9 Cybercriminaliteit en opsporing

Jan-Jaap Oerlemans & Mojdeh Kobari*

9.1 Inleiding

In opsporingsonderzoeken naar cybercriminaliteit in enge zin zijn digitale sporen, zoals een IP-adres of nickname, vaak de enige sporen die beschikbaar zijn. Het opsporingsproces ziet er daardoor heel anders uit dan opsporingsonderzoeken naar traditionele criminaliteit met een fysieke plaats delict. Ooggetuigen, DNA-materiaal of video-opnames zijn meestal niet beschikbaar. In plaats daarvan zijn opsporingsinstanties veel afhankelijker van de beschikbaarheid van gegevens bij internetdienstverleners die kunnen worden gevorderd en digitaal forensisch onderzoek op de computers van het slachtoffer en de dader.

Dit hoofdstuk richt zich op het opsporingsonderzoek in cybercriminaliteitszaken. In de praktijk vindt er uiteraard bij de politie ook informatieverzameling plaats voor het opbouwen van een informatiepositie, in het vooronderzoek van strafzaken en bij concepten als 'fenomeenonderzoeken'.[1] Ook doen private partijen steeds actiever digitaal onderzoek naar cybercriminaliteit. De politie werkt bovendien vaak samen met bedrijven en is tot op zekere hoogte afhankelijk van hen in opsporingsonderzoeken naar cybercriminaliteit (zie o.a. Boes & Leukfeldt, 2017). Dit hoofdstuk beperkt zich echter tot het gebruik van opsporingsmethoden door de politie en de regels daarvoor in het Wetboek van Strafvordering.

Het opsporingsonderzoek is opgenomen in Boek 2 van het Wetboek van Strafvordering. De regeling van het opsporingsonderzoek is inmiddels ver-

* Prof. mr. dr. J.J. Oerlemans is werkzaam als universitair docent Strafrecht bij het Instituut voor Strafrecht & Criminologie van de Universiteit Leiden. Daarnaast is hij bijzonder hoogleraar Inlichtingen en Recht bij de Universiteit Utrecht. Mr. M. Kobari is werkzaam als promovenda bij het Instituut voor Strafrecht & Criminologie van de Universiteit Leiden.

1 De commissie-Van Traa verstond onder het fenomeenonderzoek het doorlichten op aspecten van georganiseerde criminaliteit van een geografisch gebied of bevolkingsgroep, misdaadveld of criminele markt, en/of een sector of verschijnsel in de samenleving (*Kamerstukken II* 1995/96, 24072, nr. 10-11 (rapport-Van Traa)).

ouderd en door de vele opeenvolgende wijzigingen onoverzichtelijk en ontoegankelijk geworden. In het kader van de modernisering van het Wetboek van Strafvordering is in het nieuwe Boek 2 de regeling van het opsporingsonderzoek in het wetsvoorstel volledig 'geherstructureerd, vereenvoudigd en geactualiseerd'. Deze wijzigingen en aanvullingen zijn voor een belangrijk deel gebaseerd op het rapport *Regulering van opsporingsbevoegdheden in een digitale omgeving* van de Commissie modernisering opsporingsonderzoek in het digitale tijdperk (Commissie-Koops, 2018). De commissie-Koops kreeg namelijk tot taak te adviseren over de vraag 'of de wettelijke regeling van het opsporingsonderzoek, zoals neergelegd in het conceptwetsvoorstel Boek 2, voldoet of bijstelling dan wel aanvulling behoeft'. De verwachting is dat het gemoderniseerde Wetboek van Strafvordering op 1 april 2029 in werking zal treden.[2] Daar waar nodig zal bij de bespreking van de bijzondere opsporingsbevoegdheden worden verwezen naar het project Modernisering Strafvordering.

Het hoofdstuk is opgebouwd aan de hand van de drie belangrijkste uitdagingen die zich voordoen in opsporingsonderzoeken naar cybercriminaliteit, te weten: anonimiteit, versleuteling en jurisdictie (Oerlemans, 2017a). Deze uitdagingen verklaren waarom bepaalde opsporingsmethoden vaak worden ingezet in opsporingsonderzoeken naar cybercriminaliteit. Daarbij wordt ook (kort) uitgelegd op welke wijze deze opsporingsmethoden zijn gereguleerd. Ethische en juridische dilemma's die daarbij naar boven komen, worden tevens geadresseerd. In paragraaf 9.2 volgt eerst een korte uitleg over het stelsel voor de normering van opsporingsmethoden. Paragraaf 9.3 gaat over het opsporingsproces bij een IP-adres als digitaal spoor en de toegepaste opsporingsbevoegdheden, zoals het vorderen van gegevens en de inbeslagname van computers. Paragraaf 9.4 bespreekt het gebruik van anonimiseringsdiensten door cybercriminelen, openbronnenonderzoek op internet en online undercoveroperaties. In paragraaf 9.5 gaat het over het versleutelingsprobleem in opsporingsonderzoeken naar cybercriminaliteit en de hackbevoegdheid. Paragraaf 9.6 gaat in op de jurisdictieproblematiek in cyberonderzoeken. In paragraaf 9.7 vindt een korte bespreking plaats van de steeds vaker toegepaste strategie van 'verstoring van cybercriminaliteit'. Het hoofdstuk sluit af met enkele discussievragen en kernbegrippen.

2 'Nieuw Wetboek van Strafvordering treedt 1 april 2029 in werking', *Rijksoverheid.nl*, 20 maart 2024.

9.2 Het opsporingsonderzoek en de normering van opsporingsmethoden

Voordat de digitale opsporingsmethoden die worden gebruikt in cyberzaken worden besproken, is enige basiskennis over de organisatie van opsporing en de normering van opsporingsmethoden noodzakelijk. In deze paragraaf worden de betrokken organisaties in het opsporingsproces van cyberzaken beschreven en daarna wordt het stelsel van de normering van opsporingsmethoden toegelicht.

9.2.1 De organisatie van opsporing naar cybercriminaliteit in Nederland

Onder het begrip 'opsporing' wordt verstaan: 'het onderzoek in verband met strafbare feiten onder gezag van de officier van justitie met als doel het nemen van strafvorderlijke beslissingen' (art. 132a Sv). Bij de opsporing zijn drie partijen betrokken, namelijk de politie, het Openbaar Ministerie (OM) en de rechterlijke macht. Daarbinnen zijn ook diverse organisaties actief, waarop in de volgende paragrafen wordt ingegaan. De opsporingsambtenaren zijn verantwoordelijk voor het opsporingsonderzoek, waarbij de officier van justitie de leider is van het opsporingsonderzoek.[3]

9.2.2 De politie

In Nederland onderzoekt het 'Team High Tech Crime' (THTC) de georganiseerde transnationale cyberzaken, waarbij innovatie, technisch complexe zaken en zaken van nationaal belang vooropstaan (Odinot et al., 2017). Het THTC werkt daarbij ook vaak samen met internationale opsporingsinstanties, zoals het 'Federal Bureau of Investigation' (FBI) en de 'Secret Service' in de Verenigde Staten en het 'Bundeskriminalamt' (BKA) in Duitsland. Veel tijd gaat ook zitten in het uitvoeren van rechtshulpverzoeken van politiediensten uit het buitenland. Vanuit het 'European Cybercrime Centre' (EC3) bij Europol in Den Haag worden internationale politieacties gecoördineerd. In

3 Op grond van artikel 141 Sv is de officier van justitie zelf ook opsporingsambtenaar, maar in het algemeen geeft de officier van justitie leiding aan het opsporingsonderzoek. Anderen met een algemene opsporingsbevoegdheid zijn politieambtenaren, militairen van de Koninklijke Marechaussee en opsporingsambtenaren van de bijzondere opsporingsdiensten. Daarnaast kennen we op grond van artikel 142 Sv de buitengewone opsporingsambtenaren, die een beperkte opsporingsbevoegdheid hebben.

onderstaande afbeelding 9.1 is bijvoorbeeld te zien welke landen betrokken waren bij het ontmantelen van het 'Emotet-botnet'.[4]

Figuur 9.1 Infographic 'Emotet takedown' van Europol.eu[5]

Nederland kent op nationaal niveau ook gespecialiseerde teams die zich met de bestrijding van specifieke vormen van cybercriminaliteit bezighouden, zoals het Team ter Bestrijding van Kinderpornografie en Kindersekstoerisme (TBKK). Op regionaal niveau zijn door de Nationale Politie zogeheten 'cyberteams' gecreëerd, speciaal voor de inzet op cyberzaken en zijn er specialistische teams die zich bezighouden met het veiligstellen van gegevens op gegevensdragers (digitaal bewijs). Ook het Nederlands Forensisch Instituut (NFI) onderzoekt bewijsstukken in strafzaken. Het instituut houdt zich onder andere bezig met DNA-onderzoek en het openmaken, uitlezen en ontsleutelen van digitale informatie uit telefoons van verdachten.

Ten slotte zijn er nog specialistische teams bij bijzondere opsporingsdiensten, zoals de Fiscale Inlichtingen- en Opsporingsdienst (FIOD), die zich meer bezighouden met cybergerelateerde zaken, zoals het witwassen met digitale betaalmiddelen.

9.2.3 Openbaar Ministerie

Het OM is net als de Nationale Politie ingedeeld in tien regio's. Elke regio heeft een 'cybercrimeofficier' die cybercriminaliteitszaken moet oppakken

4 Openbaar Ministerie, 'Internationale politieoperatie LadyBird: botnet Emotet wereldwijd ontmanteld', *OM.nl*, 27 januari 2021.

5 Europol, 'World's most dangerous malware EMOTET disrupted through global action', *Europol.eu*, 27 januari 2021.

(Odinot et al., 2017). Daarnaast bestaat er bij het Landelijk Parket van het OM een landelijk coördinerend officier van justitie op het gebied van cybercriminaliteit en een landelijk coördinerend officier van justitie voor digitale opsporing. Zij worden bijgestaan door enkele andere officieren van justitie en parketsecretarissen. Het OM kent ook een beleidsafdeling die zich richt op de bestrijding van cybercriminaliteit.

De officier van justitie geeft de bevelen af voor de inzet van bijzondere opsporingsbevoegdheden die worden uitgevoerd door het THTC of andere politieteams. Voordat een bevel wordt afgegeven, is vaak een machtiging van een rechter-commissaris van een rechtbank noodzakelijk. De officier van justitie moet dan uitleggen waarom aan de wettelijke vereisten voor de inzet van de bijzondere opsporingsbevoegdheid is voldaan en de inzet proportioneel en subsidiair is. Proportionaliteit wil in deze context zeggen dat de mate van inbreuk op fundamentele rechten door de inzet van bijzondere opsporingsbevoegdheid evenredig moet zijn ten opzichte van het beoogde legitieme doel van de inzet van de bevoegdheid. Subsidiariteit wil zeggen dat voor de minst vergaande wijze van optreden dient te worden gekozen (Corstens/Borgers & Kooijmans, 2021).

