wel is het van belang dat duidelijkheid komt over de wijze waarop de Wet politiegegevens concreet kan worden toegepast. Dat kan mogelijk met een procedure, vergelijkbaar met het protocol voor internetrechercheren van de Nederlandse gemeenten.

Daarnaast heb ik beargumenteerd dat aparte wetgeving moet worden gecreëerd voor het gebruik van automatische systemen voor het vergaren van publiekelijk toegankelijke informatie. Daarin kan duidelijk worden gemaakt voor welke doelen dergelijke systemen mogen worden ingezet en op welke wijze invulling wordt gegeven aan de verplichtingen die voortvloeien uit de Wet politiegegevens.

Tot slot is ook een meer concrete invulling wenselijk voor toepassing van stelselmatige observatie op internet. Nu zijn de factoren om te bepalen of observatie op stelselmatige wijzig plaatsvindt zeer abstract. Jurisprudentie op dit gebied kan mogelijk een meer concreet beeld geven van de grens tussen observatie en stelselmatige observatie. Bij voorkeur neemt echter de wetgever of het Openbaar Ministerie daartoe het voortouw.

72 Zie ook *Kamerstukken II* 1996/97, 25 403, nr. 3 (MvT Wet BOB), p. 12: "*De ontwikkelingen in de diverse vormen van criminaliteit, die hun oorsprong overigens mede in allerlei technologische ontwikkelingen hebben, vereisen dat ook de opsporingsmethoden zich voortdurend verder ontwikkelen.*"

73 Toch is dit in het recente verleden wel door de wetgever overwogen. Zie het 'discussiedocument' over bijzondere opsporingsbevoegdheden van 6 juni 2014 op p. 59-60. Beschikbaar op: https://www.rijksoverheid.nl/documenten/publicaties/2014/06/06/herziening-van-het-wetboek-van-strafvordering (laatst geraadpleegd op 6 december 2016).

3 Online undercover opsporingsmethoden

In dit hoofdstuk wordt het juridisch kader omtrent online undercovermethoden toegelicht. Deze opsporingsmethode kenmerkt zich door de *interactie* tussen opsporingsambtenaren en burgers *onder dekmantel* teneinde bewijs te verzamelen in een opsporingsonderzoek.[74] De betrokken individuen zijn niet op de hoogte van het doel van de interactie noch van de identiteit van de undercoveragenten.[75] Dit hoofdstuk richt zich op de volgende online undercovermethoden: (1) de online pseudokoop, (2) online undercover interacties met anderen, en (3) online infiltratieoperaties.

Het uitvoeren een pseudokoop op internet kan het best worden omschreven als de situatie waarbij een undercoveragent zich voordoet als potentiële koper van een illegaal via internet aangeboden goed of dienst. Daarbij kan worden gedacht aan het kopen van drugs op een online drugsforum op het dark web of de aankoop van gestolen gegevens (die na het plegen van computervredebreuk buit zijn gemaakt) via internet.[76]

Online undercover interacties van een opsporingsambtenaar met anderen kunnen zich voordoen op verschillende online diensten. Daarbij kan worden gedacht aan interacties op chatkanalen, via *privatemessaging*-diensten, via sociale mediadiensten, online discussieforums en online zwarte markten.[77] Slechts met de juiste kennis van internetsubculturen, kunnen opsporingsambtenaren op een geloofwaardige manier op internet communiceren en relaties aangaan met mensen in het kader van een opsporingsonderzoek.[78]

Online infiltratieoperaties zijn vergelijkbaar met online undercover interacties als opsporingsmethode. Online infiltratieoperaties onderscheiden zich door het kenmerk dat opsporingsambtenaren (tot op zekere hoogte) strafbare feiten mogen plegen om hun dekmantel te behouden en het vertrouwen te winnen van leden van een criminele organisatie.[79] Met andere woorden, in een infiltratieoperatie *participeren* opsporingsambtenaren in een criminele organisatie teneinde bewijsmateriaal over strafbare feiten te verzamelen en toegang te krijgen tot de hogere regionen van een criminele organisatie.[80]

In paragraaf 3.1 wordt eerst de achtergrond over de regulering van undercovermethoden beschreven. Kennis over deze achtergrond is essentieel om het wettelijk systeem van de regulering van undercover opsporingsmethoden te begrijpen. Bovendien zijn de Wet bijzondere opsporingsbevoegdheden en uitgangspunten die in deze wet zijn geformuleerd belangrijk voor de regulering van andere opsporingsmethoden. In paragraaf 3.2 wordt de normering van de online pseudokoop als opsporingsmethode toegelicht. Paragraaf 3.3 onderzoekt de juridische basis voor online undercover interacties. In paragraaf 3.4 wordt de normering

74 Zie verglijkbaar Marx 1988, p. 11-13 en Kruisbergen & De Jong 2010, p. 239. In dit onderzoek worden geen opsporingsmethoden (en daarbij horende regels) besproken met betrekking tot undercovermethoden waarbij burgers worden ingezet. Zie daarover o.a. Kruisbergen & De Jong 2010.

75 Zie ook Joh 2009, p. 161.

76 Zie bijvoorbeeld ook Arrondissementsparket Amsterdam, 'Pseudokoop wapen met bitcoins door politie en OM', 17 januari 2014. Beschikbaar op: https://www.om.nl/vaste-onderdelen/zoeken/@32570/pseudokoop-wapen/ (laatst geraadpleegd op 6 december 2016).

77 Zie bijvoorbeeld ook het persbericht: Landelijk Parket, 'Undercover onderzoek naar illegale marktplaatsen op Internet', 14 februari 2014. Beschikbaar op: https://www.om.nl/@32626/undercover-onderzoek/ (laatst geraadpleegd op 6 december 2016).

78 Zie ook o.a. Siemerink 2000b, p. 145 en Petrashek 2009, p. 1528.

79 Zie voor dit onderscheid ook Joh 2009, p. 166.

80 Zie Joh 2009, p. 167.

van online infiltratieoperaties besproken. Het hoofdstuk wordt afgesloten in paragraaf 3.5 met een slotbeschouwing.

3.1 Achtergrond regulering undercover opsporingsmethoden

De regulering van undercover opsporingsmethoden vindt haar achtergrond in de IRT-affaire uit de jaren '90. In de jaren '90 werkten verschillende politiekorpsen in ons land samen in 'Interregionaal Recherche Teams'. Deze teams richtten zich op georganiseerde misdaad waarbij vaak drugshandel in het spel was. Geïnspireerd door de Amerikaanse opsporingspraktijk maakte het team gebruik van innovatieve opsporingsmethoden.[81] Onder meer werd gebruikgemaakt van zogenaamde 'groei-informanten'. Deze undercoveragenten werd de ruimte gegeven te groeien in de hiërarchie van een criminele organisatie (o.a. door drugsdeals te faciliteren) om op die manier kennis te krijgen van de organisatiestructuur en de delicten die gepleegd werden door een criminele organisatie. Daarnaast kwam het voor dat de politie op de hoogte was van een drugstransport, maar niet tot inbeslagname of ander ingrijpen overging, om geen afbreuk te doen aan het opsporingsonderzoek en om zicht te blijven houden op de criminele organisatie.[82] Op enig moment besloot de korpschef van Amsterdam uit het samenwerkingsverband te stappen en kwamen de activiteiten naar buiten. Het gebruik van deze opsporingsmethoden leidde tot controverse binnen de Nederlandse samenleving. Niet alleen om de juridische en ethische kwesties die sommige opsporingsmethoden opriepen, maar ook omdat slechts weinig leidinggevenden bij de politie, het Openbaar Ministerie en het Ministerie van Justitie op de hoogte waren van de activiteiten.[83] Naar aanleiding van deze maatschappelijk controverse werd een Parlementaire Enquêtecommissie ingesteld onder leiding van Van Traa. De Commissie Van Traa schreef een uitgebreid rapport over het gebruik van de undercover opsporingsmethoden en deed aanbevelingen om deze opsporingsmethoden in het Wetboek van Strafvordering te reguleren.[84]

De aanbevelingen werden grotendeels door de toenmalige regering overgenomen en leidde tot de creatie van de Wet bijzondere opsporingsbevoegdheden (de Wet BOB).[85] De volgende bijzondere opsporingsbevoegdheden met betrekking tot undercover opsporingsmethoden werden in het Wetboek van Strafvordering geïntroduceerd:

1. pseudokoop en pseudodienstverlening;
2. stelselmatige informatie-inwinning;
3. infiltratie.[86]

81 Zie uitgebreid Nadelmann 1993, Nadelmann 1995, in: Fijnaut & Marx 1995 en Fijnaut & Marx 1995 in: Fijnaut & Marx 1995.
82 Zie uitgebreid *Kamerstukken II* 1995/96, 24 072, nr. 10–11 (Van Traa rapport), p. 72–164.
83 Zie *Kamerstukken II* 1995/96, 24 072, nr. 10–11 (Van Traa rapport), p. 427-428
84 Daarnaast zijn ook andere aanbevelingen gedaan die betrekking hebben op het recht op een eerlijk proces van verdachten, bijvoorbeeld met betrekking tot het opmaken van een proces-verbaal en de notificatie. Bovendien zijn aanbevelingen gedaan omtrent de organisatie van het opsporingsbestel. In deze studie wordt slechts ingegaan op het recht op privacy in relatie tot de normering van opsporingsmethoden.
85 *Stb.* 1999, 245, 27 mei 1999. De Wet BOB is in werking getreden op 1 februari 2000.
86 Ook andere opsporingsmethoden zijn destijds door de wetgever in het Wetboek van Strafvordering geïntroduceerd. Zie Buruma 2001, p. 33-130 voor een uitgebreid overzicht. De (online) pseudodienstverlening wordt in deze studie niet besproken.

Voor het identificeren van de juridische basis van de undercover opsporingsmethoden in een *online context* is het van belang dat in de wetsgeschiedenis is opgemerkt dat opsporingsbevoegdheden, zoals observatie en infiltratie, onder gelijke voorwaarden in de digitale wereld kunnen worden toegepast.[87] Met andere woorden, met het aannemen van de Wet BOB heeft de Nederlandse wetgever expliciet ervoor gekozen dat de bijzondere opsporingsbevoegdheden voor het uitvoeren van undercover opsporingsmethoden ook in een online context toepasbaar zijn onder dezelfde voorwaarden als in een offline context. [88]

Daarnaast is het van belang dat in de memorie van toelichting wordt benadrukt dat art. 3 Politiewet (jo 141-142 Sv) volstaat bij de toepassing van opsporingsmethoden die slechts een geringe inmenging met de rechten en vrijheden van de betrokken individuen met zich meebrengen en geen risico voor integriteit van het opsporingsonderzoek vormen.[89] Dit uitgangspunt staat sterk in verhouding tot art. 1 Sv: *"Strafvordering heeft alleen plaats op de wijze bij de wet voorzien"*. Art. 1 Sv formuleert het zogenaamde 'strafvorderlijk legaliteitsbeginsel' en is leidend voor de opsporingsfase voorafgaand aan de zitting.[90] Als gevolg van het strafvorderlijk legaliteitsbeginsel moet een grondslag in de wet voorhanden zijn voor bewijsgaringsactiviteiten van opsporingsambtenaren. Zoals eerder in hoofdstuk 2 is aangegeven zijn niet álle opsporingsmethoden als bijzondere opsporingsbevoegdheden gereguleerd, maar is telkens een juridische basis voorhanden (namelijk minstens artikel 3 Politiewet). De bevordering van de rechtszekerheid is het voornaamste doel van het strafvorderlijk legaliteitsbeginsel.[91]

Ten slotte wordt in de memorie van toelichting opgemerkt dat technische ontwikkelingen van invloed kunnen zijn op de toepassing van opsporingsmethoden. Het Wetboek van Strafvordering moet worden aangepast, indien de toepassing van deze nieuwe opsporingsmethoden - of ingeval van gebruik van bestaande methoden in een nieuwe context - een meer dan geringe inmenging met rechten en vrijheden met zich meebrengen of een risico voor de integriteit voor de opsporingsonderzoeken vormen. [92] Het is aan de wetgever om daarop de wet aan te passen, dus niet aan de rechter en zeker niet aan opsporingsinstanties, en zo een juridische basis voor een nieuwe opsporingsmethode te creëren.[93]

87 Zie *Kamerstukken II* 1998/99, 26 671, nr. 3 (MvT Wet computercriminaliteit II), p. 36.
88 In het rapport 'recht op de elektronische snelweg' en de kabinetsreactie daarop heeft de wetgever ook aangegeven dat het beginsel wordt aangenomen dat 'wat offline geldt, ook online van toepassing' is. Zie *Kamerstukken II* 1997/98, 25 880, nr. 1, p. 1.
89 *Kamerstukken II* 1996/97, 25 403, nr. 3 (MvT Wet BOB), p. 110 en 115.
90 Zie Kooijmans & Mevis 2013, p. 3.
91 Zie Corstens & Borgers 2014, p. 19. Zie Simmelink 1987 en Groenhuijsen & Knigge 2004, p. 11-16 voor een meer uitgebreide analyse van het strafvorderlijk legaliteitsbeginsel.
92 *Kamerstukken II* 1996/97, 25 403, nr. 3 (MvT Wet BOB), p. 12. Strikt genomen wordt in de memorie van toelichting alleen gesproken van een geringe inbreuk op het recht op privacy. Door de jaren heen is helder geworden dat ook andere rechten en vrijheden van belang zijn bij de toets of opsporingsmethoden in detail gereguleerd moeten worden als bijzondere opsporingsbevoegdheden. Zie ook de aanbeveling van de Raad van Europa (Recommendation Rec (2005)10) aan lidstaten over '*special investigation techniques*' met betrekking tot ernstige misdrijven (inclusief terrorisme): "*Considering that special investigation techniques are numerous, varied and constantly evolving and their common characteristics are their cover nature and the fact that their application could interfere with fundamental rights and freedoms*" (aangenomen door de Raad van Ministers op 20 april 2005. Zie ook de meer recente conceptaanbeveling van 13-14 juni 2016 door de "SIT Drafting Group" in Rome).
93 Zie Corstens & Borgers 2014, p. 19. Wel wordt door o.a. Borgers (2015) voorgesteld dat overwogen zou kunnen worden zogenaamde 'lichte opsporingsmethoden' die op basis van art. 3 Politiewet kunnen worden ingezet, verder te reguleren in Algemene Maatregels van Bestuur (AmvB's). Zie ook het discussiestuk Contourennota 'Modernisering strafvordering' van 30 september 2015, p. 10-11. Beschikbaar op: https://www.rijksoverheid.nl/documenten/kamerstukken/2015/09/30/brief-aan-de-tweede-kamer-modernisering-wetboek-van-strafvordering-plus-contourennota (laatst geraadpleegd op 19 december 2016).

3.2 Online pseudokoop

De online pseudokoop wordt in de praktijk vaak toegepast.[94] Op rechtspraak.nl zijn de volgende voorbeelden in recente zaken te vinden: (1) het kopen van drugs op online handelsplaatsen, (2) de aankoop van illegaal vuurwerk van webwinkels, (3) de aankoop van wapens op internet, (4) de aankoop van gestolen van goederen van marktplaats.nl, en (5) zelfs ivoor van bedreigde diersoorten.[95] De online pseudokoop kan bewijs opleveren in een strafzaak, omdat de verdachte bijvoorbeeld contactgegevens bij de verkoop achterlaat. Het is ook mogelijk dat de vingerafdrukken op een afleverde pakket resultaat opleveren of dat de verdachte bewogen kan worden het pakket in persoon af te leveren, hetgeen bijvoorbeeld een kans tot observatie kan bieden. Sinds 2006 kunnen ook *gegevens* worden gekocht bij een pseudokoop (in plaats van alleen goederen).[96] Dit kan van belang zijn in cybercrimezaken, bijvoorbeeld voor de aankoop van een '*exploit kit*'[97], creditcardgegevens, of gestolen persoonsgegevens die op internet worden aangeboden.[98]

Voor de toepassing van de bijzondere opsporingsbevoegdheid is een bevel van een officier van justitie vereist. De bevoegdheid mag alleen worden toegepast in opsporingsonderzoeken met betrekking tot misdrijven zoals omschreven in art. 67 van het Wetboek van Strafvordering. Hoewel een algemeen verbod tot uitlokking al van toepassing is, wordt in art. 126i Sv nogmaals erop gewezen dat 'een persoon er niet toe mag worden bewogen om een delict te plegen dat het hij niet voornemens was'.[99] Indien iemand een (op het eerste gezicht) illegaal goed op internet te koop zet, dan zal van uitlokking bij aankoop van dat goed geen sprake zijn. Maar als voorafgaand aan de aankoop bijvoorbeeld veel online contact is geweest, waarbij de opsporingsambtenaar druk op de verdachte heeft uitgeoefend om het goed op internet aan te bieden, dan kan wel sprake zijn van uitlokking. Het bevel voor toepassing van de opsporingsbevoegdheid moet al verkregen zijn voordat de daadwerkelijke aankoop begint, dus op het moment dat de interactie met de verdachte plaatsvindt om het goed of gegevens aan te schaffen.[100]

94 Zie ook Kruisbergen & De Jong 2010, p. 216.

95 Zie Rb. Den Haag 10 juli 2008, ECLI:NL:RBSGR:2008:BD7012 (online pseudokoop van drugs), Rb. Roermond 4 maart 2009, ECLI:NL:RBROE:2009:BH4757 (online pseudokoop van gestolen goederen op Marktplaats.nl), Rb. Zutphen, 28 januari 2011, ECLI:NL:RBZUT:2011:BP2308 (online pseudokoop van illegale wapens), Rb. Oost-Brabant 6 mei 2013, ECLI:NL:RBOBR:2013:BZ9467 (online pseudokoop van illegaal vuurwerk), Rb. Overijssel, 24 februari 2014, ECLI:NL:RBOVE:2014:884 (online pseudokoop van illegaal vuurwerk), Rb. Rotterdam 8 mei 2014, ECLI:NL:RBROT:2014:3504 (online pseudokoop van drugs op Silk Road), en Rb. Overijssel, 18 april 2016, ECLI:NL:RBOVE:2016:1323 (online pseudokoop van ivoor van bedreigde diersoorten). Zie ook het persbericht van het Landelijk Parket, 'Undercover onderzoek naar illegale marktplaatsen op internet' van 12 februari 2014. Beschikbaar op: https://www.om.nl/vaste-onderdelen/zoeken/@32626/undercover-onderzoek/ (laatst geraadpleegd op 19 december 2016).

96 Zie *Kamerstukken II* 1998/99, 26 671, nr. 3 (MvT Wet computercriminaliteit II), p. 36-37.

97 Een exploit kit is een softwarebundel die bedoeld is om te draaien op webservers, met het doel om kwetsbaarheden in software te identificeren op de computers die verbinding maken met de webservers. Vervolgens worden de kwetsbaarheden misbruikt om de kwaadaardige code uit te voeren op de computers van de bezoekers. Definitie ontleend aan: https://en.wikipedia.org/wiki/Exploit_kit (laatst geraadpleegd op 19 december 2016).

98 Het wegnemen van deze gegevens kan onder omstandigheden het delict diefstal (art. 310 Wetboek van Strafrecht (Sr)) opleveren, eenvoudig gezegd wanneer de gegevens uniek en op geld waardeerbaar zijn (zie HR 31 januari 2012, ECLI:NL:HR:2012:BQ9251 (*Runescape*)). Met de Wet computercriminaliteit III wordt bovendien het 'wegnemen van privégegevens' strafbaar gesteld in art. 139c Sr en het 'helen van gegevens' strafbaar gesteld in art. 139g Sr.

99 Zie over uitlokking See HR 4 december 1979, ECLI:NL:HR:1979:AB7429, *NJ* 1980, 356, m.nt. Th.W. van Veen (*Tallon* zaak) en in het bijzonder EHRM november 2010, *Bannikova t. Rusland*, nr. 18757/06, *EHRC* 2011/9, m.nt. Ölçer op EVRM-niveau. Zie ook *Kamerstukken II* 1996/97, 25 403, nr. 3 (MvT Wet BOB), p. 31.

100 Zie Rb. Roermond 4 maart 2009, ECLI:NL:RBROE:2009:BH4757 (online pseudokoop van verdachte gestolen goederen op Marktplaats.nl) met verwijzing naar HR 30 september 2003, ECLI:NL:HR:2003:AF7331, *NJ* 2004, 84 m.nt. Y. Buruma.

3.3 Online undercover interacties met individuen

Via internet kunnen opsporingsambtenaren of burgers onder dekmantel *interacteren* met verdachten in een opsporingsonderzoeken. Deze interacties kunnen bijvoorbeeld plaatsvinden door te chatten op een chatkanaal, berichten te plaatsen op een online discussieforum, een online handelsforum en door 'vrienden te worden met de verdachte' op sociale media om vervolgens met de verdachte te communiceren. De actieve interactie in het leven van de verdachte door de opsporingsambtenaar is kenmerkend voor de opsporingsmethode. Dit gaat verder dan louter het observeren van gedrag.[101]

3.3.1 Juridische basis

De juridische basis voor dit type undercoveronderzoek is art. 3 Polw of art. 126j Sv. Dit laatste artikel is de juridische basis voor toepassing van de bijzondere opsporingsbevoegdheid 'stelselmatige informatie-inwinning'. Voor het toepassen van de bijzondere opsporingsbevoegdheid is een bevel van een officier van justitie vereist. Art. 126j Sv kan worden ingezet bij de opsporing van elk misdrijf en is daarmee niet beperkt tot opsporingsonderzoeken naar bepaalde delicten. Daar komt in de nabije toekomst wellicht verandering in, omdat is voorgesteld de opsporingsbevoegdheid te beperken tot misdrijven met een maximale gevangenisstraf van een jaar.[102] De wetgever heeft expliciet aangegeven dat de bijzondere opsporingsbevoegdheid op internet mag worden toegepast.[103]

De moeilijkheid bij deze opsporingsmethode zit in de vraag of de operatie in zijn aard als *stelselmatig* is te kwalificeren. In de memorie van toelichting zijn de vijf factoren van de (1) duur, (2) plaats, (3) intensiteit, (4) frequentie en (5) het gebruik van een technisch hulpmiddel aangedragen om te bepalen of sprake is van stelselmatigheid bij observatie.[104] Samen geven deze factoren antwoord op de vraag of een 'min of meer volledig beeld van bepaalde aspecten van iemands privéleven' wordt verkregen. Deze factoren zijn echter genoemd voor stelselmatige observatie en niet expliciet voor stelselmatige informatie-inwinning. Jurisprudentie geeft ook geen duidelijk antwoord op de vraag wanneer sprake is van stelselmatigheid bij het informatie inwinnen onder dekmantel.

3.3.2 De Context-zaak

Slechts één zaak is beschikbaar die een antwoord geeft op de bovengenoemde vraag wanneer sprake is van stelselmatigheid bij online interacties met de verdachten in een opsporingsonderzoek.[105] In de zogenoemde '*Context-zaak*' hebben opsporingsambtenaren namelijk een fictief profiel opgesteld en zichzelf als vriend toegevoegd aan het profiel van de verdachte op Facebook. Daarnaast hebben ze deelgenomen aan een Facebookgroep waarvan werd gedacht dat deze zich bezighield met jihadistische activiteiten. Kort gezegd

101 Zie *Kamerstukken II* 1996/97, 25 403, nr. 3 (MvT Wet BOB), p. 35.

102 Zie discussiestuk over de regulering van bijzondere opsporingsbevoegdheden van 6 juni 2014, p. 26.

103 Zie *Kamerstukken II* 1996/97, 25 403, nr. 3 (MvT Wet BOB), p. 34. Zie ook *Kamerstukken II* 1998/99, 26 671, nr. 3 (MvT Wet computercriminaliteit II), p. 37.

104 Zie *Kamerstukken II* 1996/97, 25 403, nr. 3 (MvT Wet BOB), p. 26-27 en *Kamerstukken II* 1998/99, 26 671, nr. 7, p. 46. Zie ook HR 12 februari 2002, NJ 2002, 301, ECLI:NL:HR:2002:AD7804, par. 3.4.

105 Zie Rb. Den Haag, 10 december 2015, ECLI:NL:RBDHA:2015:14365, m.nt. J.J. Oerlemans, *Computerrecht* 2016, nr. 2, p. 113-124.

waren de rechters van mening dat al voor het aanmaken van een profiel de bevoegdheid tot stelselmatige informatie-inwinning moest worden ingezet.[106] De opsporingsambtenaren hebben het bevel van de officier van justitie pas later verkregen en er was sprake van gebrekkige vastlegging van de opsporingshandelingen.[107] Op de uitspraak kan kritiek worden geleverd. Beargumenteerd kan worden dat de opsporingsmethode pas op enig moment stelselmatig wordt, nadat de interacties onder dekmantel met de verdachte plaatsvinden. Toch is het vereisen van de bijzondere opsporingsbevoegdheid mijns inziens terecht, omdat bij het toevoegen van een nepprofiel aan het profiel van een verdachte een grote kans is dat een 'min of meer volledig beeld van bepaalde aspecten van iemands privéleven' wordt verkregen. Op Facebookprofielen zetten mensen immers in de regel veel privégegevens online, zoals foto's, geboortedatum, interesses en relaties. Daarnaast is het gehele online sociale netwerk van de betrokkene met betrekking tot die dienst zichtbaar.

Op basis van de bovengenoemde 'Context-zaak' mag dus ervan worden uitgegaan dat op de aanmaak van een nepprofiel en het worden van Facebookvrienden met de verdachte de bijzondere opsporingsbevoegdheid van stelselmatige informatie-inwinning van toepassing is. Twijfel bestaat er mijns inziens nog wel over situaties waarbij (1) gechat wordt met de verdachte tijdens een groepschat op een bepaald chatkanaal en (2) kortstondig een privéchat plaatsvindt waarbij bijvoorbeeld een e-mailadres of telefoonnummer wordt bemachtigd om verder te communiceren. In ieder geval is het relevant dat de opsporingsambtenaar nagaat of de opsporingshandeling plaatsvindt op basis van art. 3 Polw of van de bijzondere opsporingsbevoegdheid van stelselmatige informatie-inwinning. Wellicht moet daarover met een officier van justitie worden overlegd. Het maken van een proces-verbaal van de opsporingshandeling is ook noodzakelijk.

3.3.3 De lokpuber

Ten slotte speelt nog de vraag in hoeverre een opsporingsambtenaar zich mag voordoen als minderjarige – ook wel 'lokpuber' genoemd - om bijvoorbeeld '*groomers*' op te sporen. *Grooming* is kort gezegd de strafbare gedraging waarbij een meerderjarige via internet met een minderjarige afspreekt teneinde seks te hebben.[108] Deze interacties kunnen bijvoorbeeld op een chatwebsite plaatsvinden waar ook opsporingsambtenaren zich onder dekmantel toegang kunnen verschaffen. Eerder heeft een dergelijke operatie tot vrijspraak geleid, omdat voor de delictsomschrijving is vereist dat met een *minderjarige* wordt afgesproken.[109] De undercover opsporingsambtenaar was in casu meerderjarig, waardoor niet aan de delictsomschrijving werd voldaan. Maar daarnaast speelt de vraag of het gebruik van deze 'lokpuber'-constructie niet tot uitlokking leidt. De opsporingsambtenaar zal namelijk hoogstwaarschijnlijk een seksueel getint gesprek met de verdachte moeten hebben om zo tot een afspraak over te gaan. Het is echter niet toegestaan de verdachte te brengen tot een strafbare gedraging. In Europese jurisprudentie wordt er ook op gewezen dat de opsporingsinstanties 'in essentie passief' moeten blijven tijdens een undercoveronderzoek om uitlokking tegen gaan.[110] Uit dezelfde rechtspraak volgt overigens ook dat het EHRM sterk de voorkeur geeft aan de

■

106 Zie Rb. Den Haag, 10 december 2015, ECLI:NL:RBDHA:2015:14365, r.o. 5.26-5.27.

107 Zie Rb. Den Haag, 10 december 2015, ECLI:NL:RBDHA:2015:14365, r.o. 5.27. Het maken van een proces-verbaal ook hier verplicht, omdat de opsporingshandelingen mogelijk relevant tijdens het proces kunnen zijn. De vormverzuimen leidden niet tot een sanctie. Het vormverzuim is daarmee dus 'gerelativeerd' door de rechter.

108 Grooming is strafbaar gesteld in art. 248e Sr.

109 Zie Hof Den Haag, 25 juni 2013, ECLI:NL:GHDHA:2013:2302.

110 Zie ook Smeets 2013, p. 336 en Ölçer 2014, p. 18.

betrokkenheid van een rechter-commissaris. De Nederlandse regeling voldoet daar niet aan. Daarmee is het de vraag of de wet niet moet worden aangepast door een machtiging van een rechter-commissaris voor de bevoegdheid van stelselmatige informatie-inwinning te vereisen. Ondanks deze vragen met betrekking tot uitlokking en vereiste waarborgen, heeft de wetgever in de Wet computercriminaliteit III voorgesteld om art. 248e Sr aan te passen.[111] Daarmee wordt het voor opsporingsambtenaren mogelijk om zich voor te doen als minderjarige en zo grooming op te sporen. De delictsomschrijving van grooming wordt op die wijze aangepast dat niet meer is vereist dat in werkelijkheid een zestienminner (van vlees en bloed) wordt gegroomd.[112] Ook burgers kunnen zich straks voordoen als 'lokpuber' om groomers te pakken.[113]

3.4 Online infiltratieoperaties

Infiltratieoperaties onderscheiden zich van stelselmatige inwinning in de zin dat bij infiltratieoperaties wordt *deelgenomen* aan een criminele organisatie.[114] Het is daarbij mogelijk dat (geautoriseerde) strafbare feiten worden gepleegd. De Nederlandse wetgever gaf destijds aan dat door middel van infiltratieoperaties bewijs kan worden verzameld over de strafbare feiten die in georganiseerd verband worden gepleegd (of worden gepland) en met de opsporingsmethode inzicht kan worden verkregen in de modus operandi van de verdachten.[115] Infiltratieoperaties kunnen ook in een online context worden ingezet, zoals op online fora of handelswebsites waarbij het vermoeden bestaat dat strafbare feiten in georganiseerd verband worden gepleegd.

Tijdens een infiltratieoperatie op een drugsforum is het bijvoorbeeld mogelijk ook een pseudokoop te plegen, alhoewel daarvoor ook de desbetreffende bijzondere opsporingsbevoegdheid nog apart kan worden ingezet. In de Aanwijzing opsporingsbevoegdheden wordt overigens erop gewezen dat de (pseudo) aankoop van bepaalde goederen, zoals menselijke organen, niet is toegestaan om ethische redenen.[116] Eenzelfde redenering wordt in een rapport van de Nationaal Rapporteur Mensenhandel genoemd over de handel in kinderporno door opsporingsinstanties.[117] Nederlandse opsporingsinstanties lijken niet bereid te zijn kinderporno te gebruiken om te infiltreren in een criminele organisatie die zich bezighoudt met (de distributie of zelfs vervaardiging van) kinderporno. Het achterliggende idee is dat anders de 'markt' in de handel in kinderporno in stand wordt gehouden en het slachtofferschap van de betrokken minderjarigen voortduurt. Deze toepassing van infiltratie wordt wel expliciet in de memorie van toelichting op de Wet BOB en de Wet Computercriminaliteit genoemd.[118]

■

111 Zie *Kamerstukken II* 2015/16, 34 372, nr. 2 (Wetsvoorstel computercriminaliteit III).

112 Aan de delictsomschrijving wordt het volgende onderdeel toegevoegd: "*of iemand die zich voordoet als een persoon die de leeftijd van zestien jaren nog niet heeft bereikt een ontmoeting voorstelt*".

113 Zie uitgebreid Lindenberg 2016.

114 Zie *Kamerstukken II* 1996/97, 25 403, nr. 3 (MvT Wet BOB), p. 29. Zie ook de brief van de Minister van Veiligheid en Justitie van 8 oktober 2014 (nr. 571620) over het juridische verschil tussen 'informanten' en 'individuen die in infiltreren binnen een opsporingsonderzoek'.

115 Zie *Kamerstukken II* 1996/97, 25 403, nr. 3 (MvT Wet BOB), p. 28.

116 *Stcrt.* 2014, nr. 24442.

117 Nationaal Rapporteur Mensenhandel 2011, p. 164-165.

118 *Kamerstukken II* 1996/97, 25 403, nr. 3 (MvT Wet BOB), p. 29 en *Kamerstukken II* 1998/99, 26 671, nr. 3 (MvT Wet computercriminaliteit II), p. 36-37. In de memorie van toelichting van de Wet computercriminaliteit II wordt tevens expliciet opgemerkt dat de bijzondere opsporingsbevoegdheid van infiltratie 'op internet' kan worden toegepast (*Kamerstukken II* 1998/99, 26 671, nr. 3 (MvT Wet computercriminaliteit II), p. 37).

3.4.1 Juridische basis

Voor online infiltratieoperaties is de inzet van de bijzondere opsporingsbevoegdheid tot infiltratie in art. 126h Sv van toepassing. Hierbij geldt geen drempel zoals 'systematisch infiltreren'. Zodra wordt deelgenomen aan een groep die zich bezighoudt met georganiseerde misdaad of diensten worden geleverd aan een dergelijke groep, is de bijzondere opsporingsbevoegdheid van toepassing. Een infiltratieoperatie mag alleen worden gestart nadat een bevel is verkregen van een officier van justitie in opsporingsonderzoeken naar misdrijven zoals omschreven in art. 67 Sv. Bovendien moet de rechtsorde 'ernstig geschokt'[119] zijn en moet een machtiging van een rechter-commissaris worden verkregen. Als intern controlemechanisme moet ook de Centrale Toetsingscommissie van het Openbaar Ministerie verplicht advies geven over de inzet van infiltratieoperaties.