9.2.4 Rechterlijke macht

Alle rechtbanken, gerechtshoven en de Hoge Raad in Nederland zijn bevoegd cybercriminaliteit- of cybercriminaliteitszaken te behandelen. Ook kunnen rechters-commissarissen van alle rechtbanken bij de toepassing van bepaalde dwangmiddelen of bijzondere opsporingsbevoegdheden een machtiging afgeven aan de officier van justitie om het middel in te zetten voor de bewijsverzameling in opsporingsonderzoeken.

Binnen de rechterlijke macht bestaat er wel één Kenniscentrum Cybercrime bij het Hof Den Haag. Het kenniscentrum verzamelt en beheert kennis en informatie over cybercriminaliteit voor alle rechtbanken en gerechtshoven in Nederland. Het kenniscentrum verschaft juridische en praktische kennis over cybercriminaliteit en basisinformatie over ICT aan rechters, raadsheren en gerechtsambtenaren in Nederland. Verder heeft het kenniscentrum ook een helpdesk, waar medewerkers werkzaam binnen de rechtspraak met vragen terechtkunnen.[6] De meeste gerechtshoven in Nederland hebben daarnaast een cluster opgericht om rechtszaken over cybercriminaliteit te behandelen

6 Zie de webpagina 'Kenniscentrum Cybercrime', Gerechtshof Den Haag op Rechtspraak.nl.

(ook wel 'cyberkamers' genoemd) en daarmee meer ervaring op te doen met cybercriminaliteit.

9.2.5 *Het strafvorderlijk legaliteitsbeginsel en de IRT-affaire*

Aan de basis van de normering van (digitale) opsporingsmethoden ligt het strafvorderlijk legaliteitsbeginsel. Artikel 1 Sv luidt als volgt:

> 'Strafvordering heeft alleen plaats op de wijze bij de wet voorzien.'

Als gevolg van het strafvorderlijk legaliteitsbeginsel moet in de wet een grondslag voorhanden zijn voor bewijsgaringsactiviteiten van opsporingsambtenaren (Corstens/Borgers & Kooijmans, 2021; Keulen & Knigge, 2020; Knigge & Kwakman, 2001).

De IRT-affaire heeft sterk bijgedragen aan de normering van opsporingsbevoegdheden in Nederland (Blom, 1998).[7] In de jaren negentig werkten verschillende politiekorpsen in ons land samen in Interregionale Recherche Teams (IRT's). Deze teams richtten zich op georganiseerde misdaad en met name op drugshandel. Geïnspireerd door de Amerikaanse opsporingspraktijk maakte het team gebruik van innovatieve opsporingsmethoden, onder meer van de zogenoemde 'groei-informant' die moest doordringen tot de top van de criminele organisatie (zie ook Nadelmann, 1995). 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 zicht te blijven houden op de criminele organisatie.[8] 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, niet alleen om de juridische en ethische vragen die deze innovatieve opsporingsmethoden opriepen, maar ook omdat slechts weinig leidinggevenden bij de bevoegde instanties op de hoogte waren van de activiteiten. Naar aanleiding van deze controverse werd de Parlementaire Enquêtecommissie Opsporingsmethoden ingesteld onder leiding van Maarten van Traa. De commissie-Van Traa schreef een uitgebreid rapport over het gebruik van de undercoveropspo-

7 Zie *Kamerstukken II* 1995/96, 24072, nr. 10-11 (rapport-Van Traa), p. 72-164.

8 Zie uitgebreid *Kamerstukken II* 1995/96, 24072, nr. 10-11 (rapport-Van Traa), p. 72-164.

ringsmethoden en deed aanbevelingen om deze opsporingsmethoden in het Wetboek van Strafvordering te reguleren.

De aanbevelingen tot het reguleren van opsporingsmethoden leidden in 2000 tot de Wet bijzondere opsporingsbevoegdheden (Wet BOB) (Buruma, 2001).[9] In deze wet zijn 'undercoverbevoegdheden' gereguleerd, namelijk de pseudokoop, stelselmatige observatie, stelselmatige informatie-inwinning en infiltratie. Al in 1999 gaf de wetgever aan dat bevoegdheden, zoals stelselmatige observatie en infiltratie, onder gelijke voorwaarden in de digitale wereld kunnen worden toegepast.[10] De wet moet telkens worden aangepast als dat nodig is. Daarvan is bijvoorbeeld sprake als het wenselijk wordt geacht nieuwe opsporingsmethoden in te zetten die een ernstige inmenging vormen met het recht op privacy van betrokkenen. In de memorie van toelichting van de Wet BOB werd in 1997 al opgemerkt dat:

> '(...) ontwikkelingen in de diverse vormen van criminaliteit, die hun oorsprong overigens mede in allerlei technologische ontwikkelingen hebben, vereisen dat ook de opsporingsmethoden zich voortdurend ontwikkelen. (...) Zodra als gevolg daarvan in voldoende mate is komen vast te staan dat een opsporingsmethode een inbreuk op de privacy inhoudt, zal de wetgever uiteraard zijn verantwoordelijkheid moeten nemen en een regeling van die methode moeten geven.'[11]

Verschillende malen heeft de Nederlandse wetgever de wet ook aangepast in het licht van de digitalisering van criminaliteit én van de opsporing. Daarbij kan met name worden gewezen op de Wet computercriminaliteit I in 1993, de Wet computercriminaliteit II in 2006, de Wet computercriminaliteit III in 2019 en de Innovatiewet Strafvordering in 2022. Daarnaast brengt het wetsvoorstel over het opsporingsonderzoek in het kader van modernisering van het Wetboek van Strafvordering in de toekomst mogelijk veel wijzigingen. In dit hoofdstuk wordt dan ook veelvuldig naar deze wetten verwezen.

9.2.6 Stelsel van normering van bijzondere opsporingsbevoegdheden

Het strafvorderlijk legaliteitsbeginsel is, zoals gezegd, leidend voor het regelen van opsporingsbevoegdheden. In Nederland is daaraan het criterium gekoppeld dat opsporingsmethoden die een *meer dan geringe* inmenging op de rechten en vrijheden van de betrokken individuen met zich brengen en

9 *Stb.* 1999, 245; *Stb.* 2000, 32.
10 Zie *Kamerstukken II* 1998/99, 26671, nr. 3, p. 36.
11 *Kamerstukken II* 1996/97, 25403, nr. 3, p. 12.

zeer risicovol zijn voor de integriteit en beheersbaarheid van het opsporingsonderzoek, in een daarop toegesneden wettelijke bepaling moeten worden gereguleerd (Corstens/Borgers & Kooijmans, 2021).[12]

Deze opsporingsmethoden moeten worden gereguleerd als bijzondere opsporingsbevoegdheden. Door de specifieke regels weten betrokkenen in een opsporingsonderzoek wat de reikwijdte is van de bevoegdheden die worden ingezet. De regulering van deze meer indringende opsporingsmethoden vindt plaats in het Wetboek van Strafvordering (het formele strafrecht), zodat uiteindelijk de Staten-Generaal over de wenselijkheid van het aanpassen of creëren van opsporingsbevoegdheden beslist (Koops & Oerlemans, 2019b).

Opsporingsmethoden die slechts een geringe inbreuk op de rechten en vrijheden van de betrokken individuen maken en niet zeer risicovol zijn voor de integriteit en de beheersbaarheid van het opsporingsonderzoek, kunnen worden gebaseerd op de algemene taakstelling van de politie voor handhaving van de rechtsorde in artikel 3 van de Politiewet 2012 en artikelen 141 en 142 Sv.[13] In aanvulling op deze algemene taakstellende bepalingen wordt in het gemoderniseerde Wetboek van Strafvordering in artikel 2.1.9 Sv een nieuwe algemene bevoegdheid gecreëerd voor opsporingsambtenaren om ter uitvoering van hun opsporingstaak onderzoekshandelingen te verrichten.[14]

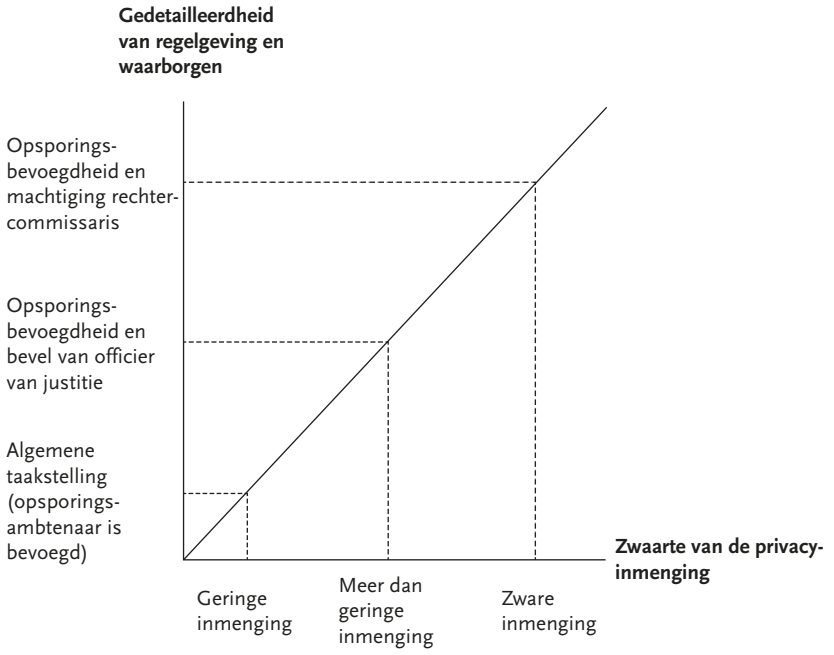
Titel IVA van het Wetboek van Strafvordering beschrijft in algemene termen en volgens een vast patroon wat de bijzondere bevoegdheden inhouden (Keulen & Knigge, 2020). Per bevoegdheid is de vereiste verdenking opgenomen. Daarnaast zijn bepaalde voorwaarden gekoppeld aan de inzet van bijzondere opsporingsbevoegdheden, zoals een schriftelijk bevel van een officier van justitie of een machtiging van een rechter-commissaris. Het idee van deze waarborgen is dat op die manier machtsmisbruik door de overheid wordt tegengegaan.

12 *Kamerstukken II* 1996/97, 25403, nr. 3, p. 110 en 115. 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 HR duidelijk dat het doorzoeken van vuilniszakken op straat niet een zodanig ernstige privacy-inmenging met zich brengt dat een bijzondere opsporingsbevoegdheid voor de opsporingsmethoden voorhanden moet zijn. Zie daarnaast ook HR 20 januari 2009, ECLI:NL:HR:2009:BF5603, HR 13 november 2012, ECLI:NL:HR:2012:BW9338, HR 1 juli 2014, ECLI:NL:HR:2014:1562 en HR 4 april 2017, ECLI:NL:HR:2017:584.

13 *Kamerstukken II* 1996/97, 25403, nr. 3, p. 110 en 115.

14 *Kamerstukken II* 2022/23, 36327, nr. 3, p. 365-366.

Op grond van jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM) en uit Nederlandse jurisprudentie is af te leiden dat de voorwaarden voor de inzet van de bevoegdheden in sterke mate afhangen van de inbreuk op het recht op privacy die daarbij wordt gemaakt (Oerlemans, 2017a; Commissie-Koops, 2018).[15] Het volgende systeem wordt daarbij zichtbaar in de normering van bijzondere opsporingsbevoegdheden.



Figuur 9.2 Schaal van de zwaarte van privacy-inmenging en bevoegde autoriteiten[16]

In figuur 9.2 is te zien dat bij een geringe inbreuk op het recht op privacy doorgaans een opsporingsambtenaar de bevoegdheid mag uitoefenen bij elk onderzoek naar een strafbaar feit. Bij een meer dan geringe inbreuk op het

15 Tot nog toe is de normering van opsporingsmethoden met name ingegeven door het recht op privacy. Naast de regulering van de bevoegdheden zelf kent het Wetboek van Strafvordering allerlei andere regels die bijvoorbeeld toezien op de verbalisering van de uitvoering van bevoegdheden, het beschikbaar stellen van het proces-verbaal over de inzet van bevoegdheden en andere relevante stukken voor de verdachten, en de notificatie van de inzet van bijzondere opsporingsbevoegdheden aan verdachten. Deze regels zijn gebaseerd op andere grondrechten en fundamentele rechten dan het recht op privacy, zoals het recht op een eerlijk proces.

16 Bron: Oerlemans 2017a, p. 78.

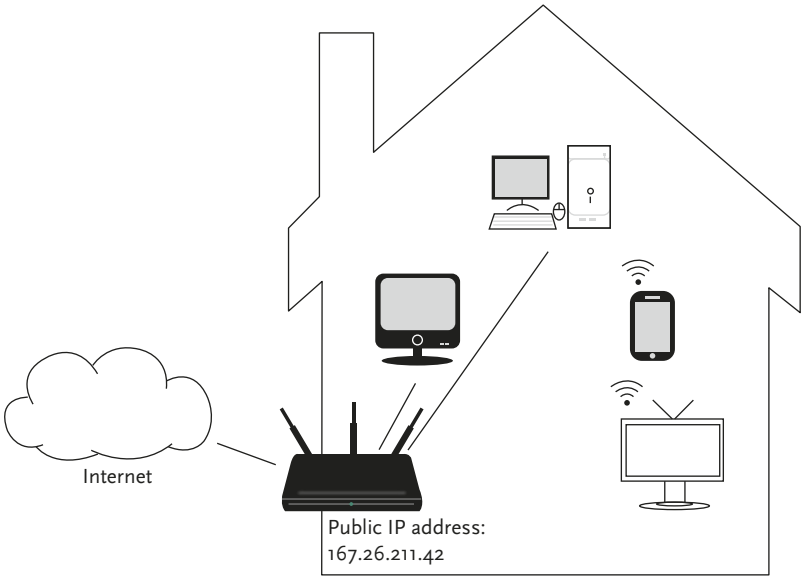
recht op privacy moet een officier van justitie een bevel afgeven voor de inzet van de bijzondere bevoegdheid. Deze bevoegdheden mogen alleen worden ingezet voor de meer ernstige misdrijven, zoals misdrijven die zijn genoemd in artikel 67 Sv. Voor de bevoegdheden die een ernstige inbreuk op de persoonlijke levenssfeer met zich brengen, moet een rechter-commissaris een machtiging afgeven. Deze toepassing is in de meeste gevallen mogelijk voor misdrijven die zijn genoemd in artikel 67 Sv, waarbij meestal is opgemerkt dat het een 'ernstige inbreuk op de rechtsorde' moet opleveren, om te benadrukken dat het om ernstige misdrijven moet gaan. Veel computerdelicten, waarvoor voorlopige hechtenis mogelijk is, zijn opgenomen in artikel 67 lid 1 sub b Sv.

9.3 Het IP-adres als digitaal spoor

Een IP-adres is een set van cijfers die een computer binnen een netwerk identificeert, zoals 84.80.247.141 (bij IPv4) of 2001:0db8:85a3:0000:0000:8a2e:0370:7334 (bij IPv6). Als een persoon thuis is en gebruikmaakt van wifi of een vaste internetverbinding, dan verloopt de internetverbinding via een modem dat door een *internet access provider* wordt geleverd.[17] Het modem krijgt een IP-adres door de internet access provider toegewezen.[18] Als een persoon via bijvoorbeeld zijn pc verbinding maakt met de webserver van een website, dan kan het IP-adres van het modem worden gelogd. Deze situatie is in figuur 8.2 gevisualiseerd.

17 De internet access provider levert de internetverbinding voor bijvoorbeeld breedbandinternet of een mobiele telefoon. Een internet service provider is een bredere term die ook betrekking kan hebben op de levering van andere internetdiensten, zoals diensten die de gebruiker via het internet kan gebruiken (zoals e-mail). De overkoepelende term internet service provider wordt in het spraakgebruik soms als synoniem voor internet access provider gebruikt.

18 Een router distribueert het internetverkeer naar de verbonden apparaten. Al die apparaten krijgen ook een IP-adres toegewezen.



Figuur 9.3 Eenvoudige weergave van een internetverbinding in een woning[19]

9.3.1 Het opsporingsproces bij een IP-adres als spoor

Een IP-adres kan een belangrijk digitaal spoor zijn in opsporingsonderzoeken naar cybercriminaliteit. Om dat duidelijk te maken bespreken we een kort scenario. Stelt u zich eens voor: na een internationale politieoperatie (gecoördineerd door Europol) ontvangt een Nederlands zedenteam van Europol een heleboel IP-adressen.[20] De IP-adressen zijn volgens Europol afkomstig van

19 Dit figuur is afkomstig uit Oerlemans (2017a, p. 29).

20 Zie bijvoorbeeld de uitspraak van Rb. Zwolle-Lelystad 1 juni 2010, ECLI:NL:RBZLY:2010:BM9626: 'Op 12 november 2007 ontving (naam), werkzaam als senior specialist expertise, in dienst van het Korps Landelijke Politiediensten, team bestrijding kinderpornografie, een rapport van Europol met betrekking tot een zaak van de Oostenrijkse politie over kinderpornografie op het internet. Uit het rapport bleek dat de Oostenrijkse politie een melding had ontvangen van de beheerder van een tweetal websites welke volgens de beheerder zouden worden misbruikt om kinderpornografisch beeldmateriaal te verspreiden. De beheerder van deze website heeft vervolgens 9737 afbeeldingen en download logfiles aan de Oostenrijkse politie overgedragen. Uit deze logfiles bleek dat tussen 29 augustus 2007 en 31 augustus 2007 110.031 keren een download van een bepaalde afbeelding had plaatsgevonden door 12.920 unieke IP-adressen. Vervolgens zijn de bijbehorende afbeeldingen, welke op een cd-rom waren bijgevoegd, door voornoemde (naam) bekeken. (naam) zag diverse afbeeldingen welke te classificeren waren als kinderpornografie zoals bedoeld in

een forum waarop seksueel materiaal met minderjarigen werd uitgewisseld. Een kopie van de server met bijbehorende berichten en materiaal is ook beschikbaar. Bij de gebruikersgegevens van de accounts op het forum behoren ook IP-adressen die zijn terug te leiden tot internet service providers in verschillende lidstaten van de Europese Unie. Europol stuurt dan de IP-adressen die te linken zijn aan Nederland door naar de Nederlandse politie. In dat geval moeten opsporingsambtenaren de IP-adressen linken aan verdachten in Nederland, zodat kan worden bewezen dat zij actief waren op het forum. Hoe gaat dat in zijn werk?

Stap 1:
Met een zoekopdracht in de zogenoemde 'Whois-database' kan een opsporingsambtenaar nagaan welke internet service provider het IP-adres heeft uitgegeven. Als het IP-adres toebehoort aan een Nederlandse internet service provider, dan is de kans aanwezig dat de verdachte een Nederlander is.

Stap 2:
In Nederland kunnen opsporingsambtenaren de gegevens van de abonneehouder (degene die doorgaans betaalt voor de internetverbinding) bij een internet access provider vorderen. Het betreft dan naam- en adresgegevens. Het betreft mogelijk het adres waar een verdachte woonachtig is.

Stap 3:
Door middel van een doorzoeking in een woning, waarvoor een bevel van een officier van justitie en een machtiging van een rechter-commissaris noodzakelijk zijn, kan binnen de woning van de verdachte bewijs over het misdrijf worden verzameld. Opsporingsambtenaren gaan dan op zoek naar gegevensdragers die mogelijk zijn gebruikt om seksueel beeldmateriaal van minderjarigen op te slaan en te verspreiden. Deze apparaten worden in beslag genomen.

Stap 4:
Opsporingsambtenaren gaan op zoek naar seksueel materiaal van minderjarigen (al dan niet geautomatiseerd) en ander bewijs van het misdrijf (zoals verstuurde berichten, loggegevens en nicknames) op de inbeslaggenomen gegevensdragers en aangelegen netwerken.

---

artikel 240b Sr. Uit de logfiles bleek dat in 134 gevallen een IP-adres was gebruikt dat toegewezen is aan een Nederlandse provider.'

Stap 5:
Het is gebruikelijk om getuigenverklaringen af te nemen van de bewoners van het pand en mogelijk wordt een verdachte gearresteerd. De verdachte wordt vervolgens verhoord.

In bovenstaand scenario is de kans groot dat de verdachte wordt geïdentificeerd en bewijs kan worden geleverd dat het de verdachte was die vanachter zijn computer seksueel materiaal van minderjarigen via het forum heeft uitgewisseld of in bezit had.