3.4.2 Infiltreren in een online drugsforum

Jurisprudentie over de online toepassing van de opsporingsbevoegdheid tot infiltratie is schaars. In slechts één zaak bij de Rechtbank Middelburg is sprake van infiltratie op een online drugsforum.[120] De opsporingsambtenaren waren voornemens om binnen een online drugshandelforum in de hiërarchie op te klimmen tot 'moderator'. Moderators managen de dagelijkse taken van een forum en controleren de naleving van interne regels door de gebruikers van een forum. Voor de operatie zelf is de bijzondere opsporingsbevoegdheid van infiltratie ingezet. Het is de opsporingsambtenaren uiteindelijk niet gelukt zelf moderator te worden op het forum, maar zij wisten wel het vertrouwen te winnen van een van de moderators op het forum. Door middel van een pseudokoop werden drugs aangekocht (de moderator verkocht zelf ook drugs) en voor de aflevering werd een afspraak in de fysieke wereld gemaakt. Na de aankoop van de drugs is de verdachte gevolgd tot zijn woonhuis door een observatieteam, waarvoor de bijzondere bevoegdheid van systematische observatie werd ingezet. De verdachte werd later gearresteerd. De advocaat van de verdachte protesteerde tegen het feit dat de operatie zowel in de fysieke wereld als 'virtueel' werd ingezet. De rechter keurde deze hybride toepassing van de bijzondere opsporingsbevoegdheid van infiltratie goed.[121] Toch is het opvallend dat maar één zaak over de toepassing van een online infiltratie beschikbaar is. Meer jurisprudentie is noodzakelijk om de reikwijdte van de toepassing van de bijzondere opsporingsbevoegdheid in een online context voldoende te beschrijven.

■

119 Zie meer hierover Blom 2007.

120 Rb. Midden-Nederland 9 Oktober 2014, ECLI:NL:RBMNE:2014:4790 en ECLI:NL:RBMNE:2014:4792. De Rechtbank beschrijft in omslachtige termen hoe de verdachten gebruikmaakten van een 'beveiligd netwerk' waarmee 'anoniem' drugs gekocht en verkocht werd op een online handelsplaats. Door de timing van de uitspraak is duidelijk dat het hierbij waarschijnlijk ging om de online marktplaatsen 'Black Market Reloaded' en 'Utopia' die alleen via Tor toegankelijk zijn. Zie ook *ANP*, 'OM wil tot zeven jaar cel voor internetdealers', *Nu.nl*, 23 september 2014. Beschikbaar op: http://www.nu.nl/internet/3885624/wil-zeven-jaar-cel-internetdealers.html (laatst geraadpleegd op 23 december 2016) en J.J. Oerlemans, 'Veroordelingen voor drugshandel via online marktplaatsen', *Computerrecht* 2015, nr. 3, p. 170.

121 Zie Rb. Midden-Nederland 9 oktober 2014, ECLI:NL:RBMNE:2014:4790 en ECLI:NL:RBMNE:2014:4792. Siemerink (2000b, p. 144) gaf in 2000 al aan dat deze hybride toepassing veel zal voorkomen. Net als in het normale leven beginnen interacties soms op internet en kunnen deze leiden tot ontmoetingen in de fysieke wereld. Naar mijn mening is het wel van belang dat in de aanvraag tot inzet van de bijzondere opsporingsbevoegdheid de toepassing zo concreet mogelijk wordt omschreven.

3.5 Slotbeschouwing

Op basis van de analyse van de opsporingsmethode is Tabel 3.1 gemaakt. De tabel verschaft een overzicht van de juridische basis van online undercover opsporingsmethoden en geeft voorbeelden van de toepassing daarvan.

Opsporingsmethode	Grondslag	Voorwaarden	Voorbeelden toepassing
Online pseudokoop	Art. 126i Sv	Bevel officier van justitie. Beperkt tot misdrijven zoals omschreven in art. 67 Sv.	De aankoop van drugs, wapens en andere illegale goederen op internet.
Online undercover interacties met individuen	Art. 126j Sv[1]	Bevel officier van justitie.	Chatten onder dekmantel, het sturen van privéberichten onder dekmantel en online undercover interacties met verdachten op sociale media.
Online infiltratie operaties	Art. 3 Polw jo 141-142 Sv of 126g Sv bij stelselmatige observatie	Bevel officier van justitie. Beperkt tot misdrijven zoals omschreven in art. 67 Sv die rechtsorde ernstig schaden. Toestemming noodzakelijk van de Centrale Toetsingscommissie.	Een infiltratieoperatie op een online forum, waarbinnen in georganiseerd verband strafbare feiten worden gepleegd.

Tabel 3.1: Overzicht van de juridische grondslag voor online undercoveroperaties.

In dit hoofdstuk zijn de juridische basis voor online undercover opsporingsmethoden besproken. De juridische basis voor undercover opsporingsmethoden zoals die zijn neergelegd in de Wet bijzondere opsporingsmethoden, als gevolg van de IRT-affaire, zijn nog steeds van toepassing. Over het geheel genomen is de reikwijdte en de toepassing van de bijzondere opsporingsbevoegdheden in een online context duidelijk. Toch is voorgesteld om de voorwaarden voor systematische informatie-inwinning aan te scherpen. Uit jurisprudentie van het EHRM blijkt bovendien dat dit hof toezicht door een rechter-commissaris prefereert.

Ten slotte moet worden benadrukt dat in deze researchpaper de internationale context van de toepassing van digitale opsporingsmethoden niet wordt meegenomen. In het meest recente '*internet organised crime threat assessment*'- (iocta-) rapport van Europol (2016) wordt echter aangeraden om op Europees niveau afspraken te maken voor het uitvoeren van undercoveroperaties op het dark web. Aan de start van het onderzoek is de locatie van de verdachte vaak niet helder en bestaat de kans dat opsporingsmethoden in het buitenland worden ingezet. In theorie is daar rechtshulp of toestemming van de betrokken staat daarvoor noodzakelijk.[122] Op Europees niveau zou dit type onderzoek kunnen worden gestroomlijnd en eventueel zelfs afspraken worden gemaakt over onder welke voorwaarden deze online undercoveroperaties mogen plaatsvinden.

■

122 Zie hierover uitgebreid Oerlemans 2017, p. 324-337.

4 Inbeslagname en onderzoek van gegevens in computers

In dit hoofdstuk wordt de opsporingsmethode van de inbeslagname en onderzoek van gegevens in computers geanalyseerd. Daarnaast wordt de opsporingsmethode van de netwerkzoeking onderzocht, aangezien deze direct na de inbeslagname van computers zal plaatsvinden op grond van dezelfde juridische basis.

In paragraaf 4.1 wordt het wettelijk kader voor de inbeslagname van computers toegelicht. In paragraaf 4.2 wordt ingegaan op de vraag of computers bijzondere bescherming binnen het Wetboek van Strafvordering moeten krijgen. In paragraaf 4.3 wordt de juridische grondslag en de reikwijdte van de netwerkzoeking onderzocht. Het hoofdstuk wordt afgesloten in paragraaf 4.4 met een slotbeschouwing.

4.1 Computers als voorwerp ter inbeslagname

Binnen het Wetboek van Strafvordering worden computers (vooralsnog) behandeld als ieder ander voorwerp. Binnen een opsporingsonderzoek zijn voorwerpen vatbaar voor inbeslagname. Deze voorwerpen kunnen aan nader onderzoek worden onderworpen.[123] Eenvoudig gesteld kunnen drie regelingen worden onderscheiden op basis waarvan een computer (en elke andere gegevensdrager) in beslag kan worden genomen.[124]

Ten eerste kan een computer na aanhouding van een verdachte door een opsporingsambtenaar in beslag worden genomen, voor zover de inbeslagname de waarheidsvinding dient of noodzakelijk is om wederrechtelijk verkregen voordeel aan te tonen.[125] De inbeslagname impliceert ook dat de gegevens die staan opgeslagen op de computer nader kunnen worden geanalyseerd.[126]

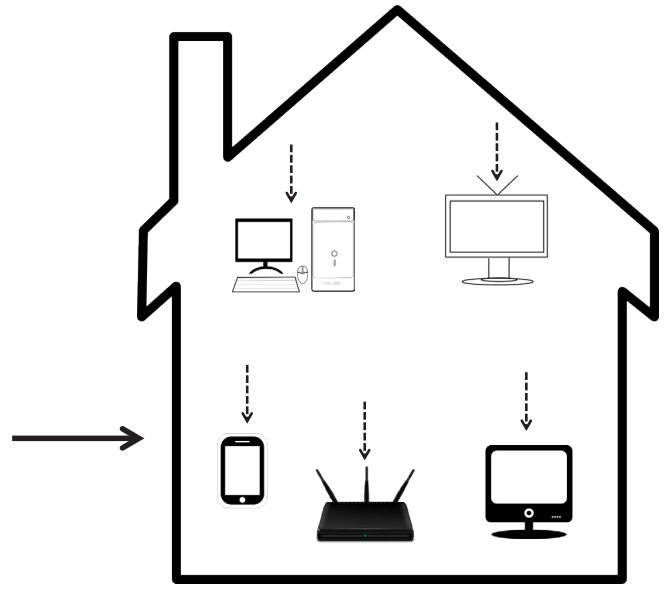
Ten tweede kunnen computers tijdens een doorzoeking van een plaats in beslag worden genomen.[127] Na inbeslagname kunnen de gegevens nader worden geanalyseerd. Op grond van art. 551 Sv kunnen ook gegevensdragers die kinderporno bevatten, worden onttrokken aan het verkeer.

Ten derde kunnen tijdens een doorzoeking ter vastlegging van gegevens op een geautomatiseerd werk op een bepaalde plaats, computers in beslag worden genomen en de gegevens nader worden geanalyseerd.[128]

123 Zie ook *Kamerstukken II* 1989/90, 21 551, nr. 3, p. 12-13.
124 Zie voor een uitgebreide analyse van het Nederlandse regime, bijvoorbeeld Wiemans 2004 en meer recent Mevis, Verbaan & Salverda 2016 en Koops, Conings & Verbruggen 2016.
125 Zie art. 53 Sv en 95 Sv. Volgens Koops, Conings en Verbruggen (2016) komt dit in de praktijk regelmatig voor.
126 Zie ook Wiemans 2004, p. 124.
127 Zie art. 96 Sv, art. 96b Sv, art. 96c Sv en art. 110 Sv.
128 Zie art. 125i Sv jo art. 96b Sv, art. 125i Sv jo art. 96c Sv en art. 125i Sv jo art. 110 Sv of art. 97 Sv. Zie ook *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 11.

4.1.1 Inbeslagname tijdens de doorzoeking

In cybercrimeonderzoeken zullen in de meeste gevallen computers in beslag worden genomen tijdens een doorzoeking van een plaats.[129] Computers zijn vatbaar voor inbeslagname, omdat zij kunnen dienen als middel om de waarheid aan het licht te brengen (art. 94 Sv).[130] Vaak zal de inbeslagname plaatsvinden tijdens een doorzoeking van een woning. Een rechter-commissaris moet uiteraard een machtiging afgeven om een woning te doorzoeken. Deze situatie is gevisualiseerd in Figuur 4.1.



Figuur 4.1: doorzoeking van een woning en inbeslagname van computers.

Figuur 4.1 illustreert hoe elke computer binnen een woning vatbaar is voor inbeslagname. De opsporingsambtenaar, officier van justitie en rechter-commissaris moeten uiteraard een inschatting maken in hoeverre de inbeslagname van het voorwerp, inclusief de daarop opgeslagen gegevens, subsidiair proportioneel is. Computers mogen alleen in beslag worden genomen als een verband bestaat tussen het voorwerp en het te onderzoeken strafbare feit.[131] In kinderpornozaken is het bijvoorbeeld gebruikelijk alle gegevensdragers in beslag te nemen.

129 Zie ook het WODC rapport van Mevis, Verbaan, & Salverda (2016, p. 52) die aangeven dat computers meestal tijdens een doorzoeking in beslag worden genomen.

130 Zie ook HR 29 maart 1994, NJ 1994, 577 m.nt. Sch. De Hoge Raad bepaalde in dit arrest dat voor de waarheidsvinding onderzoek mag worden gedaan naar inbeslaggenomen voorwerpen ten einde gegevens voor het strafrechtelijk onderzoek ter beschikking te krijgen. In computers opgeslagen gegevens zijn daarvan niet uitgezonderd.

131 Zie ook Aanwijzing inbeslagneming (Artikel 94 Wvsv), *Stcrt.* 2010, 19117.

4.1.2 Gebrek aan een procedure voor onderzoek in computers

Wegens het ontbreken van een (publiekelijk toegankelijke) landelijke procedure voor de inbeslagname en het daaropvolgend onderzoek van gegevens in computers is het onduidelijk hoe de inbeslagname precies in zijn werking gaat.[132] Ik krijg de indruk dat in de gevallen waar de gehele computer in beslag wordt genomen een image van de harde schijven wordt gemaakt om deze nader te onderzoeken met behulp van forensische software. Met behulp van filters kan eventueel meer specifiek gezocht worden naar bewijs.[133]

Het is ook mogelijk onderzoek te doen op een computer die nog 'open' staat. De eventuele encryptie van de gegevens op de harde schijf is dan nog niet ingegaan. Om te voorkomen dat de verdachte snel zijn computer uitzet, worden doorzoekingen en de daarop volgende inbeslagname van de computer van de verdachte goed gepland.[134] Bovendien kan met behulp van deze *'live forensics'* worden nagegaan welke bewoners gebruikmaken van de computer en met welke apparaten of servers de computer in verbinding staat.[135] Voor het zoeken in aangesloten computers binnen een netwerk is een aparte grondslag (de netwerkzoeking) in het Wetboek van Strafvordering gecreëerd (zie paragraaf 4.3).

4.2 Bijzondere bescherming voor computers

In 2015 is de discussie in Nederland opgelaaid over de vraag of de bestaande wettelijke regeling voor de inbeslagname van computers en het daarbij horende nader onderzoek van opgeslagen gegevens voldoende is.[136] Moeten computers, vergeleken met andere 'voorwerpen' die vatbaar zijn voor inbeslagname, extra bescherming genieten? In computers liggen tenslotte foto's, video's en andere persoonlijke bestanden opgeslagen.[137] Het is vanwege het intieme karakter en hoeveelheid van gegevens die in computers kunnen worden opgeslagen, te beargumenteren dat computers niet hetzelfde zijn als andere voorwerpen.[138]

In de Verenigde Staten hebben de hoogste Amerikaanse rechters in een baanbrekend arrest gesteld dat altijd een '*warrant*' (een machtiging van een rechter) is vereist voor de inbeslagname van smartphones. Deze warrant is zelfs vereist als het apparaat direct na de arrestatie van de verdachte in beslag wordt genomen. Voorheen bestond daar een uitzondering op, onder de zogenaamde '*search-incident-to-arrest exception to the warrant requirement*'. Als toelichting bij deze beslissing legt het Amerikaanse 'Supreme Court' uit:

132 Zie ook Mevis, Verbaan & Salverda 2016, p. 78.

133 Zie ook Koops, Conings & Verbruggen 2016, p. 77.

134 Zie ook Casey e.a. 2011, p. 131 en de gebeurtenissen in de Silk Road-zaak (Joshuah Bearman, 'Silk Road: The Untold Story', *Wired*, 23 mei 2015. Beschikbaar op: http://www.wired.com/2015/05/silk-road-untold-story/ (laatst geraadpleegd op 30 december 2016).

135 Zie meer uitgebreide informatie over live forensics bijvoorbeeld Casey e.a. 2011, p. 132.

136 Zie Hof Arnhem-Leeuwarden 22 april 2015, ECLI:NL:GHARL:2015:2954, m.nt. J.J. Oerlemans, *Computerrecht* 2015, nr. 4, 210-215. en HR 25 oktober 2016, ECLI:NL:PHR:2016:1049, met concl. A-G, r.o. 70-83. Zie ook Koops, Conings & Verbruggen 2016, p. 78-80.

137 Zie ook het discussiestuk 'Onderzoek ter plaatse, inbeslagneming en doorzoeking en onderzoek van gegevensdragers en in geautomatiseerde werken', 4 juni 2014, p. 52-53. Beschikbaar op: https://www.rijksoverheid.nl/documenten/publicaties/2014/06/06/onderzoek-ter-plaatse-inbeslagneming-en-doorzoeking-en-onderzoek-van-gegevensdragers-en-in-geautomatiseerde-werken-discussiestuk (laatst geraadpleegd op 2 januari 2017). Zie ook Hof Arnhem-Leeuwarden 22 april 2015, ECLI:NL:GHARL:2015:2954, m.nt. J.J. Oerlemans, *Computerrecht* 2015, nr. 4, 210-215.

138 Zie ook bijvoorbeeld Groothuis & De Jong (2010, p. 280), Conings & Oerlemans (2013, p. 2) en Koops, Conings & Verbruggen (2016, p. 81-82). Zij pleiten voor een beschermingsniveau dat enigszins vergelijkbaar is met een doorzoeking van een woning.

"Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life' (...). The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple - get a warrant."[139]

Ook in Nederland buigt de Hoge Raad zich op het moment van schrijven (januari 2017) over de vraag of de huidige regeling voor de inbeslagname van computers in strijd is met het recht op privacy zoals bedoeld in art. 8 EVRM. Advocaat-Generaal Bleichrodt betoogde in zijn conclusie dat er onvoldoende waarborgen gelden binnen de Nederlandse regeling.[140] Het EHRM lijkt een machtiging van een onderzoeksrechter te prefereren als er sprake is van inbeslagname en een daaropvolgend onderzoek van gegevens die liggen opgeslagen in computers.[141] De Minister van Veiligheid en Justitie, Van der Steur, heeft in juni 2015 te kennen gegeven de huidige Nederlandse regeling te willen aanpassen, gezien de ernstige inmenging met het recht op privacy dat de inbeslagname van computers met zich meebrengt. Het is echter nog onduidelijk hoe een gewijzigde regeling er in concept uit zal zien. Een belangrijke vraag die beantwoord zal moeten worden, is of het wenselijk is dat een bevel van een officier van justitie als voldoende waarborg wordt beschouwd of dat daarbij nog een machtiging van een rechter-commissaris wenselijk is.[142] Bovendien is het de vraag of een bevel of machtiging is gepast bij de inbeslagname of tijdens het daaropvolgende onderzoek van de gegevens die staan opgeslagen op de gegevensdrager. Een aspect dat in deze discussie opvallend afwezig is, is de vraag op welke wijze moet worden omgegaan met het veilig stellen van gegevens die opgeslagen zijn op servers elders (ook wel 'in de cloud' genoemd). Mijns inziens zou bovendien een uniforme procedure voor de inbeslagname van computers op landelijk niveau wenselijk zijn. Daarnaast moet worden nagedacht over de privacyinmenging die plaatsvindt als software steeds beter in staat is grote hoeveelheden gegevens te analyseren, visualiseren, en in verband te brengen met andere gegevens die zijn verkregen binnen de politieorganisatie.

4.3 De netwerkzoeking

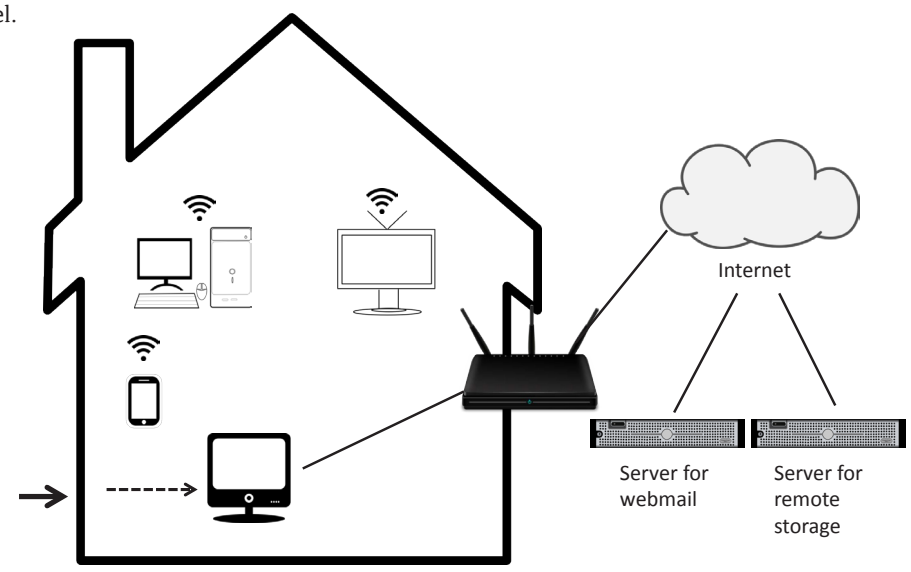
De netwerkzoeking is een opsporingsbevoegdheid die het mogelijk maakt om computers in aanliggende netwerken tijdens een doorzoeking te doorzoeken. De opsporingsbevoegdheid mag dus alleen worden toegepast tijdens een doorzoeking van een plaats. Met een netwerkzoeking kunnen bijvoorbeeld andere computers (zoals laptops, pc's, mediaspelers en harde schijven) die zijn aangesloten op een intranet worden doorzocht. Ook is het mogelijk tijdens een doorzoeking van een kantoorpand met een netwerkzoeking bijvoorbeeld de mailserver van het bedrijf in een datacentrum te doorzoeken. Het idee is dat voor die extra doorzoeking niet nog eens een aparte bevoegdheid behoef te worden ingezet. In de memorie van toelichting is destijds ook nadrukkelijk aangegeven dat de netwerkzoeking niet verder mag reiken dan die systemen waartoe de personen of werknemers van de plek waar de doorzoeking plaatsvindt, gerechtigd zijn.[143]

De voorwaarden om een netwerkzoeking uit te voeren, is afhankelijk van de locatie waar een doorzoeking plaatsvindt.[144] De regeling van de netwerkzoeking in art. 125j Sv verwijst namelijk terug naar de doorzoekingsbepalingen binnen het Wetboek van Strafvordering. Ter illustratie, tijdens een opsporingsonderzoeken naar misdrijven als omschreven in art. 67 Sv, kunnen opsporingsambtenaren een netwerkzoeking uitvoeren:

1. in een auto;
2. in elke andere plaats (behalve woningen of kantoren van mensen met geheimhouderstukken), nadat toestemming is verkregen van een officier van justitie;
3. in een woning of kantoor van een verschoningsgerechtigde, nadat een toestemming is verkregen van een officier van justitie en een machtiging van een rechter-commissaris is verkregen.[145]

4.3.1 Reikwijdte van de netwerkzoeking

De netwerkzoeking als opsporingsmethode is gevisualiseerd in figuur 4.2. Naar verwachting vindt de netwerkzoeking meestal plaats tijdens een doorzoeking van een woning, dus dat is het uitgangspunt in het model.



Figuur 4.2: Visualisatie van de netwerkzoeking.

139 U.S. Supreme Court, 25 juni 2014, *Riley v. California*, 573 U.S., r.o. 32 (2014).
140 Zie HR 25 oktober 2016, ECLI:NL:PHR:2016:1049, met concl. A-G, r.o. 70-83.
141 Zie o.a. EHRM 3 juli 2012, *Robathin t. Australië*, nr. 30457/06, § 48 en EHRM 30 september 2014, *Prezhdarovi t. Bulgarije*, nr. 8429/05, § 49. In de zaak *Petri Sallinen e.a. t. Finland* (27 september 2005, nr. 50882/99) merkte het hof op dat zij zeer verrast was door het gebrek aan toezicht door een rechter of onafhankelijk toezicht. In deze laatste zaak betrof het een doorzoeking van een advocatenkantoor. Vanwege de geheimhoudersstukken was in dit geval ook sprake van een bijzondere situatie.
142 Zie het discussiestuk 'Onderzoek ter plaatse, inbeslagneming en doorzoeking en onderzoek van gegevensdragers en in geautomatiseerde werken', 4 juni 2014, p. 52-53.
143 *Kamerstukken II* 1989/90, 21 551, nr. 3 (MvT Wet computercriminaliteit I), p. 27.
144 Verschillende auteurs, waaronder ikzelf, hebben hierop kritiek geleverd. De privacybescherming van het onderzoek van gegevens op computers zou niet moeten afhangen van de locatie van de computers. Zie Koops e.a. 2012b, p. 59 en Conings & Oerlemans 2013, p. 26.
145 De juridische basis is dan respectievelijk (1) art. 125j Sv jo art. 96b Sv, (2) art. 125j Sv jo art. 96c Sv en (3) art. 125j Sv jo art. 110 or 97 Sv. Zie ook Conings & Oerlemans 2013, p. 24.

Figuur 4.2 illustreert hoe tijdens de doorzoeking van een woning toegang kan worden verkregen tot andere computers, zoals servers, in een datacentrum. In de discussiestukken die beschikbaar zijn gesteld voor het project Modernisering Strafvordering, stellen de auteurs dat de netwerkzoeking ook kan strekken tot een doorzoeking van een webmailaccount (zoals Gmail) of een online opslagdienst (zoals Dropbox).[146] Mijns inziens houdt de tekst van het artikel als zodanig deze interpretatie van de bevoegdheid niet tegen, voor zover de bevoegdheid tijdens een doorzoeking van een plaats wordt ingezet.[147] Het probleem is echter dat de beschikbare wetsgeschiedenis geen enkele indicatie geeft van deze toepassing van een netwerkzoeking. Dat is ook niet verassend, aangezien het grootste deel van de beschikbare wetgeschiedenis afkomstig is van de memorie van toelichting op de Wet computercriminaliteit I in 1990.

4.3.2 Grensoverschrijdende netwerkzoeking

In de Wet computercriminaliteit II wordt erop gewezen dat de bevoegdheid niet mag leiden tot het doorzoeken van gegevens die opgeslagen liggen in een computer in het buitenland.[148] Koops e.a. (2012b, p. 36) hebben beargumenteerd dat de netwerkzoeking strikt genomen niet strekt tot een doorzoeking van bijvoorbeeld webmail van een Amerikaanse provider, omdat redelijkerwijs mag worden aangenomen dat deze gegevens in het buiteland liggen opgeslagen. In mijn dissertatie heb ik betoogd dat het mogelijk zou moeten zijn onder een netwerkzoeking toegang te verschaffen tot de webmail of online opslagdienst waarvan een verdachte op Nederlands grondgebied gebruikmaakt. De benodigde logingegevens zijn niet zelden te vinden in de apps op een smartphone of cookies van de browsergeschiedenis op een tablet of computer.

De doorzoeking is theoretisch gezien begrensd tot de Nederlandse landsgrenzen is omdat een grensoverschrijdende netwerkzoeking inbreuk zou maken op de territoriale soevereiniteit van een ander land. Toch zie ik niet in hoe tijdens een Nederlands opsporingsonderzoek en tijdens (of wellicht direct na) een doorzoeking op Nederlands grondgebied, slechts het toegang verschaffen en eventueel kopiëren van gegevens een ontoelaatbare inbreuk op de soevereiniteit van een andere staat oplevert.[149] Binnen het Cybercrime Verdrag wordt een dergelijke extraterritoriale netwerkzoeking niet expliciet legitiem, noch verboden verklaard.[150] Toch moet erop worden gewezen dat op grond van het 'geldende internationale recht', grensoverschrijdende doorzoekingen van computers zonder verdragsbasis of toestemming van de betrokken staat niet is toegestaan.[151] In de memorie van toelichting van de wet computercriminaliteit II en III wordt ook wel opgemerkt dat indien de locatie van de gegevens niet redelijkerwijs kan worden vastgesteld, bijvoorbeeld wanneer cloudcomputingtechnieken gebruikt worden, een grensoverschrijdende zoeking op afstand is toegestaan.[152]

4.4 Slotbeschouwing

Dit hoofdstuk heeft laten zien dat computers op het moment van schrijven (januari 2017) nog worden gezien als elk ander voorwerp dat binnen een opsporingsonderzoek voor de waarheidsvinding in beslag kan worden genomen. Vervolgens kan nader onderzoek worden gedaan naar de opgeslagen gegevens in computers. De laatste jaren is echter steeds meer discussie over de vraag of de regeling voor de inbeslagname van computers nog voldoende is. De Hoge Raad en wetgevingsjuristen buigen zich daarom over de vraag of meer waarborgen moeten gelden voor de inbeslagname van computers en/of het daaropvolgende onderzoek van gegevens. Het is uiteindelijk aan de Nederlandse wetgever om de regeling aan te passen. Ik heb betoogd dat op dit punt aanpassingen binnen het Wetboek van Strafvordering noodzakelijk zijn en dat daarnaast een uniforme procedure over de inbeslagname van computers en het daaropvolgende onderzoek naar de gegevens moet worden gemaakt.

De netwerkzoeking kan tijdens een doorzoeking worden uitgevoerd en strekt zich ook uit tot aangesloten computers (of servers) op andere plaatsen. De netwerkzoeking maakt het bijvoorbeeld mogelijk de mailserver in een datacentrum elders in Nederland te doorzoeken. Er bestaat echter onduidelijkheid over gegevens die in het buitenland liggen opgeslagen, zoals een netwerkzoeking binnen een webmailserver. Strikt genomen mogen deze gegevens niet worden ingekeken of worden gekopieerd zonder verdragsbasis of toestemming van de betrokken staat. Wellicht vraagt dit om meer flexibiliteit. Juristen die zich bezighouden met het project Modernisering Strafvordering leken ervan uit te gaan dat een netwerkzoeking binnen een Gmail-mailbox of Dropbox reeds mogelijk is. Het verdient aanbeveling de reikwijdte over de netwerkzoeking mee te nemen bij het vraagstuk over de inbeslagname en onderzoek van gegevens op computers. Tegenwoordig liggen gegevens immers steeds vaker elders (in de cloud) opgeslagen.

146 Zie het discussiestuk 'Onderzoek ter plaatse, inbeslagneming en doorzoeking en onderzoek van gegevensdragers en in geautomatiseerde werken' van 6 juni 2014, p. 52-53.

147 Indien een Gmail-account van buitenaf, dus niet tijdens een doorzoeking, wordt ingezet is sprake van een online doorzoeking. Dat is een vorm van hacken als opsporingsmethode die in hoofdstuk 6 wordt behandeld.

148 Zie *Kamerstukken II* 2004/05, 26 671, nr. 10, p. 13. Ingeval de locatie van de gegevens niet helder is, mag de netwerkzoeking toch worden toegepast. Zie *Kamerstukken II* 2004/05, 26 671, nr. 10, p. 23.

149 Praktisch gezien is het bovendien lastig aan te wijzen waar de gegevens liggen opgeslagen en van welke staat de territoriale soevereiniteit zou worden geschonden.

150 Zie ook het Explanatory Report bij het Cybercrimeverdrag, §293, beschikbaar op http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm (laatst geraadpleegd op 4 januari 2016).

151 Zie *Kamerstukken II* 1989/90, 21 551, nr. 3 (MvT Wet Computercriminaliteit I), p. 11-12. Zie uitgebreid Koops & Goodwin 2014. Overigens stellen ook deze auteurs op p. 79 van hun rapport, dat een unilaterale potentieel grensoverschrijdende netwerkzoeking vanuit een doorzoeking op een Nederlandse plek geen zeer ernstige soevereiniteitsinbreuk oplevert.

152 Zie *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT Wet computercriminaliteit III), p. 51-52. Zie ook *Kamerstukken II* 2000/01, 23 530, nr. 45, p. 4.

5 Vorderen van gegevens bij online serviceproviders

In dit hoofdstuk wordt de opsporingsmethode van het vorderen van gegevens bij online serviceproviders besproken. Daarbij wordt ingegaan op de bevoegdheden in het Wetboek van Strafvordering voor de volgende vier typen gegevens: (1) gebruikersgegevens, (2) verkeersgegevens, (3) andere gegevens en (4) inhoudelijke gegevens.

In paragraaf 5.1 wordt eerst aangegeven wat het belang is van het vorderen van gegevens bij online serviceproviders in cybercrimezaken. In paragraaf 5.2 wordt de wetsystematiek van de bevoegdheden voor het vorderen van gegevens binnen het Wetboek van Strafvordering toegelicht. De juridische basis en reikwijdte van de vier categorieën van gegevens worden geanalyseerd in paragraaf 5.3-5.6. Het hoofdstuk wordt afgesloten in paragraaf 5.7 met een slotbeschouwing.

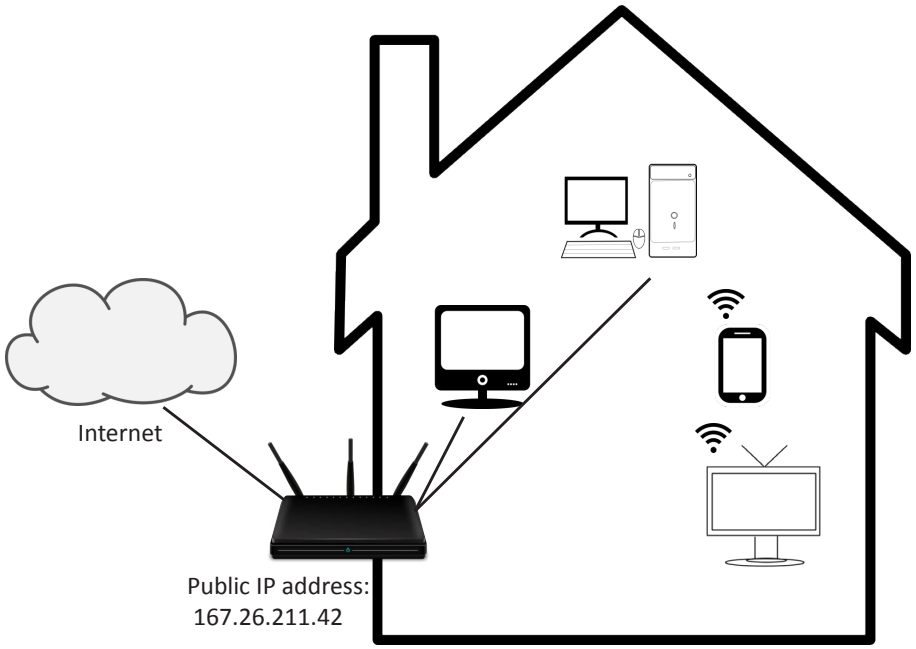
5.1 Het belang van gegevens bij online serviceproviders

Het vorderen van gegevens bij online serviceproviders is een niet te onderschatten opsporingsmethode in cybercrimeonderzoeken. De reden daarvoor is dat gebruikersgegevens kunnen leiden tot identificatie van een verdachte. Dat gaat in veel gevallen als volgt te werk. Na aangifte van een cybercrimedelict of naar aanleiding van digitaal forensisch onderzoek komt vaak een IP-adres bovendrijven. Het betreft in zo'n geval het IP-adres van een computer waarvan de verdachte vermoedelijk gebruik heeft gemaakt. Met behulp van online tools kan via de Whois-database de online serviceprovider worden opgezocht waartoe het IP-adres behoort. Het IP-adres in combinatie met een bedrijf of instelling waar gegevens gevorderd kunnen worden, kan uiteindelijk leiden tot identificatie van de verdachte.[153] In paragraaf 5.1.1-5.1.3 worden drie situaties besproken waar gegevens beschikbaar kunnen zijn, namelijk bij breedband internetproviders, anonimiseringsdienstverleners en andere online serviceproviders.