Het is belangrijk zich te realiseren dat bovenstaand scenario vanuit opsporingsperspectief het ideale scenario is. In de praktijk maken cybercriminelen vaak gebruik van anonimiseringstechnieken om hun IP-adres te verbergen. Ook brengen technologische ontwikkelingen, zoals de uitrol van IPv6-adressen en het gebruik van internet op andere plaatsen dan een woning, uitdagingen voor de identificatie van internetgebruikers aan de hand van een IP-adres met zich (Van der Vorst et al., 2019). In paragraaf 9.4 wordt uitgebreid op anonimiseringstechnieken ingegaan.

Bij de bespreking van het opsporingsproces bij een digitaal spoor van een IP-adres zijn verschillende opsporingsmethoden langsgekomen die op een of andere wijze zijn geregeld in het Wetboek van Strafvordering. Hieronder worden kort enkele opsporingsmethoden en de regulering daarvan besproken.

9.3.2 Het vorderen van gegevens

Nederland kent door de Wet vorderen gegevens telecommunicatie[21] en Wet bevoegdheden vorderen gegevens[22] uitgebreide bevoegdheden voor het vorderen van gegevens. In opsporingsonderzoeken naar cybercriminaliteit gaat het met name om het verzamelen van gegevens van internet service providers (in strafvordering 'aanbieders van een communicatiedienst'[23] genoemd), zoals internet access providers, hosting providers, webmail providers en socialemediadiensten.

Het vorderen van de gebruikersgegevens bij een IP-adres van een internet access provider is mogelijk in een opsporingsonderzoek naar elk misdrijf.

21 *Stb.* 2004, 105.
22 *Stb.* 2005, 390.
23 Zie artikel 138g Sv.

Een opsporingsambtenaar mag deze gegevens vorderen.[24] Als dat noodzakelijk wordt geacht voor het opsporingsonderzoek, kunnen bijvoorbeeld ook loggegevens van een internetdienstverlener worden gevorderd. Voor deze vordering moet een officier van justitie een bevel afgeven en de vordering mag alleen worden verstuurd in opsporingsonderzoeken naar de meer ernstige misdrijven, zoals genoemd in artikel 67 Sv.[25] Computermisdrijven waarop geen maximale gevangenisstraf van vier jaar of meer staat, zoals computervredebreuk en ddos-aanvallen, zijn ook opgenomen in artikel 67 Sv. Een officier van justitie kan ook een bevel afgeven om de gegevens op computers 'te bevriezen', zodat deze later alsnog met een vordering kunnen worden verkregen.[26] Opgeslagen e-mailberichten kunnen alleen worden gevorderd met een machtiging van een rechter-commissaris in opsporingsonderzoeken naar ernstige strafbare feiten.[27]

Verschillende typen gegevens worden met verschillende bevoegdheden gevorderd.[28] In het gemoderniseerde Wetboek van Strafvordering worden de bevoegdheden tot het vorderen van gegevens geherstructureerd en daarmee eenvoudiger gemaakt. Deze worden allemaal ondergebracht in een nieuwe afdeling van het wetboek. Afhankelijk van de zwaarte van de privacy-inmenging zitten daar verschillende voorwaarden aan vast. In opsporingsonderzoeken naar cybercriminaliteit zullen doorgaans ook gegevens worden gevorderd van andere bedrijven dan internetdienstverleners. Daarbij kan worden gedacht aan openbaarvervoersbedrijven, camerabeelden van banken (van pinautomaten) en particulieren en de administratie van bijvoorbeeld autoverhuurders of verhuurders van panden of opslagboxen.

In 2021 bepaalde het Hof van Justitie van de Europese Unie (HvJ EU) dat verkeersgegevens van communicatie, waaronder locatiegegevens, zeer privacygevoelig zijn. In het Prokuratuur-arrest oordeelde het daarom dat alleen een onafhankelijke instantie of een rechter mag oordelen dat deze gegevens in het kader van opsporingsonderzoeken voor zware criminaliteit gevorderd mogen worden.[29] Het OM wordt door het HvJ EU niet als voldoende onafhankelijk gezien. Daarop volgde ook een arrest in Nederland, waarin de Hoge Raad

24 Zie artikel 126na Sv.
25 Zie artikel 126nd Sv.
26 Zie artikel 126ni Sv.
27 Zie artikel 126ng lid 2 Sv.
28 Het vorderen van gegevens bij elektronische communicatieaanbieders is geregeld in artikel 126na-126ni Sv.
29 HvJ EU 2 maart 2021, C-746/18, ECLI:EU:C:2021:152 (*Prokuratuur*).

bepaalde dat bij het vorderen van verkeersgegevens (waaronder locatiegegevens), naast een bevel van een officier van justitie, ook een machtiging van een rechter-commissaris noodzakelijk is (Sholeh, 2022).[30] Het arrest laat zien hoe de jurisprudentie van het HvJ EU (en het EHRM) doorwerking heeft in ons nationale rechtsstelsel en tot wijzigingen voor de normering van bevoegdheden kan leiden (Van Horssen, 2024).[31] Het roept tegelijkertijd ook vragen op – die vooralsnog onbeantwoord blijven – zoals: wat moet worden verstaan onder 'zware criminaliteit'? En: geldt deze extra waarborg van een machtiging van de rechter-commissaris ook voor andere locatiegegevens, zoals reisbewegingen die worden vastgelegd door OV-chipkaarten, of via camera's en andere sensoren boven snelwegen?

9.3.3 Digitaal bewijs en onderzoek op gegevensdragers

In veel opsporingsonderzoeken naar cybercriminaliteit zal onderzoek op gegevensdragers noodzakelijk zijn, omdat daar mogelijk (digitaal) bewijs is te vinden van het gepleegde feit. Bij gegevensdragers, zoals laptops, pc's, smartphones en USB-sticks, kan digitaal forensisch onderzoek worden uitgevoerd. In de klassieke vorm wordt daarbij een kopie gemaakt van bijvoorbeeld een harde schijf, waarna de kopie (een *image*) op bewijs wordt onderzocht. In moderne onderzoeken wordt bij voorkeur (ook) *live forensics* uitgevoerd, waarbij bijvoorbeeld ook het werkgeheugen van computers wordt veiliggesteld en in computernetwerken onderzoek wordt gedaan. Daarmee kan onder andere worden nagegaan welke gebruikers recentelijk waren ingelogd (Casey, 2011). Met de toepassing van de bevoegdheid tot een netwerkzoeking is het daarbij ook mogelijk in accounts waar een verdachte gebruik van maakt in te loggen en de gegevens ten behoeve van het opsporingsonderzoek te bekijken en/of vast te leggen.

Software maakt het mogelijk de verschillende typen bestanden te ordenen en elk bestand te analyseren. Ook verwijderde bestanden kunnen vaak worden hersteld. De ontwikkelingen bij digitaal forensisch onderzoek en digitaal

30 HR 5 april 2022, ECLI:NL:HR:2022:475, *Computerrecht* 2022/186, m.nt. J.J. Oerlemans en A. Berlee.

31 Regels van het internationaal recht maken deel uit van de Nederlandse rechtsorde. Zodra regels van het internationaal recht het Koninkrijk der Nederlanden op internationaal niveau binden, heeft het Koninkrijk de verplichting deze regels na te komen, ook in de nationale rechtsorde. Voor eenieder verbindende bepalingen van verdragen en van besluiten van internationale organisaties geldt op grond van artikel 93 van de Grondwet dat zij verbindende kracht hebben zodra zij zijn bekendgemaakt in het Tractatenblad.

bewijs gaan snel. Steeds moeten bijvoorbeeld nieuwe typen apparaten met nieuwe besturingssystemen worden onderzocht. Ook worden de hoeveelheid en het type gegevens dat moet worden onderzocht, elk jaar groter (Henseler, 2017). Software kan helpen deze zoekslagen effectiever en efficiënter uit te voeren.

Het 'Hansken'-platform

Het NFI heeft een innovatief systeem ontwikkeld voor het doorzoeken van gegevens. Met het Hansken-platform kunnen zeer grote hoeveelheden gegevens snel, grondig en gecontroleerd geanalyseerd worden. Datasets zijn snel te doorzoeken om zo verbanden te leggen tussen verschillende attributen, zoals gebruikersnamen, bijnamen, telefoonnummers en e-mailadressen. Hierdoor kunnen rechercheurs en analisten sneller en effectiever werken in een opsporingsonderzoek (Van Beek et al., 2015). De software wordt bijvoorbeeld ingezet in diverse onderzoeken naar zware drugscriminaliteit en liquidaties in Nederland en heeft in bepaalde zaken belangrijk bewijs opgeleverd. Een voorbeeld is de zaak tegen Naoufal 'Noffel' F., die werd verdacht van het aansturen van een liquidatie (Schermer & Oerlemans, 2020).[32]

Veel Nederlandse verdachten communiceerden in deze zaken met elkaar via speciaal geprepareerde 'PGP-telefoons'. Dat zijn 'cryptotelefoons' waarmee verdachten beveiligd en versleuteld (met het Pretty Good Privacy (PGP) protocol) met elkaar kunnen communiceren. Na een aantal politieoperaties zijn inmiddels meer dan een miljard berichten die met verschillende cryptotelefoons zijn verzonden veiliggesteld.[33] Al deze gegevens kunnen met behulp van tientallen forensische tools op het Hansken-platform worden onderzocht. Het is mogelijk met behulp van sleutelwoorden door de berichten te zoeken en er kan gebruik worden gemaakt van AI-technieken, zoals objectherkenning en automatische vertaling.[34] De inhoud van deze berichten kan wijzen op

32 Rb. Amsterdam 19 april 2018, ECLI:NL:RBAMS:2018:2504.

33 H. van Gelder, 'Politie beschikt over 1 miljard "criminele" chats en de teller loopt door: "Goud in handen"', *AD.nl*, 13 april 2023. Zie ook J.J. Oerlemans, 'Overzicht cryptophone-operaties', *jjoerlemans.com*, 19 november 2023.

34 C. van der Meer & M. Willebrands, 'Duizenden foto's sneller doorzoeken dankzij slim algoritme', *Magazines Forensisch Instituut* 27 januari 2021.

strafbare feiten en wordt dikwijls als bewijs gebruikt in strafzaken. De politie en het OM moeten dan ook bewijzen dat de verdachte gebruik heeft gemaakt van de mobiele telefoon. Dat is mogelijk door bijvoorbeeld nicknames en andere metadata van berichten te koppelen aan de verdachte. Daarnaast worden ook vaak andere bronnen van bewijs meegewogen in de strafzaken.