5.1.1 Gegevens bij breedband internetproviders

In het beste geval behoort het IP-adres toe aan een breedband internetaanbieder, zoals KPN of Ziggo in Nederland. Meestal kan de online serviceprovider zijn klant identificeren op basis van het IP-adres. De serviceprovider gaat na aan welke klant het IP-adres is gedistribueerd (op een bepaalde datum en tijdstip). Het IP-adres is in deze situatie toegewezen aan de router van waaruit ook vaak wifi en gekabeld internet in huis wordt verspreid. Dit wordt gevisualiseerd in Figuur 5.1.

153 Zie ook Clayton 2004, p. 17-25.



Figuur 5.1: Model van een thuisnetwerk.

Met een vordering tot gebruikersgegevens kan een opsporingsambtenaar de naam en het adres van de klant van de online serviceprovider vorderen.[154] Op basis van deze adresgegevens kan vervolgens via het GBA-register worden nagegaan of de verdachte ook op het adres woonachtig is. Vervolgens kan tijdens een huiszoeking de computer(s) van de verdachte worden veilig gesteld. Met behulp van digitaal forensisch onderzoek en de gebruikelijke onderzoeksmethoden, zoals het ondervragen van de bewoners, kan mogelijk meer bewijs worden vergaard. Toch moet niet onderschat worden hoe lastig het is bewijs van een cybercrime te vinden; zelfs in de hierboven geschreven ideale situatie waarbij de verdachte gebruikmaakt van zijn eigen thuisnetwerk, moet bewezen worden dat een bepaald individu achter het toetsenbord zat toen het misdrijf werd gepleegd.

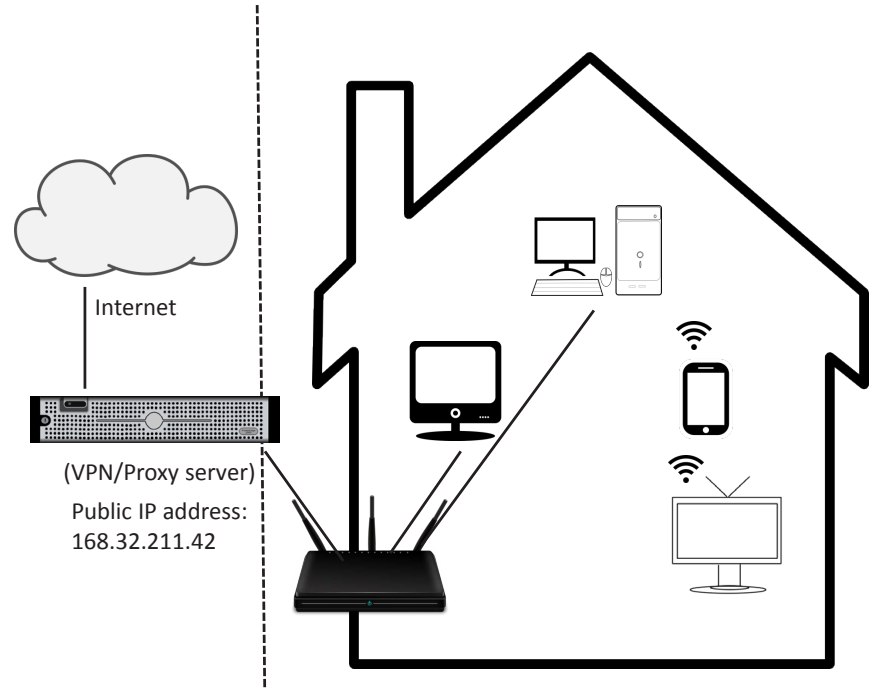
5.1.2 Gegevens bij anonimiseringsdienstverleners

In veel gevallen maken cybercriminelen ook gebruik van anonimiseringstechnieken. Het gebruik van Tor is al in hoofdstuk 2 beschreven. In dat geval heeft het geen zin gegevens te vorderen, zelfs als de exit relay van Tor lokaliseerbaar is. Zoals in het hoofdstuk 2 is uitgelegd kan het gebruik van undercover opsporingsmethoden mogelijk toch resultaat opleveren. Hacken als opsporingsmethode zou in dit geval ook

154 Zie ook uitgebreid: Clayton 2004, p. 17-25.

een oplossing kunnen zijn voor het anonimiteitsprobleem. Deze opsporingsmethode wordt besproken in hoofdstuk 6.

Ingeval de verdachte gebruikmaakt van een proxy- en/of VPN-dienst wordt het netwerkverkeer naar een server in een datacentrum omgeleid. Deze situatie wordt gevisualiseerd in Figuur 5.2.



Figuur 5.2: Model van een thuisnetwerk met gebruikmaking van een proxy- of VPN-dienstverlener.

Figuur 5.1 maakt duidelijk hoe in dit geval het spoor niet direct leidt tot de woning van de verdachte, maar de server van de proxy- of VPN-dienstverlener. Als de proxy- of VPN-dienstverlener lokaliseerbaar is, kunnen mogelijk gebruikersgegevens van de dienstverlener gevorderd worden. Zoals in 2011 een hacker van het LulzSec-collectief heeft mogen ervaren, kan dit tot identificatie van de verdachte leiden.[155] Maar ook financiële gegevens, zoals een betaling voor dienst met een creditcard of een online betalingsdienst als PayPal kan waardevolle informatie en een verder spoor opleveren dat kan leiden tot de identificatie van de verdachte.

155 Zie A. Martin, 'LulzSec hacker exposed service he thought would hide him', *The Atlantic Wire*. Beschikbaar op: http://www.theatlanticwire.com/technology/2011/09/lulzsec-hacker-exposed-service-he-thought-would-hide-him/42895/ (laatst geraadpleegd op 27 december 2016). Helaas komt het veel voor dat nepgegevens worden ingevuld of zelfs van de identiteitsgegevens van anderen gebruik wordt gemaakt.

5.1.3 Gegevens bij andere online serviceproviders

Waardevolle informatie kan natuurlijk ook liggen bij webmaildiensten zoals Hotmail (nu: 'Outlook mail' geheten) en Gmail, online forums waarop de verdachte actief is en sociale mediadiensten (zoals Facebook). Het is niet altijd eenvoudig of mogelijk deze gegevens te verkrijgen, mede omdat veel dienstaanbieders in het buitenland zijn gevestigd en vaak slechts onder de voorwaarden van een bepaald rechtssysteem de gegevens verstrekken. Toch kan in het algemeen worden gesteld dat het eenvoudiger is gebruikersgegevens en verkeersgegevens te vorderen dan profielgegevens (incl. foto's) en privéberichten die over en weer zijn verstuurd. In het overige deel van dit hoofdstuk zal uitvoerig worden ingegaan op de wetgeving omtrent het vorderen van gegevens in Nederland.

5.2 Wetssystematiek vorderen van gegevens

Het stelsel van het vorderen van gegevens door de Nederlandse politie en justitie is complex. De reden is dat er *twee* juridische raamwerken voor het vorderen van gegevens in het Wetboek van Strafvordering gelden. Daarnaast bestaan er veel verschillende categorieën gegevens die allemaal onder verschillende bevoegdheden moeten worden gevorderd.[156]

Enerzijds kunnen er gegevens worden gevorderd (1) bij aanbieders van elektronische communicatiediensten en anderzijds (2) anderzijds bij *een ieder*, zoals een persoon, bedrijf, of instelling.[157] Hierdoor dringt de vraag zich op onder welk regime het vorderen van gegevens bij online serviceproviders valt. In de regel zullen online serviceaanbieders bestempeld kunnen worden als elektronische communicatiediensten.[158] Internet access providers (die toegang tot internet faciliteren), VPN-diensten, sociale mediadiensten, en online forums, verlenen bijvoorbeeld elektronische communicatiediensten. Twijfel kan bestaan over bijvoorbeeld hosting providers, maar ook daarvan wordt aangenomen dat het bijna altijd elektronische communicatiediensten zullen zijn. Om deze reden wordt in dit hoofdstuk alleen het regime omtrent het vorderen van gegevens van aanbieders van elektronische communicatiediensten behandeld. Indien in de praktijk een dienstaanbieder toch geen elektronische communicatiedienst is, kan altijd een vordering uit het andere regime worden ingezet.[159]

156 De Hoge Raad heeft in 2011 in een arrest bevestigd dat de politie gegevens moet vorderen (HR 21 December 2010, ECLI:NL:HR:2010:BL7688). Het is niet toegestaan om het afgeven van de gegevens te verzoeken. Wel is het mogelijk dat een partij bij aangifte vrijwillig gegevens verstrekt (zoals logbestanden of ander bewijs dat ze zelf hebben verzameld).

157 Zie de Wet vorderen gegevens telecommunicatie, *Stb.* 2004, 105 en de Wet vorderen gegevens, *Stb.* 2005, 390. Voor het vorderen van gegevens bij geheimhouders of verschoningsgerechtigden gelden bijzondere regels. Deze worden in deze korte studie niet behandeld. De Commissie Van Traa had al in 1996 aanbevolen opsporingsbevoegdheden te creëren in het Wetboek van Strafvordering voor het vorderen van gegevens bij derden door opsporingsdiensten (*Kamerstukken II* 1995/96, 24 072, nr. 11, p. 466). De aanbevelingen van de Commissie Mevis uit 2011 (Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij) hebben uiteindelijk geleid tot de Wet vorderen gegevens.

158 Zie ook Koops e.a. 2012b, p. 42.

159 Zie paragraaf 2.3 van de Aanwijzing bijzondere opsporingsbevoegdheden. Zie ook *Kamerstukken II* 2003/04, 29 441, nr. 3 (MvT Wet vorderen gegevens), p. 13-14.

Voor het vorderen van gegevens in cybercrimezaken worden de volgende relevante categorieën onderscheiden: (1) gebruikersgegevens, (2) verkeersgegevens, (3) andere gegevens en (4) inhoudelijke gegevens.[160] Het juridisch kader voor het vorderen van gegevens in deze categorieën wordt in paragraaf 5.3-5.6 toegelicht.

5.3 Vorderen van gebruikersgegevens

De volgende gegevens kunnen worden gevorderd met een vordering met betrekking tot gebruikersgegevens: (1) naam, (2) adres, (3) postcode, (4) woonplaats, (5) nummer en (6) soort dienst van een gebruiker van een communicatiedienst.[161] Uit de memorie van toelichting wordt duidelijk dat met de categorie 'nummers' ook e-mailadressen en IP-adressen worden bedoeld.[162]

Gebruikersgegevens kunnen worden gevorderd in opsporingsonderzoeken naar misdrijven zoals omschreven in art. 67 Sv en moeten op bevel van een opsporingsambtenaar worden afgegeven.

Uit de beschikbare jurisprudentie op rechtspraak.nl valt op dat gebruikersgegevens op basis van een IP-adres opvallend vaak in kinderpornozaken worden gevorderd.[163] Een mogelijke verklaring is dat een verdacht IP-adres vaak door online serviceproviders wordt overgedragen of door buitenlandse politiediensten naar Nederlandse autoriteiten wordt verstuurd. In de aangehaalde zaken leidde het IP-adres in combinatie met gebruikersgegevens vaak tot een huiszoeking, waarna - na analyse van de aanwezige gegevensdragers - het bezit van kinderporno kon worden bewezen. Ik verwacht een toename van dit type vordering bij sociale mediadiensten ten behoeve van cybercrimeonderzoeken waarbij de verdachte moet worden geïdentificeerd en ten behoeve van bewijsmateriaal bij delicten als smaad en belediging die steeds vaker in een online context worden gepleegd.

5.4 Vorderen van verkeersgegevens

Verkeersgegevens betreffen eenvoudig gezegd gegevens over de (1) tijd, (2) duur, (3) gebruikte apparatuur, (4) afgenomen diensten en (5) de locatie van het netwerkaansluitpunt bij een communicatie of van de geografische positie van de randapparatuur van een gebruiker.[164] In art. 2 van het Besluit vorderen telecommunicatiegegevens zijn verkeersgegevens nader gespecifieerd die bij telecommunicatieaanbieders kunnen worden gevorderd. Verkeersgegevens kunnen worden gevorderd op bevel van officier van justitie in opsporingsonderzoeken naar misdrijven zoals omschreven in art. 67 Sv.[165] Met de vordering in art. 126n Sv kunnen overigens ook gebruikersgegevens worden gevorderd.

160 Zie bijvoorbeeld T-CY 2016, p. 12. Deze werkgroep onderscheidt drie relevante categorieën van gegevens, namelijk gebruikersgegevens, verkeersgegevens en inhoudelijke gegevens.

161 Art. 126na Sv.

162 *Kamerstukken II* 2001/02, 28 059, nr. 3 (MvT Wet vorderen gegevens telecommunicatie), p. 11.

163 Zie, bijvoorbeeld, Rb. Groningen, 22 oktober 2009, ECLI:NL:RBGRO:2009:BK1004, Rb. Noord-Nederland, 4 februari 2013, ECLI:NL:RBNNE:2013:BZ9666, Rb. Noord-Holland, 10 september 2015, ECLI:NL:RBNHO:2015:8404 en Hof Den Haag, 17 november 2015, ECLI:NL:GHDHA:2015:3257.

164 Zie uitgebreid Koops & Smits 2014 over het onderscheid tussen verkeersgegevens en inhoudelijke gegevens.

165 Zie art. 126n Sv.

Alle beschikbare gegevens kunnen met de juiste vordering bij online serviceproviders worden gevorderd. De Wet bewaarplicht verplichtte in het verleden aanbieders van openbare telecommunicatiediensten en -netwerken om gebruikersgegevens en verkeersgegevens voor een bepaalde duur te bewaren, zodat ze op een later moment gevorderd kunnen worden door opsporingsdiensten. Aanbieders van openbare telecommunicatiediensten en -netwerken zijn *niet gelijk* aan aanbieders van elektronische communicatiediensten. Eenvoudig gezegd bieden aanbieders van openbare telecommunicatiediensten en -netwerken de internettoegangsdiensten zelf, terwijl de online communicatiediensten diensten aanbieden over de infrastructuur heen, zoals sociale mediadiensten. Diensten zoals Facebook, Skype en Whatsapp vallen dan ook niet onder de (huidige) telecommunicatiewet en hoeven geen aftapinfrastructuur te installeren om taps te installeren. Dit is de reden dat een telefoontap of internettap op een telefoon of breedbandinternetverbinding kan worden gezet, maar (tot nog toe) geen tap kan worden gezet bij een sociale mediadiensten om privéberichten te onderscheppen.[166] Deze laatstgenoemde diensten zijn niet verplicht een tapinfrastructuur op basis van de Telecommunicatiewet te implementeren om de interceptie van gesprekken voor opsporingsdiensten te faciliteren.

De stevige privacyinmenging die de bewaarplicht en het vorderen van verkeersgegevens met zich kan meebrengt, hebben tot rechtszaken geleid. De Europese richtlijn voor de bewaarplicht is in 2014 ongeldig verklaard en de Nederlandse Wet bewaarplicht in 2015.[167] Met een nieuw 'concept Wet bewaarplicht' is de sterkere waarborg van een machtiging van een rechter-commissaris (naast het bevel van een officier van justitie) voor het vorderen van verkeersgegevens geïntroduceerd.[168] Op 21 december 2016 heeft het Hof van Justitie echter geoordeeld dat de bewaarplicht als algemene maatregel op zichzelf niet toelaatbaar is en beperkt moet zijn door 'objectieve elementen'.[169] Het is op het moment van schrijven (januari 2017) nog niet duidelijk of de Wet bewaarplicht voor telecommunicatiegegevens in Nederland zal terugkeren.

Alle beschikbare gegevens bij aanbieders van openbare telecommunicatiediensten en -netwerken en online serviceproviders kunnen echter gevorderd worden. Naast de gebruikersgegevens die noodzakelijk zijn bij de registratie van de dienst, zijn in veel gevallen ook loggegevens beschikbaar die bestaan uit verkeersgegevens. Het genereren van deze gegevens is vaak noodzakelijk voor de dienstverlening en beveiliging van netwerken. Zonder een bewaarplicht worden deze gegevens echter niet voor een bepaalde tijd opgeslagen, zodat de beschikbaarheid van deze gegevens in opsporingsonderzoeken naar ernstige misdrijven voor opsporingsdiensten niet is verzekerd.

5.5 Vorderen van 'andere gegevens'

Gegevens die vallen onder de categorie 'andere gegevens' kunnen worden beschreven als gegevens die geen gebruikersgegevens, verkeersgegevens of inhoudelijke gegevens zijn. Het betreffen bijvoorbeeld registratiegegevens van gebruikers bij een website, zoals betalingsgegevens.[170] Ook kan worden gedacht aan profielgegevens van een internetgebruiker. Met de vordering in art. 126nd Sv kunnen 'andere gegevens' worden gevorderd van online serviceproviders, nadat een bevel van een officier van justitie is verkregen. Dit geldt alleen voor opsporingsonderzoeken naar delicten zoals omschreven in art. 67 Sv.[171]

Daar waar de gegevens gevoelige gegevens betreffen, zoals gegevens over geloofsovertuigingen, ras, politieke affiliatie, gezondheid, seksuele leven en lidmaatschap van een vakbond, gelden strengere eisen.[172] Hiervan kan bijvoorbeeld sprake zijn als foto's van individuen worden verkregen (wegens ras- en gezondheidsgegevens) of profielinformatie over religie of seksuele voorkeur wordt verkregen. Gevoelige gegevens kunnen alleen worden verkregen als ook een machtiging van een rechter-commissaris is afgegeven en het delict de 'rechtsorde ernstig schokt'. Bij cybercrimedelicten is het bijvoorbeeld de vraag of een 'eenvoudige hack' of DDoS-aanval[173] de rechtsorde ernstig schokt. Wanneer de aanvallen veel schade tot gevolg hebben of bijvoorbeeld vitale infrastructuren raken zal daar wel sprake van zijn.

De verkrijging van gevoelige gegevens kan ook van tevoren in een vordering worden uitgesloten. Ik benadruk op deze plaats dat opsporingsambtenaren en de officier van justitie *altijd* moeten nagaan of wat ze vorderen proportioneel is (wordt er niet meer gevraagd dan noodzakelijk?) en subsidiair is (zijn er minder ingrijpende alternatieven om de benodigde informatie te verkrijgen beschikbaar?).

5.6 Vorderen van inhoudelijke gegevens

De categorie 'inhoudelijke gegevens' is (nog) geen officiële categorie van gegevens binnen het Wetboek van Strafvordering. In de wetgeschiedenis en de Aanwijzing bijzondere opsporingsbevoegdheden wordt alleen aangegeven dat opgeslagen e-mails bij online serviceproviders moeten worden gevorderd op basis van art. 126ng lid 2 Sv.[174]

In art. 126ng Sv staat dat 'opgeslagen gegevens bij een aanbieder van elektronische communicatiediensten' slechts op bevel een officier van justitie kunnen worden gevorderd, nadat een machtiging van een rechter-commissaris is verkregen, voor zover het belang van het onderzoek dit dringend vordert, bij verdenking van misdrijven die een ernstige inbreuk op de rechtsorde opleveren.

De ratio voor deze strenge voorwaarden voor toepassing van de bevoegdheid ligt mede in het recht op bescherming van vertrouwelijke communicatie. Om deze reden mag ervan worden uitgegaan dat ook opge-

166 Zie uitgebreid Oerlemans 2012.
167 Zie HvJ EU 8 april 2014, C-293/12 (*Digital Rights Ierland t. Ierland*) en C-594/12 (*Seitlinger, Tschohl e.a.. t. Kärtner Landsregierung*) en Rb. Den Haag, 11 maart 2015, ECLI:NL:RBDHA:2015:2498.
168 Zie *Kamerstukken II* 2015/16, 34 537, nr. 2.
169 Zie HvJ EU 21 december 2016, C-203/15, ECLI:EU:C:2016:970 (*Tele2 Sverige AB t. Post-och telestyrelsen*).
170 Het is in deze context zelfs mogelijk 'toekomstige gegevens' te vorderen met art. 126ne Sv. De serviceprovider moet in dat geval de gegevens direct verstrekken aan de politie op het moment dat na de vordering nieuwe gegevens gegenereerd worden. Een interessante vraag is overigens of de vordering ook kan bewerkstelligen dat 'realtime' verkeersgegevens worden doorgestuurd naar de politie (o.g.v. art. 126ne Sv jo 126n Sv). Hierover wordt in de beschikbare bronnen (wetsgeschiedenis, jurisprudentie en de Aanwijzing opsporingsbevoegdheden) geen duidelijkheid gegeven.
171 Art. 126ng(1) jo art. 126nd Sv.
172 Zie art. 126ng(1) jo art. 126nf Sv.
173 Een 'Distributed Denial of Service'-aanval (ook wel verstikkingsaanval genoemd) is een aanval waarbij grote hoeveelheden internetverkeer naar een server worden verstuurd, waardoor deze overbelast raakt en minder goed bereikbaar is. Zie Blom 2007 voor een uitgebreide analyse van het begrip 'ernstige inbreuk op de rechtsorde'.
174 *Kamerstukken II* 2003/04, 29 441, nr. 3 (MvT Wet vorderen gegevens), p. 14. Zie ook het rapport van de Commissie Mevis van 2001, p. 89. Zie ook Rb. Rotterdam, 26 maart 2010, ECLI:NL:RBROT:2010:BM2520.

slagen privéberichten bij diensten als Facebook slechts onder deze strenge voorwaarden gevorderd kunnen worden. Daarnaast ben ik van mening dat ook opgeslagen documenten die beschikbaar kunnen zijn bij online serviceproviders zoals Google (met hun Google Drive-service), Microsoft (met Microsoft SkyDrive) en Dropbox, slechts onder de voorwaarden van art. 126ng lid 2 Sv gevorderd mogen worden.[175] In de Verenigde Staten kunnen deze inhoudelijke gegevens namelijk ook alleen maar worden verkregen onder een warrant. Deze wordt ook slechts onder een machtiging van een rechter afgegeven.[176] In Nederland is het vooralsnog onduidelijk of opgeslagen documenten onder art. 126ng lid 2 Sv moeten worden gevorderd of onder de minder strenge voorwaarden met een vordering tot 'andere gegevens' in art. 126ng jo art. 126nd Sv.[177] Deze vraag blijft natuurlijk theoretisch van aard zolang de gegevens van Amerikaanse online serviceproviders slechts met een Amerikaanse warrant kunnen worden verkregen.

5.7 Slotbeschouwing

Op basis van de analyse van de opsporingsmethode in dit hoofdstuk is Tabel 5.1 gemaakt. De tabel verschaft een overzicht van de juridische basis voor de bevoegdheden omtrent het vorderen van gegevens van online serviceproviders.

Categorie van gegevens	Juridische basis	Type gegevens	Voorwaarden
Gebruikersgegevens	126na Sv	Naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van een communicatiedienst.	Bevel opsporingsambtenaar.
Verkeersgegevens	126n Sv	Tijd, duur, gebruikte apparatuur, afgenomen diensten en locatiegegevens.	Bevel officier van justitie, in opsporingsonderzoeken naar misdrijven zoals omschreven in art. 67 Sv.
Andere gegevens	126nd Sv	O.a. betalingsgegevens en profielgegevens, niet zijnde gevoelige gegevens.	Bevel officier van justitie, in opsporingsonderzoeken naar misdrijven zoals omschreven in art. 67 Sv.
Inhoudelijke gegevens	126ng lid 2 Sv	Opgeslagen e-mail gegevens. Mogelijk andere inhoudelijke gegevens, zoals opgeslagen documenten.	Bevel officier van justitie, machtiging rechter-commissaris, indien het onderzoek het dringend vordert en de rechtsorde wordt geschaad, in opsporingsonderzoeken naar misdrijven zoals omschreven in art. 67 Sv.

Tabel 5.1: Overzicht van de juridische grondslag voor het vorderen van verschillende typen gegevens van online serviceproviders.

■

175 Zie Oerlemans 2017, p. 196-197.

176 Zie bijvoorbeeld de uitleg van Google over het vorderen van gegevens: https://www.google.com/transparencyreport/userdatarequests/legalprocess/ (laatst geraadpleegd op 27 december 2016). Daar wordt uitgelegd dat een Amerikaans huiszoekingsbevel is vereist om Google te dwingen tot "*openbaarmaking van gegevens met betrekking tot zoekopdrachten van de gebruiker en privé-inhoud opgeslagen op een Google-account, zoals Gmail-berichten, documenten, foto's en YouTube-video's*".

177 Zie ook Koops e.a. 2012b, p. 43-44.

In dit hoofdstuk is een aantal keer erop gewezen dat in de praktijk gegevens vaak moeten worden gevorderd bij Amerikaanse online serviceproviders. Microsoft geeft op haar website aan dat gebruikersgegevens en verkeersgegevens vaak via een lokaal advocatenkantoor (in Nederland) aangevraagd kunnen worden. Praktisch gezien is de Nederlandse regelgeving voor het vorderen van dit type gegevens zeer vergelijkbaar met de Amerikaanse regelgeving (in de '*Stored Communications Act*').[178] Via direct contact met de betreffende bedrijven kunnen gegevens redelijk snel worden verkregen, voor zover de Amerikaanse bedrijven hiervoor een procedure hebben en vrijwillig mee werken. Het vorderen van inhoudelijke gegevens in de vorm van e-mails of opgeslagen documenten moet vaak via rechtshulp en een Amerikaanse warrant. Binnen de Raad van Europa is een werkgroep bezig om het vorderen van gegevens bij buitenlandse online serviceproviders te stroomlijnen. Dit blijkt echter een moeizaam proces, maar wellicht kunnen resultaten worden geboekt met een geharmoniseerde procedure voor het direct vorderen van gebruikersgegevens en verkeersgegevens.[179] Gezien het feit dat het digitaal bewijs bij online serviceproviders vaak over verschillende jurisdicties ligt verspreid en veel mensen van buitenlandse communicatiediensten gebruikmaken, is het verder faciliteren van deze vorm van bewijsgaring van groot (opsporings-)belang.

■

178 Zie Oerlemans 2017, p. 316-323.

179 Zie TC-Y 2016.

6 Hacken als opsporingsmethode

In dit hoofdstuk wordt hacken als opsporingsmethode onderzocht. Daarbij wordt ingegaan op de volgende drie typen van hacken als opsporingsmethode: (1) de doorzoeking op afstand, (2) het gebruik van policeware en (3) het ontoegankelijk maken van gegevens op afstand.

In paragraaf 6.1 wordt de aanleiding voor het regelen van hacken als opsporingsmethode als bijzondere opsporingsbevoegdheid in de Wet computercriminaliteit III besproken. In paragraaf 6.2 wordt de reikwijdte en regeling van de doorzoeking op afstand geanalyseerd. Paragraaf 6.3 gaat in op het gebruik van policeware in de praktijk en de regeling van de opsporingsmethode in de Wet computercriminaliteit III. In paragraaf 6.4 wordt de toepassing van de bevoegdheid in de vorm van het ontoegankelijk maken van gegevens op afstand besproken. Het hoofdstuk wordt in paragraaf 6.5 afgesloten paragraaf met een slotbeschouwing.

6.1 Aanleiding tot normering van hacken als opsporingsmethode

Het wetsvoorstel Computercriminaliteit III is in december 2014 naar de Tweede Kamer gestuurd en op 21 december 2016 door de Tweede Kamer aangenomen.[180] De voorbereidingen voor een 'hackbevoegdheid' zijn echter terug te voeren tot 2009.

In een Kamerbrief uit 2009 gaf de toenmalige Minister van Justitie aan dat het opsporen van cybercrime door anonimiseringstechnieken en encryptie "extreem gecompliceerd" is geworden.[181] Om met deze problematiek om te gaan is in de Wet computercriminaliteit III een nieuwe opsporingsbevoegdheid voorgesteld om hacken mogelijk te maken.[182] De 'hackbevoegdheid' - officieel het 'toegang verschaffen op afstand tot een geautomatiseerd werk' genoemd - wordt geregeld in art. 126nba Sv. In paragraaf 6.1.1 wordt kort uitgelegd voor welke oplossingen de nieuwe opsporingsbevoegdheid moet zorgen. In paragraaf 6.1.2 wordt de tekst van de nieuwe opsporingsbevoegdheid geanalyseerd.

6.1.1 Beoogde oplossing voor problematiek binnen de opsporing

De voorgestelde hackbevoegdheid kan in bepaalde omstandigheden een oplossing voor het anonimiteitsprobleem in opsporingsonderzoeken bieden. Zoals in hoofdstuk 2 is uitgelegd kunnen internetgebruikers gebruikmaken van anonimiseringstechnieken, zoals Tor en proxy- en VPN-diensten, om hun eigen IP-adres te maskeren. Door hacken kan *rechtstreeks* toegang worden verschaft tot de computer waarvan een verdachte gebruikmaakt. Technisch gezien bestaat ook de mogelijkheid om met behulp van een program-

180 Zie *Kamerstukken II* 2015/16, 34 372, nr. 2 (Voorstel van Wet). De verwachting is dat het voorstel in 2017 wordt aangenomen.

181 Zie *Kamerstukken II* 2008/09, 28 684, nr. 232, p. 2-3.

182 In de praktijk is het wetsvoorstel enige malen ingezet op basis van art. 125i Sv jo art. 94 Sv (zie voor een overzicht: Oerlemans 2017, p. 258-261). Zie ook het 'Antwoord op Kamervragen van 17 oktober 2014 over het hacken van servers door de politie terwijl de zogenaamde hackwet nog niet door de Kamer is behandeld', beschikbaar op: https://www.rijksoverheid.nl/documenten/kamerstukken/2014/10/18/antwoorden-kamervragen-over-het-hacken-van-servers-door-de-politie-terwijl-de-zogenaamde-hackwet-nog-niet-door-de-kamer-is-beha (laatst geraadpleegd op 29 december 2016).

ma (ook wel '*policeware*'[183] genoemd, als zijnde de goedaardige variant van malware), het echte IP-adres van de gebruiker en andere identificerende gegevens naar opsporingsdiensten toe te sturen.[184]

Andere functies van policeware kunnen het vervolgens mogelijk maken om met de encryptieproblematiek om te gaan. Ten eerste houdt de encryptieproblematiek in dat het netwerkverkeer 'in transport' wordt versleuteld. Als gevolg daarvan is de inhoudelijke communicatie in onderschept netwerkverkeer via een telecommunicatietap niet meer leesbaar.[185] Door bijvoorbeeld op afstand de microfoon in een computer aan te zetten kunnen VoIP-gesprekken worden opgenomen en worden doorgestuurd naar de politie. Ook is het mogelijk met behulp van een '*keylogger*' toetsaanslagen van een computergebruiker af te vangen en deze later door te sturen naar politie. Op deze wijze wordt 'bij de bron' afgetapt nog voordat het communicatie wordt versleuteld.[186] Ten tweede houdt de encryptieproblematiek in dat gegevens 'in opslag' worden versleuteld. Na inbeslagname van een gegevensdrager zijn de gegevens in veel gevallen niet meer leesbaar, omdat de gegevens versleuteld zijn en deze zonder sleutel niet meer ontsleuteld kunnen worden.[187] De hierboven beschreven keyloggerfunctie van malware kan inlognamen en wachtwoorden onderscheppen. De wachtwoorden kunnen op hun beurt de mogelijkheid geven om achter de sleutel te komen waardoor de gegevens alsnog kunnen worden ontsleuteld.[188]

Ten slotte is de hackbevoegdheid ook nadrukkelijk geïntroduceerd om met het probleem van cloud computing in opsporingsonderzoeken om te gaan.[189] Bij gebruik van cloud computing is het vaak niet meer redelijkerwijs vast te stellen waar gegevens zich op enig moment bevinden. Deze bevinden zich vaak (verspreid) op servers in datacentrums in het buitenland. Met de inzet van de hackbevoegdheid kunnen opsporingsambtenaren – voor zover aan alle voorwaarden van de voorgestelde bevoegdheid wordt voldaan – webmail accounts of accounts die worden gebruikt voor online opslagdiensten hacken om op die wijze een 'online doorzoeking' van het account uit te voeren.[190]

183 Zie Jacobs 2012.
184 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT Wet Computercriminaliteit III), p. 20.
185 Zie uitgebreid Oerlemans 2012. Nog steeds zijn in dat geval de verkeersgegevens zichtbaar, waar ook strategisch interessante informatie uit kan worden afgeleid.
186 Zie ook Abate 2011, p. 124 en *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT Wet Computercriminaliteit III), p. 10.
187 Moderne versleutelprogramma's zoals TrueCrypt zijn naar verluidt moeilijk te kraken. Natuurlijk blijft het een kat-en-muisspel tussen de makers en de krakers van encryptie en wordt de techniek constant verbeterd om encryptie robuuster te maken. Het is daarom lastig te zeggen of de encryptieproblematiek in de toekomst meer of minder wordt. De laatste jaren heeft het een ernstig obstakel voor de politie opgeleverd, met name ook in kinderpornozaken (zie uitgebreid Oerlemans 2017, p. 44-52). Maar het is ook denkbaar dat in de toekomst met behulp van kwantumcomputers het kraken van versleutelde gegevens weer eenvoudiger wordt.
188 Zie ook Fox 2007, p. 828 en *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT Wet Computercriminaliteit III), p. 21.
189 Zie ook *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT Wet Computercriminaliteit III), p. 6-15.
190 Daarbij moet wel worden opgemerkt dat zich hierbij mogelijk problemen met betrekking tot de territoriale soevereiniteit van andere staten kunnen voordoen. In deze studie wordt daarop niet uitgebreid ingegaan. Zie bijvoorbeeld Koops 2012b, Koops & Goodwin 2014 en Oerlemans 2017, p. 293-356 voor meer informatie over het onderwerp.