Sommige auteurs stellen dat opsporingsonderzoeken door data-analyse op die veiliggestelde cryptoberichten fundamenteel is veranderd. Vanuit de data worden nieuwe opsporingsonderzoeken gestart, hetgeen 'datagedreven opsporing' wordt genoemd (Hirsch Ballin & Oerlemans, 2023). De regels die daarbij van toepassing zijn – en steeds belangrijker worden – staan niet alleen in het Wetboek van Strafvordering, maar ook in de Wet politiegegevens. Onder andere om deze reden pleiten juridische auteurs voor meer aandacht voor de naleving en controle van deze regels in strafzaken (Fedorova et al., 2022; Hirsch Ballin & Oerlemans, 2023; Te Molder et al., 2023; Schermer & Galiç, 2022; Stevens, 2021).

Bovenstaand voorbeeld illustreert ook dat digitaal bewijs op gegevensdragers niet alleen in opsporingsonderzoeken naar cybercriminaliteit een rol speelt. Steeds vaker speelt digitaal bewijs bijvoorbeeld ook een rol in meer traditionele strafzaken.

Daarnaast kan het bij digitaal bewijs soms zo zijn dat het belangrijker is om te weten met wie is gecommuniceerd, waar iemand is geweest, wat die persoon heeft gedaan en wanneer, dan om te weten *wat* er is gecommuniceerd (Henseler & De Poot, 2020). Daarvoor wordt een ander type digitaal bewijs gebruikt dan de inhoud van gegevens die staan opgeslagen op computers. Denk daarbij bijvoorbeeld aan locatiegegevens uit de metadata van foto's, GPS-signalen en wifi- en bluetoothverbindingen. Steeds meer jurisprudentie laat ook zien dat dergelijke locatiegegevens en metadata, met name op smartphones, een rol spelen in moordzaken.[35] Kortom, digitaal bewijs kan niet

35 Zie bijvoorbeeld Rb. Zeeland-West-Brabant 28 juni 2016, ECLI:NL:RBZWB:2016:3865 (doodslag in het verkeer) en Rb. Midden-Nederland 17 december 2013, ECLI:NL:RBMNE:2013:7258 (moord), waarbij bluetooth-gegevens van sensoren langs de weg een belangrijke bewijsrol speelden in de strafzaken. Zie ook Rb. Zeeland-West-Brabant 14 februari 2019, ECLI:NL:RBZWB:2019:575 over het gebruik van gegevens over wifi-verbindingen, en Rb. Noord-Nederland 11 juli 2019, ECLI:NL:RBNNE:2019:2986

alleen goed helpen bij het beantwoorden van de wie-vraag, door te achterhalen welke gebruiker schuilging achter een e-mailadres, user account of een telefoonnummer, maar kan ook de activiteiten van een gebruiker (wat), de plaats (waar) en tijd (wanneer) in kaart brengen (Henseler & De Poot, 2020).

9.3.4 Regels voor de inbeslagname en onderzoek op gegevensdragers

De hoofdregel is dat computers net als andere 'voorwerpen' vatbaar zijn voor inbeslagname tijdens een doorzoeking die wordt uitgevoerd in een opsporingsonderzoek.[36] Ten behoeve van de waarheidsvinding mogen opsporingsambtenaren onderzoek doen aan het inbeslaggenomen 'voorwerp'.[37] De bevoegdheid tot het doen van onderzoek ligt dus in de inbeslagnemingsbevoegdheid besloten (het is dus niet nodig daar extra bevoegdheden voor in te zetten).

De regels voor een doorzoeking en inbeslagname van gegevens op de plaats van de doorzoeking verschillen naar gelang de plaats waar een doorzoeking wordt gedaan (Gritter, 2016; Royer & Oerlemans, 2017). In principe mag – voor zover dat noodzakelijk, proportioneel en subsidiair is – een opsporingsambtenaar bijvoorbeeld een auto doorzoeken en voorwerpen in beslag nemen ten behoeve van de waarheidsvinding. Voor een doorzoeking in een kantoor of bij een hosting provider is een bevel van een officier van justitie vereist. Voor een doorzoeking in een woning is tevens een machtiging van een rechter-commissaris vereist.[38]

Het Smartphone-arrest

In het richtinggevende Smartphone-arrest uit 2017 heeft de Hoge Raad de nodige duidelijkheid verschaft over het onderzoek aan inbeslaggenomen gegevensdragers.[39] In dit arrest heeft de Hoge Raad bepaald dat onderzoek aan een inbeslaggenomen gegevensdrager door de officier van justitie of zelfs de rechter-commissaris is aangewezen als het 'onderzoek zo verstrekkend is dat een min of meer compleet beeld is verkregen van bepaalde aspecten van het persoonlijk leven van de gebruiker van de gegevensdrager of het

over een moordzaak waarbij de verdachte werd gelokaliseerd op basis van locatiegegevens uit het besturingssysteem voor smartphones van Google. Zie ook J.J. Oerlemans, 'Digitaal bewijs in moordzaken', *jjoerlemans.com*, 16 april 2018 en 20 april 2019.

36 Zie HR 29 maart 1994, ECLI:NL:HR:1994:AD2076; HR 20 februari 2007, ECLI:NL:HR:2007:AZ3564.

37 Zie artikel 94 Sv.

38 Zie artikel 125i Sv.

39 HR 4 april 2017, ECLI:NL:HR:2017:584.

geautomatiseerde werk'.[40] Bij onderzoek op smartphones is de kans groot dat een min of meer volledig beeld van bepaalde aspecten van het privéleven wordt verkregen, gezien de informatie die op smartphones is te vinden, zoals foto's, video's, privéberichten, agenda-items, contactlijsten en internethistorie.

Het idee is dat hoe indringender de analyse van de gegevens op de inbeslaggenomen gegevensdrager is, hoe meer waarborgen daar tegenover moeten staan. Met het Smartphone-arrest kan de volgende driedeling met waarborgen worden gemaakt bij de inbeslagname en analyse van gegevens op een gegevensdrager:

1.	Bij een zoeking op een inbeslaggenomen gegevensdrager waarbij een beperkte inbreuk op de privacy plaatsvindt, is een opsporingsambtenaar de bevoegde autoriteit.
2.	Bij een 'meer dan beperkte inbreuk' is onderzoek door een officier van justitie of zelfs door de rechter-commissaris vereist.
3.	Bij een 'zeer ingrijpende inbreuk' is de betrokkenheid van een rechter-commissaris vereist.

Er is sprake van slechts een *beperkte inbreuk* op de privacy, indien het onderzoek bestaat uit het slechts raadplegen van een gering aantal op de gegevensdrager opgeslagen of beschikbare gegevens. Een dergelijk onderzoek mag door een opsporingsambtenaar worden verricht. De jurisprudentie laat zien dat hiervan sprake kan zijn bij het bekijken van enkele foto's op een smartphone,[41] het lezen en kopiëren van enkele WhatsApp-berichten,[42] en het onderzoeken van herinneringen én het uitlezen van berichten op een geprepareerde 'PGP-telefoon'.[43]

Er is sprake van een *meer dan beperkte inbreuk* als met het onderzoek een min of meer compleet beeld is verkregen van bepaalde aspecten van het persoonlijke leven van de gebruiker. Hiervan zal volgens de Hoge Raad in het bijzonder sprake van kunnen zijn indien het onderzoek betreft van alle in de gegevensdrager opgeslagen of beschikbare gegevens met gebruikmaking van een technisch hulpmiddel, zoals software voor digitaal forensisch onderzoek.[44] Bij dergelijk onderzoek is betrokkenheid van de officier van justitie of rechter-commissaris vereist.

40 HR 4 april 2017, ECLI:NL:HR:2017:584, 588 en 592, r.o. 3.4.
41 HR 10 juli 2018, ECLI:NL:HR:2018:1121.
42 Zie bijvoorbeeld Hof Arnhem-Leeuwarden 14 juli 2017, ECLI:NL:GHARL:2017:6069.
43 Zie bijvoorbeeld Hof Amsterdam 14 december 2018, ECLI:NL:GHAMS:2018:4610.
44 Zie ook Hof Amsterdam 23 april 2018, ECLI:NL:GHAMS:2018:1435 en Hof Amsterdam 25 juni 2019, ECLI:NL:GHAMS:2019:2179.

Indien op voorhand is te voorzien dat met het onderzoek aan de gegevensdrager de inbreuk op privacy *zeer ingrijpend* zal zijn, is de rechter-commissaris de aangewezen autoriteit. Daarvan is bijvoorbeeld sprake als een verdachte met een advocaat heeft gecommuniceerd ('geheimhouderscommunicatie').

Niet iedereen is het eens met deze uitkomst van het Smartphone-arrest. Royer en Oerlemans (2017) hebben bijvoorbeeld bepleit dat de inbeslagname en het onderzoeken van gegevens op een smartphone *altijd* een meer dan beperkte privacyinbreuk met zich brengt. Volgens hen is minstens een bevel van een officier van justitie, maar bij voorkeur een machtiging van een rechter-commissaris wenselijk bij het uitlezen van de gegevens op een inbeslaggenomen smartphone. Ook brengt de driedeling onduidelijkheid voor de praktijk met zich mee. In de Verenigde Staten heeft het Hooggerechtshof in 2014 in de zaak *Riley t. California* bijvoorbeeld heel anders geoordeeld. Daar is nu een rechterlijk bevel (een *warrant*) vereist voor het kennisnemen van de gegevens op een inbeslaggenomen smartphone (Skovánek et al., 2019).[45]

In het gemoderniseerde Wetboek van Strafvordering heeft de wetgever ervoor gekozen om de bevoegdheid tot het verrichten van onderzoek aan gegevens wettelijk vast te leggen in artikel 2.7.38 Sv en daarmee dus los te koppelen van de inbeslagnamebevoegdheid.[46] De voorgestelde regeling is voor een belangrijk deel gebaseerd op de aanbevelingen van de commissie-Koops. Ook in het wetsvoorstel wordt uitgegaan van een driedeling, maar die driedeling wordt daarbij – op advies van de commissie-Koops – opgehangen aan het kerncriterium van 'stelselmatigheid'. Bij niet-stelselmatig onderzoek wordt er slechts een beperkte inbreuk op de privacy gemaakt en mag het onderzoek door een opsporingsambtenaar worden verricht op grond van de algemene bevoegdheidsbepaling. Hierbij kan worden gedacht aan het handmatig en gericht bekijken van de belgeschiedenis van een gegevensdrager, teneinde te achterhalen met wie er in de afgelopen periode is gebeld.

Als op voorhand redelijkerwijs voorzienbaar is dat een min of meer volledig beeld van bepaalde aspecten van iemands privéleven kan ontstaan, is er sprake van *stelselmatig* onderzoek dat een meer dan geringe inbreuk op de privacy oplevert. Voor het verrichten van dergelijk onderzoek is een bevel van

45 U.S. Supreme Court 25 juni 2014, 573, p. 28 (*Riley t. California*). Zie ook het citaat: '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".'

46 *Kamerstukken II* 2022/23, 36327, nr. 3, p. 568-577.

de officier van justitie vereist. Van dit onderzoek kan onder andere sprake zijn als de inhoud van een gegevensdrager volledig wordt gekopieerd.

Als op voorhand redelijkerwijs voorzienbaar is dat een ingrijpend beeld van iemands privéleven kan ontstaan, dient het onderzoek te worden aangemerkt als *ingrijpend stelselmatig*. Bij dergelijk onderzoek is een bevel van de officier van justitie vereist, maar dat bevel kan pas worden verstrekt als het belang van het onderzoek dit dringend vereist en de rechter-commissaris daartoe een machtiging heeft gegeven. De wetgever benadrukt dat het hierbij om uitzonderingsgevallen gaat en geeft als enige voorbeeld het onderzoek waarbij redelijkerwijs voorzienbaar gegevens worden onderzocht die onder het professioneel verschoningsrecht vallen.[47]

9.3.5 De netwerkzoeking

Met de Wet computercriminaliteit I creëerde de wetgever al in 1993 de mogelijkheid om met een zogenoemde 'netwerkzoeking' onderzoek te doen aan aanliggende netwerken van de gegevensdrager waarnaar onderzoek wordt gedaan.[48] Het is met deze opsporingsbevoegdheid bijvoorbeeld mogelijk onderzoek te doen op andere computers (zoals laptops, pc's, mediaspelers en harde schijven) die zijn aangesloten op een intern netwerk (intranet) en de gegevens daarop te analyseren. Het idee van de regeling is dat niet telkens een aparte procedure moet worden doorlopen voor het onderzoek op gegevensdragers. Met de netwerkzoeking kan bijvoorbeeld ook tijdens een doorzoeking in een kantoorpand de mailserver van het bedrijf in een datacentrum (zoals van Microsoft) worden doorzocht. Een opsporingsambtenaar kan dit onderzoek niet zelfstandig verrichten, maar heeft een bevel van de officier van justitie nodig.

Aangenomen wordt dat met een netwerkzoeking ook webmailaccounts (zoals Gmail) of online opslagdiensten (zoals Dropbox) van een verdachte mogen worden doorzocht tijdens de doorzoeking (Commissie-Koops, 2018). Al vele jaren is het een strategie van opsporingsinstanties om cybercriminelen aan te houden terwijl zij zijn ingelogd op hun computers. Als de computer aanblijft tijdens de doorzoeking, kunnen vanaf die computers aanliggende netwerken (en dus ook accounts) worden doorzocht.[49] De verwachting is dat het onder-

47 *Kamerstukken II* 2022/23, 36327, nr. 3, p. 575.

48 Zie artikel 125j Sv.

49 Zie bijvoorbeeld ook R. Wassens, 'Celstraf voor 21-jarige malware-ontwikkelaar', *NRC.nl*, 19 maart 2020 m.b.t. de uitspraak Rb. Rotterdam 19 maart 2020,

zoek van gegevens in een aangesloten genetwerkte computer, zoals een server in een datacentrum, steeds belangrijker wordt. De reden is dat in toenemende mate gegevens elders liggen opgeslagen of gebruik wordt gemaakt van de verwerkingscapaciteit van een genetwerkte computer op een andere locatie (Commissie-Koops, 2018).

De netwerkzoeking op grond van artikel 125j Sv kan slechts worden uitgeoefend tijdens een doorzoeking ter vastlegging van gegevens en kan slechts worden toegepast vanaf de plaats die wordt doorzocht. Dit bleek in de praktijk problemen op te leveren, voornamelijk in de situatie waarin pas na onderzoek van een inbeslaggenomen gegevensdrager bleek dat relevante informatie niet op de gegevensdrager zelf was opgeslagen, maar in een online opslagdienst.[50] Daarnaast duurt het soms te lang of is het niet wenselijk om een netwerkzoeking uit te voeren op de plek waar een doorzoeking plaatsvindt. Binnen woningen met veel huisgenoten of tijdens een doorzoeking in een kantoor kan het behoorlijke hinder veroorzaken als een doorzoeking en het onderzoek op gegevensdragers veel tijd in beslag nemen. Praktisch gezien is dat niet altijd nodig, omdat met forensische software bijvoorbeeld ook de gegevens op aangesloten computers gekopieerd kunnen worden en elders bij het NFI of het politiebureau kunnen worden onderzocht.

Vanwege bovenstaande problematiek is – op advies van de commissie-Koops – in het kader van de modernisering van het Wetboek van Strafvordering de netwerkzoeking uitgebreid in artikel 557 Sv. Op grond van dit artikel is los van de context van de doorzoeking de netwerkzoeking ook mogelijk na de inbeslagname van een gegevensdrager. Dit artikel is inmiddels bij de Innovatiewet Strafvordering ingevoerd.[51] Vanwege de ernstige privacyinbreuk die plaatsvindt tijdens een netwerkzoeking is naast een bevel van een officier van justitie, ook een machtiging van een rechter-commissaris voor de opsporingshandeling vereist.

In de praktijk vragen officieren van justitie echter ook om een machtiging van een rechter-commissaris om – los van een doorzoeking of inbeslagname van een gegevensdrager – in te loggen op een account van een verdachte.[52] Dit

ECLI:NL:RBROT:2020:2395, *Computerrecht* 2020/88, m.nt. J.J. Oerlemans. Zie ook Rb. Overijssel 15 januari 2019, ECLI:NL:RBOVE:2019:161.

50 *Kamerstukken II* 2022/23, 36327, nr. 3, p. 580.

51 *Stb.* 2022, 276.

52 Dit betreft een vordering ex artikel 181 juncto 177 Sv, waarbij analoge toepassing van artikel 126ng lid 2 Sv wordt gevraagd.

wordt ook wel een 'online doorzoeking' of 'doorzoeking op afstand' genoemd. Die toestemming is in het verleden ook gegeven voor het inloggen op bijvoorbeeld een webmail- en Telegramaccount.[53] Het pijnpunt is dat geen bijzondere opsporingsbevoegdheid voor deze opsporingsmethode voorhanden is. Dit staat in spanning met het strafvorderlijk legaliteitsbeginsel en kan leiden tot afwijkende rechterlijke beslissingen en rechtsonzekerheid. Sommige auteurs pleiten daarom voor een nieuwe regeling (Kazlova, 2024).

9.4 Opsporingsmethoden en de uitdaging van anonimiteit

Het probleem van anonimiteit in opsporingsonderzoeken naar cybercriminaliteit is goed gedocumenteerd (zie o.a. Bernaards et al., 2012; Brenner, 2010; Oerlemans, 2017a; UNODC, 2013). In paragraaf 9.3 is uitgelegd en geïllustreerd hoe zelfs in een ideale situatie – waarbij een verdachte gebruikmaakt van zijn vaste internetverbinding vanuit huis – het veel inspanning kost om bewijs te verzamelen op basis van een IP-adres als digitaal spoor. Daarnaast kunnen personen door het gebruik van pseudoniemen (*nicknames*) en virtuele betalingsdiensten ook tot op zekere hoogte anoniem blijven. Veel criminelen maken echter foutjes in hun *operational security* ('opsec') door bijvoorbeeld hetzelfde taalgebruik, uitdrukkingen of quotes te gebruiken die te linken zijn aan de persoon. Opsporingsinstanties kunnen bij de toepassing van opsporingsmethoden gebruikmaken van de foutjes van cybercriminelen of onderling wantrouwen (zie uitgebreid Van de Sandt, 2019).

In deze paragraaf worden eerst belangrijke anonimiseringstechnieken besproken waar cybercriminelen vaak gebruik van maken (paragraaf 9.4.1). Daarna wordt uitgelegd hoe met onderzoek in publiek toegankelijke bronnen (paragraaf 9.4.2) en online undercoverbevoegdheden (paragraaf 9.4.3), ondanks het gebruik van deze anonimiseringstechnieken, in veel gevallen toch bewijs kan worden verzameld.

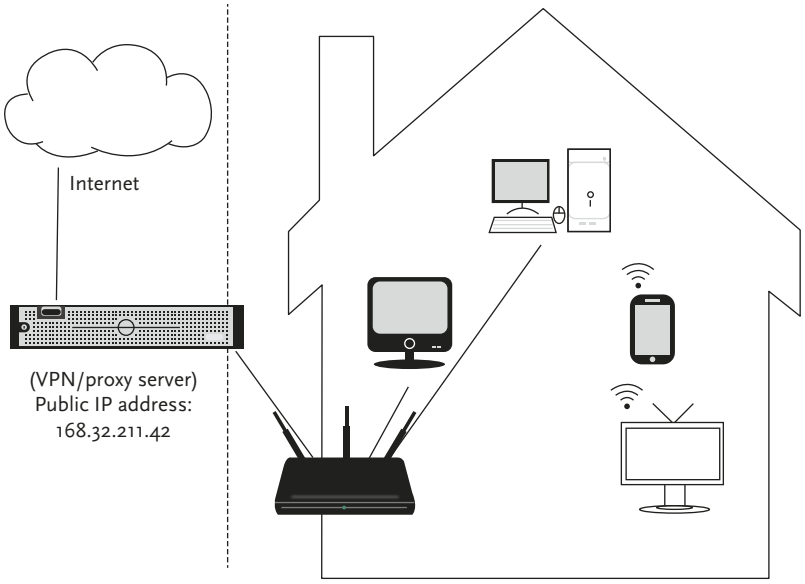
9.4.1 Anonimiseringstechnieken

Een proxydienst fungeert als een tussenstap voordat een computer via internet verbinding maakt met een andere computer, zoals een webserver om een website te bezoeken. Proxydiensten sturen het verkeer door naar de andere computer en wijzigen daarbij het IP-adres van de computer die verbinding

53 Hof Den Haag 19 december 2018, ECLI:NL:GHDHA:2018:3529, *Computerrecht* 2019/51, m.nt. J.J. Oerlemans.

maakt. Het publieke IP-adres waarvan de internetgebruiker gebruikmaakt, verandert in dat geval in het IP-adres van de desbetreffende server van de proxydienst (zie o.a. Hagy, 2007). Cybercriminelen hacken ook computers om deze als proxydienst te laten fungeren (Bernaards et al., 2012).