6.1.2 Inhoud van de nieuwe bevoegdheid

De nieuwe 'hackbevoegdheid' in art. 126nba Sv kan het best worden omschreven als een paraplubevoegdheid, waarbij opsporingsambtenaren zich op afstand toegang verschaffen tot een geautomatiseerd werk[191]. Vervolgens mogen opsporingsambtenaren – indien is voldaan aan de voorwaarden in de wet – de volgende opsporingshandelingen inzetten:

1. het vaststellen van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker, zoals de identiteit of locatie, en de vastlegging daarvan;
2. het onderscheppen van communicatie, zoals bedoeld in art. 126l Sv of 126m Sv;
3. het stelselmatig observeren van gedrag van een persoon met een technisch hulpmiddel, zoals bedoeld in art. 126g Sv;
4. het vastleggen van gegevens op een computer; en
5. de ontoegankelijkheidsmaking van gegevens.[192]

In de vorige paragraaf is de werking van de opsporingsmethode om 'bepaalde kenmerken van het geautomatiseerde werk of de gebruiker' toegelicht. Deze opsporingsmethode kan met behulp van policeware worden ingezet. De toepassing van de bevoegdheid ter observatie van een persoon is mogelijk door een GPS-signaal op een gehackte computer aan te zetten en de informatie door te sturen naar de politie. Het onderscheppen van communicatie is mogelijk met policeware door een microfoon of keylogfunctie aan te zetten en screenshots te maken. Met het vastleggen van gegevens die door een geautomatiseerd werk zijn verwerkt, wordt waarschijnlijk gedoeld op de online doorzoeking die veelal ook zal worden inzet om informatie uit online accounts te vergaren. Met de 'ontoegankelijkheidsmaking' van gegevens wordt bedoeld dat gegevens op een computer op afstand versleuteld worden of dat de IT-infrastructuur op afstand onklaar wordt gemaakt.

De hackbevoegdheid is niet beperkt tot een bepaald type computers. Dat is verklaarbaar vanuit juridisch perspectief, omdat gekozen is voor een 'techniekonfhankelijke formulering'. Hierdoor is de bevoegdheid wel erg breed geworden. Zoals de regering zelf ook aangeeft is het zeer de vraag of het proportioneel is om een pacemaker of zelfrijdende auto te hacken.[193] Een dergelijke toepassing ligt dan ook niet voor de hand.

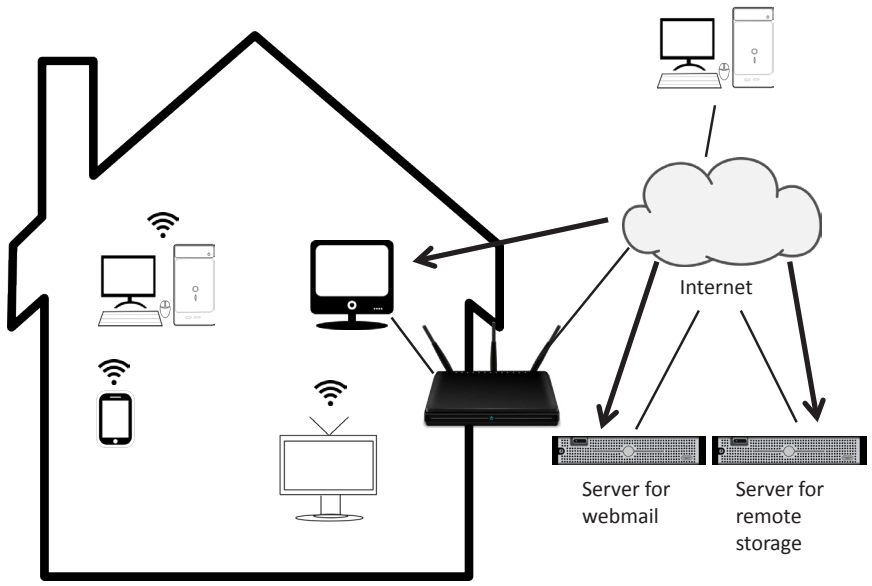
De officier van justitie, rechter-commissaris én de Centrale Toetsingscommissie zullen elk een afweging maken of inzet van de bevoegdheid proportioneel en subsidiair is. Daarbij zullen de omstandigheden van het geval in overweging moeten worden genomen. De bijzondere opsporingsbevoegdheid mag verder slechts worden ingezet in opsporingsonderzoeken naar misdrijven zoals omschreven in art. 67 Sv die de rechtsorde ernstige schaden en voor zover dat strikt noodzakelijk is. De inzet tot de bevoegdheid tot het ontoegankelijk maken van gegevens is nog verder beperkt tot misdrijven met een gevangenisstraf van

191 het begrip 'geautomatiseerd werk' is gedefinieerd in art. 80sexies Sr. Het betreft "een inrichting die bestemd is om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen". In de Wet computercriminaliteit III wordt voorgesteld het begrip te wijzigen in: "een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken". De definitie omvat computers, servers, modems, smartphones en tablets, maar bijvoorbeeld ook een (smart) televisie, navigatiesysteem of pacemaker. Zie Kamerstukken II 2015/16, 34 372, nr. 3 (MvT Wet computercriminaliteit III), p. 85-86.
192 Zie ook uitgebreid *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT Wet Computercriminaliteit III), p. 21-31.
193 Zie ook *Kamerstukken II* 2016/17, 34 372, nr. 6, p. 35-36.

maximaal acht jaar of meer en tot een lijst met misdrijven die binnen een algemene maatregel van bestuur wordt opgenomen. In deze lijst worden typische cyberdelicten opgenomen, zoals (het bezit, verspreiding en vervaardiging) van kinderporno, het gebruik en exploitatie van *botnets* (als gekwalificeerde variant van computervredebreuk) en grooming.[194]

6.2 De doorzoeking op afstand

De doorzoeking op afstand wordt geregeld in art. 126nba lid 4 Sv. De opsporingsmethode is gevisualiseerd in Figuur 6.1.



Figuur 6.1: Visualisatie van de doorzoeking op afstand.

Figuur 6.1 laat zien hoe op afstand toegang kan worden verschaft tot een computer om vervolgens gegevens te onderzoeken. In het bovenstaande model bevinden de computers zich in een woning. Nadat toegang is verschaft, kunnen bijvoorbeeld screenshots worden gemaakt en gegevens worden gekopieerd ten behoeve van de bewijsgaring.

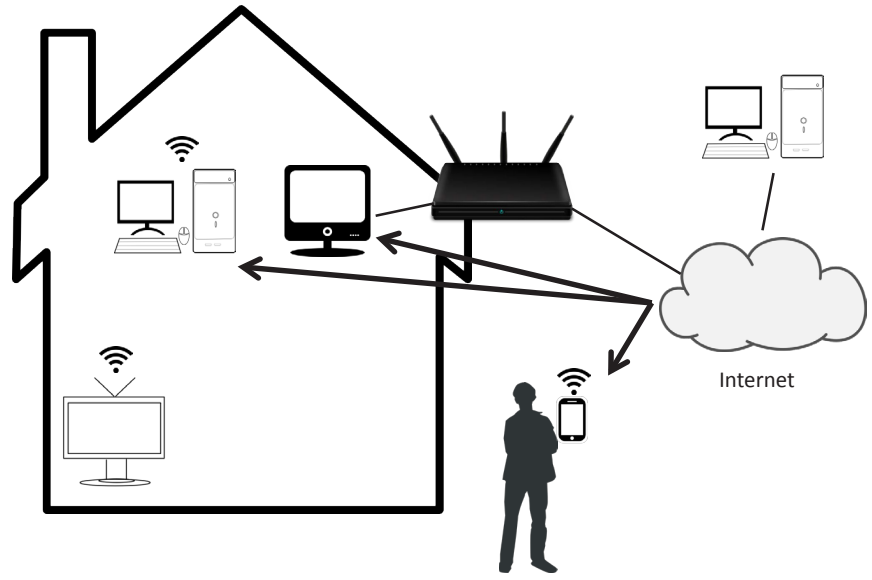
Het is ook mogelijk dat op afstand een online account wordt binnengedrongen, bijvoorbeeld van een webmaildienst of online opslagdienst.[195] De benodigde inloggegevens kunnen in die situatie van tevoren op

194 Zie *Kamerstukken II* 2016/17, 34 372, nr. 6, p. 40.
195 Zie *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT Wet Computercriminaliteit III), p. 11-12. Technisch gezien wordt dan natuurlijk een server binnengedrongen.

verschillende wijzen worden verkregen. Het is denkbaar dat ze worden verkregen van derden (zoals informanten) of tijdens een huiszoeking op een papiertje of in een bestand zijn gevonden. Na het binnendringen van het online account kan relevante informatie worden vastgelegd. In de memorie van toelichting en het nader verslag wordt aangegeven dat het hele proces wordt vastgelegd door middel van logging. Een technisch rechercheur doet de uitvoering, terwijl een tactisch rechercheur de operatie heeft bedacht en aangeeft waar de politie naar op zoek is.[196] In mijn dissertatie en in deze studie is niet onderzocht of deze wijze van bewijsgaring rechtmatig wordt geacht tijdens de zitting. Uiteindelijk moet de rechter overtuigd zijn van de betrouwbaarheid van het bewijs. Met andere woorden, opsporingsdiensten moeten er rekening mee houden dat het bewijsgaringsproces in de rechtszaal moet worden verantwoord.

6.3 Het gebruik van policeware

Het gebruik van policeware als opsporingsmethode onder de hackbevoegdheid wordt in Figuur 6.2 gevisualiseerd.



Figuur 6.2: Visualisatie van het gebruik van policeware.

In Figuur 6.2 is te zien hoe policeware op verschillende apparaten kan worden geïnstalleerd. Gezien de werking van commercieel verkrijgbare policeware van FinFisher en Hacking Team, wordt de software vaak op pc's of mobiele telefoons geïnstalleerd.[197] Vervolgens kan van veel verschillende functionaliteiten gebruik worden gemaakt. Daarbij moet volgens de memorie van toelichting worden gedacht aan:

196 Zie *Kamerstukken II* (2015/16, 34 372, nr. 6, p. 45-46 en 66.
197 Zie Morgan Marquis-Boire, 'From Bahrain With Love: FinFisher's Spy Kit Exposed?', *Citizen Lab*, 25 juli 2012 en Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire en John Scott-Railton, 'Mapping Hacking Team's "Untraceable" Spyware', *Citizen Lab*, 17 februari 2014.

1. het opnemen van geluid (via de microfoon);
2. het vastleggen en doorsturen van toetsaanslagen;
3. het maken van screenshots;
4. het aanzetten van de camera; en
5. het creëren van een achterdeurtje voor toegang op afstand.[198]

De FBI heeft in het verleden ook regelmatig van software gebruikgemaakt die gericht was op het vastleggen van het IP-adres en andere identificerende gegevens van computergebruikers.[199] Zoals in paragraaf 6.1.2 is uitgelegd, worden deze toepassingen ook onder strikte voorwaarden met de hackbevoegdheid mogelijk gemaakt. Daarbij moet tevens worden opgemerkt dat de mogelijkheid om daadwerkelijk toegang te krijgen afhankelijk is van de omstandigheden van het geval, zoals (1) het type apparaat waarvan de verdachte gebruikmaakt, (2) de ernst van het misdrijf en (3) de beveiligingsmaatregelen die een verdachte heeft genomen. Nog te vaak krijg ik de indruk dat opsporingsambtenaren denken dat de bevoegdheid een volwaardig alternatief zal zijn voor tappen of andere opsporingsbevoegdheden. Bovengenoemde lijst van mogelijke functionaliteiten laat bovendien zien dat het gebruik van policeware andere gegevens oplevert dan een telefoon- of internettap en een andere - meer vergaande - privacyinmenging oplevert. De betrokken opsporingsautoriteiten zullen telkens moeten nagaan welke opsporingshandelingen en -functionaliteiten van policeware precies noodzakelijk zijn om het omschreven doel in het schriftelijke bevel van de officier van justitie te bereiken.

6.4 Het ontoegankelijk maken van gegevens

Het ontoegankelijk maken van gegevens op afstand is verder beperkt tot misdrijven met een gevangenisstraf van acht jaar of meer en tot een beperkte lijst van cybercrimes. In de memorie van toelichting en het nader verslag wordt opgemerkt dat het hier in het bijzonder gaat om het op afstand ontoegankelijk maken van kinderporno en onklaar maken van botnets.[200]

In het verleden heeft de politie al eens een operatie uitgevoerd waarbij 220.000 kinderpornoafbeeldingen en –video's op het dark web werden vervangen door een Nederlands politielogo.[201] Ook heeft de Nederlandse politie al eens een botnetinfrastructuur in Nederland onklaar gemaakt.[202] In Europees verband is het EC3-centrum van Europol actief in het coördineren van internationale acties om botnets uit te schakelen.[203]

In de memorie van toelichting wordt opgemerkt dat deze bevoegdheid ook nadrukkelijk wordt ingezet om cybercrime te 'verstoren'.[204] Het ligt daarbij voor de hand dat dit doel wordt ingezet náást het doel van het verzamelen van bewijs voor de vervolging van een verdachte. Daar zijn de bijzondere bevoegdheden in het Wetboek van Strafvordering immers ook voor bedoeld.

6.5 Slotbeschouwing

In dit hoofdstuk is de nieuwe bijzondere opsporingsbevoegdheid van art. 126nba Sv nader onderzocht. Kort gezegd is art. 126nba Sv een paraplubevoegdheid voor hacken als opsporingsmethode, waarbij op afstand toegang kan worden verkregen tot een computer. Vervolgens kunnen andere opsporingshandelingen plaatsvinden, zoals (1) het vastleggen van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker, (2) het onderscheppen van communicatie, (3) het stelselmatig observeren van gedrag van een persoon, (4) het vastleggen van gegevens op een computer, en (5) het op afstand ontoegankelijk maken van gegevens. In de praktijk het afhankelijk zijn van de omstandigheden van het geval en de technologie die de betrokkene gebruikt, of hacken als opsporingsmethode succesvol kan worden toegepast.

In dit hoofdstuk is niet ingegaan op vraagstukken met betrekking tot jurisdictie in verband met een grensoverschrijdende toepassing van hacken als opsporingsmethode. Een dergelijke analyse valt buiten het bestek van de studie. Toch is het relevant om op te merken dat het in beginsel niet is toegestaan om zonder toestemming van de betrokken staat en zonder verdragsbasis een computer op buitenlands grondgebied te hacken. In de memorie van toelichting en nader verslag wordt op dit aspect uitgebreid ingegaan.[205] Daarin wordt aangegeven dat wanneer de locatie van de computer die op afstand wordt betreden niet meer redelijkerwijs kan worden vastgesteld, het mogelijk is op afstand toegang te verschaffen tot een computer die zich mogelijk in het buitenland bevindt. Een officier van justitie moet daarvan aantekening maken in zijn aanvraag tot een machtiging voor de inzet van de bevoegdheid aan de rechter-commissaris.[206] Concreet kan deze situatie zich voordoen indien de betrokkene in het opsporingsonderzoek gebruikmaakt van (1) cloudcomputingtechnologie of (2) van anonimiseringsdiensten, zoals VPN-diensten en Tor.[207] Zodra de lo-

198 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT Wet computercriminaliteit III), p. 23, 25-26, 28-30 en 34.

199 De software kon volgens officiële documenten de volgende informatie weergeven: het IP-adres van de computer, (b) MAC-adres, (c) lijst van open TCP- en UDP-poorten, (d) lijst van uitvoerende programma's, (e) informatie over de 'operating system', (f) gebruikte internetbrowser en -versie, (g) geregistreerde gebruiker van het systeem, (f) de ingelogde gebruiker, en (h) laatste geraadpleegde URL. Zie Kevin Poulsen, 'FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats', *Wired*, 18 juli 2007 en Kevin Poulson, 'Documents: FBI Spyware Has Been Snaring Extortionists, Hackers for Years', *Wired*, 16 april 2009. Beschikbaar op: http://archive.wired.com/politics/law/news/2007/07/fbi_spyware. Zie ook meer recent Kevin Poulson, 'The FBI Used the Web's Favorite Hacking Tool to Unmask Tor Users', *Wired*, 16 december 2014 over operatie 'Torpedo', waarbij het IP-adres van Tor-gebruikers zeer waarschijnlijk met behulp van soortgelijke software op grotere schaal is ontmaskerd. Beschikbaar op: https://www.wired.com/2014/12/fbi-metasploit-tor (laatst geraadpleegd op 29 december 2016).