Bij VPN-diensten wordt het verkeer ook doorgeleid door verschillende servers en wordt het verkeer versleuteld. Versleuteling biedt internetgebruikers extra veiligheid tegen derden die de inhoud van netwerkverkeer willen uitlezen, bijvoorbeeld om wachtwoorden of financiële gegevens over te nemen. Figuur 9.4 illustreert het gebruik van proxy- en VPN-diensten in een woning.



Figuur 9.4 Visualisatie van een proxy- en VPN-dienst[54]

VPN-diensten zijn commerciële diensten. Dat betekent dat personen of instanties zich moeten registreren en betalen voor het gebruik van de diensten. Ook houden VPN-diensten meestal bij wie op welk moment met hun diensten een verbinding maakt. Opsporingsinstanties kunnen in dat geval loggegevens en gebruikersgegevens vorderen om een verdachte te identificeren (Casey, 2011; zie ook paragraaf 9.3.2).

54 Bron: Oerlemans 2017a, p. 39.

Cybercriminelen zullen in veel gevallen echter zo min mogelijk gegevens opgeven bij registratie of (nep)gegevens van iemand anders invoeren. Betaling met bijvoorbeeld prepaidkaarten of virtueel geld biedt ook meer anonimiteit. Gevorderde gegevens zullen daarom niet altijd bruikbaar zijn voor opsporingsinstanties en niet alle dienstverleners werken mee aan vorderingen of verzoeken van opsporingsinstanties.

Bij Tor wordt het internetverkeer langs (ten minste drie) servers gestuurd en wordt het netwerkverkeer versleuteld (zie ook paragraaf 4.2). De tussenliggende Tor-servers leggen geen gegevens vast en alleen het IP-adres van de laatste Tor-server (ook wel 'Tor exit node' of 'Tor exit relay' genoemd) is zichtbaar. Vergelijkbaar met een proxy- en VPN-dienst wordt daarmee het IP-adres van het netwerk van de internetgebruiker verhuld. Het is niet mogelijk gegevens te vorderen bij het Tor-systeem.

9.4.2 Publiek toegankelijke bronnen

Als het opsporingsonderzoek op basis van een IP-adres spaak loopt, zijn er mogelijk andere digitale sporen die opsporingsinstanties kunnen volgen. Daarbij kan met name worden gedacht aan de digitale sporen die personen achterlaten bij gebruik van het internet. Cybercriminelen zijn bijvoorbeeld net als alle andere mensen vaak actief op sociale media. Opsporingsambtenaren kunnen de 'digitale broodkruimels' van de identiteit van mensen op internet volgen om bijvoorbeeld meer te weten te komen over de verdachte, het slachtoffer, de omgeving van de verdachte en het slachtoffer en mogelijk om meer informatie te verzamelen over strafbare feiten. Het verzamelen van gegevens uit publiek toegankelijke bronnen wordt ook wel 'openbronnenonderzoek' of *open source intelligence* (OSINT) genoemd.

Bij onderzoek in publiek toegankelijke bronnen kan onderscheid worden gemaakt tussen het 'handmatig' en 'geautomatiseerd' verzamelen van gegevens (Oerlemans & Koops, 2012). Bij het handmatig vergaren van publiekelijk toegankelijke online gegevens moet worden gedacht aan het vergaren van gegevens die na het invoeren van zoektermen in zoekmachines zoals Google beschikbaar zijn. Daarnaast kan worden gedacht aan het zoeken binnen online telefoongidsen, online discussieforums en socialemediadiensten; ook als registratie is vereist. In het verleden heeft het simpelweg invullen van een nickname van een vermoedelijke hacker in Google al eens in een cyber-

criminaliteitzaak tot identificatie van de verdachte geleid.[55] Ook leverde het e-mailadres van de online drugsbaron bij een advertentie van een voorganger van de beruchte darknet market 'Silk Road' destijds een belangrijk spoor op voor de FBI.[56]

Onderzoek in publiek toegankelijke bronnen kan deels worden geautomatiseerd door gebruik te maken van software. Hierbij kan worden gedacht aan commerciële tools, zoals 'SpiderFoot' en 'Maltego'. Met dergelijke tools kunnen verschillende zoekmachines, internetforums en sociale media tegelijkertijd worden bevraagd met sleutelwoorden. Ook bevatten deze tools vaak optionele betaalde modules of plug-ins. Met behulp van een plug-in of module kan een gebruiker met een aantal muisklikken een bron bevragen. Deze bron kan ook een samengestelde dataset zijn of bestaan uit persoonsgegevens met locatiegegevens die van gebruikers van apps zijn verzameld.[57] De toezichthouder op inlichtingen- en veiligheidsdiensten waarschuwt dan ook dat onderzoek in publiek toegankelijke bronnen niet meer alleen het 'naslaan' van telefoonboeken of het zoeken van gegevens op internet met een zoekmachine is. Met 'automated OSINT' kunnen honderden bronnen van diverse herkomst tegelijkertijd worden geraadpleegd, waaronder locatiegegevens of gegevens uit gelekte datasets. Dat brengt een ernstigere privacy-inbreuk met zich mee dan voorheen door de wetgever werd voorzien (CTIVD, 2021). Ondanks dit vermoedelijk wijdverbreide gebruik van publiek toegankelijke bronnen en OSINT-tools door de politie en andere opsporingsinstanties is hier nauwelijks jurisprudentie over beschikbaar.

Wettelijke basis voor onderzoek in publiek toegankelijke bronnen

Al jaren woedt er een discussie over de vraag hoe onderzoek in publiek toegankelijke bronnen is genormeerd (Oerlemans & Koops, 2012). Het kernprincipe blijft van toepassing dat de algemene taakstellende bepalingen volstaan als wettelijke grondslag, als de inbreuk op privacy slechts beperkt is. Op het moment dat het onderzoek in publiek toegankelijke bronnen een meer dan beperkte inbreuk op het recht op privacy oplevert, is een expliciete wettelijke grondslag vereist (Commissie-Koops, 2018). Dit is zoals eerder genoemd het

55 Zie G. Cutlack, 'Police Caught an Anonymous Hacker by Googling his IRC Name', *Gizmodo*, 12 december 2012.

56 Zie K. Zetter, 'How the Feds Took Down the Silk Road Drug Wonderland', *Wired.com*, 18 november 2015.

57 J. Cox, 'How the U.S. Military Buys Location Data from Ordinary Apps', *Vice.com*, 16 november 2020.

geval als met het onderzoek een min of meer volledig beeld van bepaalde aspecten van het persoonlijk leven van de betrokkene ontstaat.

Als expliciete wettelijke grondslag worden meestal de bijzondere bevoegdheden van stelselmatige observatie (art. 126g Sv) en stelselmatige informatie-inwinning (art. 126j Sv) genoemd (Feenstra, 2018).[58] Een probleem hierbij is echter dat het voor opsporingsambtenaren niet altijd voldoende helder is wanneer het criterium van 'stelselmatigheid' wordt bereikt (zie o.a. Stol & Strikwerda, 2018). Dit probleem is ook uitgebreid aan bod gekomen in het rapport van de commissie-Koops. Deze commissie stelt voor om zo spoedig mogelijk een nieuwe bijzondere opsporingsbevoegdheid tot het 'stelselmatig verzamelen van gegevens omtrent een persoon' te reguleren (Commissie-Koops, 2018).

De wetgever heeft naar aanleiding van dit voorstel in het gemoderniseerde Wetboek van Strafvordering in artikel 2.8.8 Sv voorzien in een wettelijke grondslag voor stelselmatig onderzoek in publiek toegankelijke bronnen. Bij deze nieuwe bevoegdheid gaat het om onderzoek naar 'historische gegevens' die al beschikbaar zijn.[59] Hierin verschilt deze bevoegdheid met de stelselmatige observatie en stelselmatige informatie-inwinning, waarbij het gaat om het 'real-time' waarnemen of volgen van een persoon. De regeling geeft geen concreet moment (bijvoorbeeld in tijd of een situatie) waarbij sprake is van stelselmatigheid. Mogelijk blijft daardoor onduidelijkheid bij opsporingsambtenaren en is het voor de betrokkene minder goed voorzienbaar in welke situatie deze bevoegdheid wordt ingezet.
Opsporingsinstanties zullen ook aan de hand van ervaringsleer moeten bepalen in welke situatie het 'op voorhand redelijkerwijs' voorzienbaar is dat het verzamelen van persoonsgegevens over een persoon stelselmatig is. Dit kan vervolgens in beleid worden vastgelegd.

9.4.3 Undercoverbevoegdheden

Voor opsporingsinstanties is het heel interessant om onder dekmantel de interactie aan te gaan met personen die op internet actief zijn. Net zoals het internet een grenzeloos medium is voor criminelen om met (relatieve) anonimiteit activiteiten te ontplooien, biedt het internet ook voor opsporings-

58 Rb. Den Haag 10 december 2015, ECLI:NL:RBDHA:2015:14365, *Computerrecht* 2016/47, m.nt. J.J. Oerlemans en Hof Den Haag 25 mei 2018, ECLI:NL:GHDHA:2018:1248.

59 *Kamerstukken II* 2022/23, 36327, nr. 3, p. 679.

instanties interessante mogelijkheden. Opsporingsambtenaren kunnen net zo anoniem communiceren als anderen op internet, zonder (direct) lijfelijk risico te lopen en zonder de bureaustoel te hoeven verlaten (Oerlemans, 2018b).

In deze paragraaf worden achtereenvolgens de volgende undercoveropsporingsbevoegdheden besproken: online pseudodoop, stelselmatige informatieinwinning en infiltratie.[60]

Online pseudokoop

De online pseudokoop wordt in de strafrechtpraktijk veelvuldig toegepast door de politie (Kruisbergen & De Jong, 2010). Gepubliceerde uitspraken laten bijvoorbeeld zien dat de bijzondere opsporingsbevoegdheid van pseudokoop in artikel 126i Sv wordt toegepast voor de aankoop van drugs, vuurwapens, vuurwerk, ivoor van bedreigde diersoorten en andere gestolen goederen op online handelsplaatsen.[61] De online pseudokoop biedt opsporingsautoriteiten de mogelijkheid na te gaan wie het pakketje met het goed of de gegevens verzendt. Als de verdachte de verzending zelf verzorgt, dan geeft hij of zij mogelijk identificerende gegevens vrij. Een pakketje met drugs kan bijvoorbeeld vingerafdrukken of DNA-materiaal (via een postzegel) bevatten, op basis waarvan verder onderzoek kan plaatsvinden.[62] Bij de aankoop van goederen of gegevens via internet gaat daar soms online communicatie aan vooraf. Tijdens deze communicatie is het wellicht mogelijk identificerende gegevens van een verdachte te achterhalen, zoals een nickname, naam, en/of e-mailadres. Deze gegevens bieden op hun beurt weer mogelijkheden voor andere opsporingshandelingen, zoals het vorderen van gegevens bij internetdienstverleners.