200 Zie *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT Wet Computercriminaliteit III), p. 21-22 en *Kamerstukken II* 2016/17, 34 372, nr. 6, p. 40. Een botnet is een netwerk van geïnfecteerde computers, dat door een derde via een '*command-and-control*'-server wordt aangestuurd. Zie uitgebreid Hogben (red.) 2011, p. 16-25.

201 Zie Landelijk Parket, 'Kinderporno op anonieme, diep verborgen websites', 31 augustus 2011. Beschikbaar op: http://www.om.nl/onderwerpen/zeden-kinderporno/@156657/kinderporno-anonieme/. Zie ook Wil Thijssen, 'De digitale onderwereld', *Volkskrant* 10 maart 2012. Beschikbaar op: http://www.volkskrant.nl/archief/de-digitale-onderwereld~a3223214/

202 Zie Landelijk Parket, 'Nationale Recherche haalt berucht botnet neer', 25 oktober 2010. Beschikbaar op https://www.om.nl/vaste-onderdelen/zoeken/@28331/nationale-recherche-o/ (laatst geraadpleegd op 29 december 2016).

203 Zie bijvoorbeeld de volgende artikelen op de website van Europol: 'Notorious botnets infecting 2 million computers disrupted', 5 december 2013. Beschikbaar op: https://www.europol.europa.eu/content/notorious-botnet-infecting-2-million-computers-disrupted, 'Global action targeting Skylock malware', 10 juli 2014. Beschikbaar op: https://www.europol.europa.eu/content/global-action-targeting-shylock-malware en 'Botnet taken down through international law enforcement cooperation', 25 februari 2015. Beschikbaar op: https://www.europol.europa.eu/content/botnet-taken-down-through-international-law-enforcement-cooperation en ' 'Avalanche' network dismantled in international cyber operation', 1 december 2016 (laatst geraadpleegd op 29 december 2016).

204 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT Wet Computercriminaliteit III), p. 50.

205 Zie *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT Wet Computercriminaliteit III), p. 42-50 en *Kamerstukken II* 2016/17, 34 372, nr. 6, p. 17, 109-111. In het verslag wordt aangegeven dat nadere regelgeving in een OM-Aanwijzing kan plaatsvinden.

206 Zie *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT Wet Computercriminaliteit III), p. 42 en *Kamerstukken II* 2016/17, 34 372, nr. 6, p. 62.

207 Interessant is dat in de Verenigde Staten een voorstel loopt om onder gelijke voorwaarden het mogelijk te maken toegang te verschaffen tot computers die mogelijk in het buitenland staan. Zie uitgebreid Oerlemans 2017, p. 338-351.

catie van de computer wel duidelijk is en blijkt dat computer in het buitenland stond, moet de betrokken staat alsnog hierover in kennis worden gesteld.

De problematiek met betrekking tot jurisdictie in digitale opsporingsonderzoeken is niet beperkt tot hacken als opsporingsmethode. Dit is een vraagstuk dat nadere uitwerking in onderzoek behoeft en mogelijk in internationale verdragen. In de tussentijd zullen we afwachten wat de digitale opsporingspraktijk ons brengt en waar nadere normering noodzakelijk zal zijn.

Literatuurlijst

Abate 2011
Abate, C. (2011), 'Online-Durchsuchung, Quellen-Telekommunikationsüberwachung und die Tücke im Detail', *Datenschutz und Datensicherheit*, nr. 2, p. 122-125.

Beijer e.a. 2004
Beijer, A., Bokhorst, R.J., Boone, M., Brants, C.H., Lindeman, J.M.W. (2004), 'De Wet bijzondere opsporingsbevoegdheden – Eindevaluatie', WODC, nr. 222, Den Haag: Boom Lemma Uitgevers.

Blom 2007
Blom, T. (2007), 'Een ernstige inbreuk op de rechtsorde', *Delikt & Delinkwent*, vol. 58, p. 626-638.

Boehm & Cole 2014
Boehm, F. & Cole, M.D. (2014), 'Data Retention after the Judgement of the Court of Justice of the European Union', report for the Greens/EFA Group in the European Parliament, Münster/Luxembourg, 30 juni 2014.

Borgers 2009 (red.)
Borgers, M.J. e.a. (red.) (2009), *Politie in beeld. Liber amicorum Jan Naeyé*, Nijmegen: Wolf Legal Publishers.

Borgers 2015
Borgers, M.J. (2015), 'Normering van "lichte" opsporingsmethoden', *Delikt & Delinkwent* 2015/15.

Brinkhoff 2016
Brinkhoff, S. (2016), 'Big data datamining door de politie', *Nederlands Juristenblad*, vol. 20, p. 1400-1407.

Buruma 2001
Buruma, Y. (2001), *Buitengewone opsporingsbevoegdheden*, tweede druk, Deventer: W.E.J. Tjeenk Willink.

Casey e.a. 2011
Casey, E., Fellows, G., Geiger, M., & Stellatos, G. (2011), 'The growing impact of full disk encryption on digital forensics', *Digital Investigation*, vol. 8, nr. 2, 129-134.

Ciancaglini et al. 2013
Ciancaglini, V., Balduzzi, M., Goncharov, M., McArdle, R. (2013), 'Deepweb and Cybercrime. It's Not All About TOR', Trend Micro.

Clarke e.a. 2001
Clarke, I., Sandberg, O., Wiley, B. & Hong, T.W. (2001), 'Freenet: a distributed anonymous information storage and retrieval system', in: *Designing Privacy Enhancing Technologies*, pp. 46-66, Springer: Berlin Heidelberg.

Clarke e.a. 2010
Clarke, I., Sandberg, O., Toseland, M., & Verendel, V. (2010), 'Private Communication Through a Network of Trusted Connections: The Dark Freenet', paper submitted to PET.

Clayton 2004
Clayton, R. (2004), *Anonymity and traceability in cyberspace*, diss. Cambridge, 2004.

Conings & Oerlemans 2013
Conings, C. & Oerlemans, J.J. (2013), 'Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend?', *Computerrecht*, nr. 1, p. 23-32.

Corstens & Borgers 2014
Corstens, G.J.M. & Borgers, M.J. (2014), *Het Nederlands strafprocesrecht*, 8e druk, Deventer: Kluwer.

CTIVD 2014
Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD), 'Toezichtsrapport inzake onderzoek door de AIVD op sociale media', nr. 39, 16 juli 2014.

Dingledine, Mathewson & Syverson 2004
Dingledine, R., Mathewson, N. & Syverson, P. (2004), 'Tor: The second-generation onion router', Naval Research Lab: Washington DC.

Eijkman & Weggemans 2012
Eijkman, Q.A.M. & Weggemans, D. (2012), 'Open source intelligence and privacy dilemmas: Is it time to reassess state accountability?', *Security and Human Rights*, vol. 23, nr. 4, p. 285-296.

Fijnaut & Marx in: Fijnaut & Marx 1995
Fijnaut, C.J.C.F. & Marx, G.T. (1995), 'The normalization of undercover policing in the West: Historical and contemporary perspectives', p. 1-27, in: Fijnaut & Marx 1995.

Fijnaut & Marx 1995
Fijnaut, C.J.C.F. & Marx, G.T. (red.) (1995), *Undercover: Police surveillance in comparative perspective*, Den Haag: Kluwer.

Fokkens & Kirkels-Vrijman 2009 in: Borgers e.a. (red.) 2009
Fokkens, J.W. & Kirkels-Vrijman, N. (2009), 'De artikelen 2 Politiewet 1993 en 141 en 142 Strafvordering als basis voor opsporingsbevoegdheden', p. 105-124, in: Borgers 2009.

Fox 2007
Fox, D. (2007), 'Realisierung, Grenzen und Risiken der "Online-Durchsuchung"', *Datenschutz und Datensicherheit*, p. 827-834.

Groenhuijsen & Knigge 2004
Groenhuijsen, M.S. & Knigge, G. (red.) (2004), *Afronding en verantwoording. Onderzoeksrapport strafvordering 2001*, Deventer: Kluwer.

Groothuis & De Jong 2010
Groothuis, M.M. & Jong, T. de (2010), 'Is een nieuw grondrecht op integriteit en vertrouwelijkheid van ICT-systemen wenselijk?', *Privacy & Informatie*, nr. 6, p. 270-303.

Hogben (red.) 2011
Hogben, G. (red.), Plohmann, D., Gerhards-Padilla, E. & Leder, F. (2011), 'Botnets: Detection, Measurement, Disinfection & Defence', ENISA.

Jacobs 2012
Jacobs, B. (2012), 'Policeware', *Nederlands Juristenblad*, nr. 39, p. 2761-2764.

Joh 2009
Joh, E.E. (2009), 'Breaking the Law to Enforce It: Undercover Police Participation in Crime', *Stanford Law Review*, vol. 61, p. 155-198.

Kooijmans & Mevis 2013
Kooijmans, T. & Mevis, P.A.M. (2013), 'ICT in the context of criminal procedure: The Netherlands', TLS/EUR/AIDP.

Koops 2012
Koops, B.J. (2012), 'Politieonderzoek in open bronnen op Internet. Strafvorderlijke aspecten', *Tijdschrift voor Veiligheid*, vol. 11, nr. 2, p. 30-46.

Koops e.a. 2012a
Koops, B.J., Bodea, G. Broenink, G., Cuijpers, C.M.K.C., Kool, L. Prins, J.E.J. & Schellekens, M.H.M. (2012), 'Juridische scan openbrononderzoek. Een analyse op hoofdlijnen van de juridische aspecten van de iRN/iColumbo-infrastructuur en HDIeF-tools', TILT: Tilburg.

Koops e.a. 2012b
Koops, B.J., Leenes, R.E., Hert, P.J.A. de & Olislaegers, S. (2012), 'Misdaad en opsporing in de wolken: Knelpunten en kansen van cloud computing voor de Nederlandse opsporing', TILT/WODC: Tilburg/Den Haag.

Koops 2013
Koops, B.J. (2013), 'Police investigations in internet open sources: Procedural-law issues', *Computer Law and Security Review*, p. 645-665

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

Koops & Goodwin 2014
Koops, B.J. & Goodwin, M.E.A. (2014), 'Cyberspace, the cloud and cross-border criminal investigation. The limits and possibilities of international law', TILT/WODC.

Koops & Oerlemans 2015
Koops, B.J. & Oerlemans, J.J. (2015), 'Commentaar bij het Cybercrimeverdrag', in: Verrest & Paridaens 2015.

Koops, Conings & Verbruggen 2016
Koops, B.J., Conings, C. & Verbruggen, F. (2016), 'Zoeken in computers naar Nederlands en Belgisch recht. Welke plaats hebben 'digitale plaatsen' in de systematiek van opsporingsbevoegdheid', Preadvies voor de jaarvergadering van de Nederlands-Vlaamse Vereniging voor Strafrecht, Oisterwijk: Wolf Legal Publishers.

Kruisbergen & De Jong 2010
Kruisbergen, E.W. & Jong, D. de (2012), 'Undercoveroperaties: een noodzakelijk kwaad? Heden, verleden en toekomst van een omstreden opsporingsmiddel', *Justitiële verkenningen*, vol. 38, nr. 3, p. 50-67.

Lindenberg 2016
Lindenberg, K. (2016), 'De lokpuber verstopt zich in het materiële recht: Over het aanpassen van de zedendelicten door Computercriminaliteit III en hoe dit meer is dan het lijkt', *Ars Aequi*, nr. 10, p. 942-950.

Lodder e.a. 2014
Lodder, A.R., Meulen, N. van der, Wisman, T.H.A., Meij, L. & Zwinkels, C.M.M. (2014), 'Big Data, Big Consequences? Een verkenning naar privacy en big data gebruik binnen de opsporing, vervolging en rechtspraak', VU/WODC.

Lodder & Schuilenburg 2016
Lodder, A.R., & Schuilenburg, M.B. (2016), 'Politie-webcrawlers en Predictive policing', *Computerrecht*, nr. 3, p. 150-154.

Marx 1988, p. 11-13
Marx, G.T. (1988), *Undercover. Police Surveillance in America*, London: University of California Press.

Mevis, Verbaan & Salverda 2016
Mevis, P.A.M., Verbaan, J.H.J., Salverda, B.A. (2016), 'Onderzoek aan in beslag genomen elektronische gegevensdragers en geautomatiseerde werken ten behoeve van de opsporing en vervolging van strafbare feiten', Erasmus University/WODC.

Moore & Rid 2016
Moore, D. & Rid, T. (2016), 'Cryptopolitik and the Darknet', *Survival*, vol. 58, nr. 1, p. 7-38.

Nadelmann 1993
Nadelmann, E.A. (1993), *Cops across borders: the internationalization of U.S. criminal law enforcement*, Pennsylvania: The Pennsylvania State University Press.

Nadelmann 1995, in: Fijnaut & Marx 1995
Nadelmann, E.A. (1995), 'The DEA in Europe', in: Fijnaut & Marx 1995.

Nationaal Rapporteur Mensenhandel 2011
Nationaal Rapporteur Mensenhandel (2011), 'Kinderpornografie – Eerste rapportage van de nationaal rapporteur', Den Haag: BNRM.

Oerlemans 2011
Oerlemans, J.J. (2011), 'Hacken als opsporingsbevoegdheid', *Delikt & Delinkwent*, nr. 8, p. 888-908.

Oerlemans 2012
Oerlemans, J.J. (2012), 'Mogelijkheden en beperkingen van de Internettap', *Justitiële Verkenningen*, vol. 38, nr. 3, p. 20-39.

Oerlemans & Koops 2012
Oerlemans, J.J. & Koops, E.J. (2012), 'Surveilleren en opsporen in een Internetomgeving', *Justitiële Verkenningen*, nr. 5, p. 35-49.

Oerlemans 2017
Oerlemans, J.J. (2017), *Investigating Cybercrime*, diss. Leiden, Amsterdam: Amsterdam University Press.

Ölçer 2014
Ölçer, F.P. (2014), 'De lokmethode bij de opsporing van grooming', *Computerrecht*, nr. 1, p. 10-19.

Ölçer 2015
Ölçer, F.P. (2015), 'Modernisering van de bijzondere opsporing. Van BOB naar h(eimelijke) BOB', *Strafblad*, nr. 4, p. 298-307.

Oosterhoff 2016
Oosterhoff, M. (2016), 'Opsporing op social media', master scriptie Open Universiteit.

Petrashek 2009
Petrashek, N. (2009), 'Fourth Amendment and the Brave New World of Online Social Networking', *The Marquette Law Review*, nr. 93, p. 1495-1532.

Siemerink 2000a
Siemerink, L.A.R. (2000), *De wenselijkheid en mogelijkheid van infiltratie en pseudokoop op het internet*, ITeR, nr. 30, Deventer: Kluwer.

Siemerink 2000b
Siemerink, L.A.R. (2000), 'Bob logt in: infiltratie en pseudokoop op internet', *Computerrecht*, nr. 3, p. 141-147.

Simmelink 1987
Simmelink, J.B.H.M. (1987), *De rechtsstaatgedachte achter art. 1 Sv. Gedachten over de betekenis van art. 1 Sv voor het handelen van de overheid in de opsporingsfase*, Arnhem: Gouda Quint.

Smeets 2013
Smeets, S.F.J. (2013), 'De 'lokpuber': een mislukt experiment', *Strafblad*, p. 332-338.

T-CY 2016
Cybercrime Convention Committee (T-CY), 'Criminal justice access to electronic evidence in the cloud: Recommendations for consideration', final report of the T-CY Cloud Evidence Group, 16 september 2016, Straatsburg: Frankrijk.

Van der Bel, van Hoorn & Pieters 2013
Bel, D. van der, Hoorn, A.M. van, Pieters, J.J.T.M. (2013), *Informatie en opsporing: handboek informatieverwerving, -verwerking en -verstrekking ten behoeve van de opsporingspraktijk*, 3e druk, Zeist: Uitgeverij Kerckebosch.

Verrest & Paridaens 2015
Verrest, P.A.M. & Paridaens, P.J.M.W., *Tekst & Commentaar Internationaal Strafrecht*, 6e druk, Deventer: Kluwer.

Wiemans 2004
Wiemans, F.P.E. (2004), *Onderzoek van gegevens in geautomatiseerde werken*, diss. Tilburg, Nijmegen: Wolf Legal Publishers.

WRR 2016
WRR (2016), 'Big Data in een vrije en veilige samenleving', Amsterdam: Amsterdam University Press.

Over de auteur

Mr. dr. Jan-Jaap Oerlemans heeft IT recht en strafrecht gestudeerd aan de Universiteit Leiden en de Universiteit van Amsterdam. Op 10 januari 2017 heeft hij zijn proefschrift '*Investigating Cybercrime*' verdedigd aan de Universiteit Leiden. Van 2010 tot en met 2015 was hij werkzaam als onderzoeker en juridisch adviseur bij het IT beveiligingsbedrijf Fox-IT. Daarnaast is hij werkzaam geweest als onderzoeker bij het Wetenschappelijk Onderzoeks- en Documentatiecentrum (WODC) van het Ministerie van Veiligheid en Justitie en de Nederlandse Defensie Academie. Jan-Jaap houdt zich bezig met cybercrime, cybersecurity, privacy en digitale opsporing. Hij is verbonden als onderzoeker bij eLaw, het centrum voor Recht en Digitale Technologie van de Universiteit Leiden.