60 De regels voor de inzet van burgers bij undercoveroperaties komen in deze paragraaf niet aan de orde. Zie daarvoor o.a. de Aanwijzing bijzondere opsporingsbevoegdheden, *Stcrt.* 2014, 24442.

61 Zie bijvoorbeeld Rb. Roermond 4 maart 2009, ECLI:NL:RBROE:2009:BH4757 (goederen op Marktplaats.nl), Rb. Zutphen 28 januari 2011, ECLI:NL:RBZUT:2011:BP2308 (illegale wapens), Rb. Oost-Brabant 6 mei 2013, ECLI:NL:RBOBR:2013:BZ9467 (illegaal vuurwerk), Rb. Rotterdam 8 mei 2014, ECLI:NL:RBROT:2014:3504 (drugs op Silk Road), Rb. Overijssel 18 april 2016, ECLI:NL:RBOVE:2016:1323 (ivoor van bedreigde diersoorten), Rb. Den Haag 17 mei 2018, ECLI:NL:RBDHA:2018:5775 (creditcardgegevens van LizardSquad-verdachte), Rb. Noord-Nederland 21 april 2022, ECLI:NL:RBNNE:2022:1356 (ritalin op Dream Market), Rb. Overijssel 14 juni 2022, ECLI:NL:RBOVE:2022:4059 (drugs op darknet market), Rb. Noord-Nederland 19 januari 2023, ECLI:NL:RBNNE:2023:165 (erectiemiddel op clear web website).

62 Zie bijvoorbeeld Rb. Overijssel 14 juni 2022, ECLI:NL:RBOVE:2022:4059.

De opsporingsbevoegdheid van de pseudokoop mag worden toegepast jegens de verdachte, nadat een bevel van een officier van justitie is afgegeven om een goed of gegevens aan te kopen. Daarbij moet het gaan om opsporingsonderzoeken met betrekking tot misdrijven zoals omschreven in artikel 67 Sv. Hoewel een algemeen verbod tot uitlokking altijd van toepassing is, wordt in artikel 126i lid 2 Sv er nogmaals op gewezen dat 'een persoon er niet toe mag worden bewogen om een delict te plegen dat hij niet voornemens was'.[63] Als een verdachte een illegaal goed of gegevens op internet aanbiedt en een opsporingsambtenaar koopt vervolgens het aangeboden goed of de gegevens, dan zal van uitlokking niet snel sprake zijn. De opsporingshandelingen in undercoveroperaties moeten zorgvuldig worden geverbaliseerd, zodat ter zitting kan worden nagegaan dat er geen sprake geweest is van uitlokking en het recht op een eerlijk proces in artikel 6 van het Europees Verdrag voor de Rechten van de Mens (EVRM) niet is geschonden.

In het gemoderniseerde Wetboek van Strafvordering wordt de kring van personen tegen wie de bevoegdheid tot pseudokoop kan worden ingezet uitgebreid.[64] In het wetsvoorstel wordt namelijk gesproken van 'een persoon'. Hierdoor kan de bevoegdheid ook worden ingezet jegens een persoon die niet als verdachte kan worden aangemerkt, maar die bijvoorbeeld slechts een tussenpersoon – denk hierbij aan een koerier – is die geen weet heeft van de illegale activiteiten. Door de bevoegdheid jegens de koerier in te zetten, kan worden achterhaald wie de achterliggende verdachte is voor wie de koerier werkzaam is.

Stelselmatige informatie-inwinning

Via internet kunnen opsporingsambtenaren onder dekmantel de interactie aangaan met verdachten en personen in diens omgeving. Deze interacties vinden bijvoorbeeld plaats op chatkanalen, online discussie- of handelsforums of door 'vrienden' te worden met de verdachte of diens vrienden op sociale media om vervolgens met hen te communiceren. Het is daarbij zelfs denkbaar dat het account van een persoon wordt overgenomen en onder

63 Zie verder over het uitlokkingsverbod 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 4 november 2010, nr. 18757/06, ECLI:CE:ECHR:2010:1104JUD001875706, *EHRC* 2011/9, m.nt. F.P. Ölçer (*Bannikova t. Rusland*). Zie ook *Kamerstukken II* 1996/97, 25403, nr. 3, p. 31.

64 *Kamerstukken II* 2022/23, 36327, nr. 3, p. 688.

de identiteit van iemand anders met een verdachte wordt gecommuniceerd (Oerlemans, 2018b).[65]

De opsporingsmethode mag plaatsvinden op basis van de algemene taakstelling in artikel 3 Politiewet en artikelen 141 en 142 Sv, voor zover het niet op stelselmatige wijze wordt toegepast. Bij stelselmatige informatie-inwinning is de bijzondere opsporingsbevoegdheid van artikel 126j Sv van toepassing.[66] Zoals eerder is uitgelegd in paragraaf 9.3.4, is sprake van stelselmatigheid als een 'min of meer volledig beeld van bepaalde aspecten van iemands privéleven' wordt verkregen.[67] Het is voor deze bevoegdheid kenmerkend dat er een actieve interferentie in het leven van de verdachte plaatsvindt; het gaat verder dan louter om het (passief) observeren van het gedrag van personen of zaken.[68] De bevoegdheid tot stelselmatige informatie-inwinning kan worden ingezet bij de opsporing van elk misdrijf voor een (verlengbare) periode van drie maanden. Voor de inzet is een bevel van een officier van justitie vereist. Voor de uitvoering worden doorgaans leden van het team 'Werken onder Dekmantel' van de politie ingezet.[69]

De toepassing van stelselmatige informatie-inwinning kan een ernstige inbreuk op de persoonlijke levenssfeer van de verdachte opleveren, omdat de undercoveragent in een langdurig traject een relatie met de verdachte kan opbouwen. Het is goed mogelijk dat de verdachte in de veronderstelling is een innige vriendschappelijke band te hebben, waarna blijkt dat hij is 'verraden' vanwege misleiding door de undercoveragent (Kruisbergen & De Jong, 2012).

Welke grondslag in het Wetboek van Strafvordering ook wordt toegepast, het is van belang dat opsporingsinstanties de opsporingshandelingen voldoende vastleggen (bijvoorbeeld met behulp van software), zodat de verdediging en rechter kunnen nagaan of van stelselmatigheid sprake is geweest en het uitlokkingsverbod niet is geschonden.

65 Zie bijvoorbeeld ook Rb. Noord-Nederland 21 december 2022, ECLI:NL:RBNHO:2022:11404.

66 Zie Rb. Noord-Nederland 27 juli 2017, ECLI:NL:RBNNE:2017:2882, *Computerrecht* 2018/6, m.nt. J.J. Oerlemans.

67 Zie *Kamerstukken II* 1996/97, 25403, nr. 3, p. 26-27.

68 Zie *Kamerstukken II* 1996/97, 25403, nr. 3, p. 35.

69 Zie de Aanwijzing opsporingsbevoegdheden, *Stcrt.* 2014, 24442.

Casus: Facebookvrienden worden met de verdachte

De 'Context-zaak' is een terrorismezaak waarbij verdachten zijn vervolgd en veroordeeld voor opruiing tot een terroristisch misdrijf en het (medeplegen) van de verspreiding van tot terroristisch misdrijf opruiend materiaal via YouTube en sociale mediadiensten zoals Facebook en Twitter.[70] Opsporingsambtenaren hebben in deze zaak 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. Het hof Den Haag overweegt in zijn arrest dat 'met het handmatig vergaren van (persoons)gegevens (bijvoorbeeld door het bekijken van een openbaar profiel op sociale media) slechts sprake is van een geringe inmenging in de rechten en vrijheden van de betrokkene en de integriteit van het opsporingsonderzoek wordt daarmee niet in gevaar gebracht'.[71]

Voor het aanmaken van het account op Facebook was volgens het hof wel de inzet van de bijzondere opsporingsbevoegdheid van stelselmatige informatie-inwinning vereist. Ook was door gebrekkige vastlegging niet meer precies na te gaan welke opsporingshandelingen plaatsvonden, waardoor niet goed kon worden nagegaan met wie de politie nu precies Facebook-vrienden is geworden en welke berichten door de politie zelf zijn verspreid.[72] Deze vormverzuimen zijn volgens vaste jurisprudentie gerelativeerd tot vaststelling van de gebreken, zonder consequenties voor de strafmaat. De verdachten zijn in deze zaak veroordeeld tot vijfenhalf jaar gevangenisstraf.

De wetgever maakt in het kader van de modernisering van het Wetboek van Strafvordering in artikel 2.8.11 Sv een onderscheid tussen een lichtere

70 Rb. Den Haag 10 december 2015, ECLI:NL:RBDHA:2015:14365, *Computerrecht* 2016/46, m.nt. J.J. Oerlemans, Hof Den Haag 25 mei 2018, ECLI:NL:GHDHA:2018:1248 en HR 24 maart 2020, ECLI:NL:HR:2020:447 (*Context*-zaak). Zie ook o.a. D. de Staaij (red.), 'Jihadnetwerk Den Haag "terroristische organisatie"', *Een Vandaag*, 3 oktober 2014.

71 Hof Den Haag 25 mei 2018, ECLI:NL:GHDHA:2018:1248.

72 Zie ook M. Haenen & A. Kouwenhoven, 'Infiltratie gelukt, gegevens weg', *NRC.nl*, 9 oktober 2015.

en zwaardere variant van stelselmatige informatie-inwinning.[73] De lichtere variant in het eerste lid van artikel 2.8.11 Sv sluit aan bij het huidig recht, met de aanpassing dat ook hier de bevoegdheid jegens 'een persoon' mag worden uitgeoefend. Deze persoon hoeft dus niet zoals bij het wetsvoorstel met betrekking tot de pseudokoop de verdachte te zijn. Bij deze lichtere variant kan worden gedacht aan het onderhouden van (intensief) contact met die persoon. De zwaardere variant in het tweede lid van artikel 2.8.11 Sv ziet op de stelselmatige informatie-inwinning van een persoon door diegene activiteiten te laten verrichten, hetgeen verder gaat dan het 'slechts' onderhouden van contact op grond van het eerste lid. De activiteiten worden door de politie geïnitieerd, waarbij volgens de wetgever kan worden gedacht aan het door de desbetreffende persoon laten verrichten van werkzaamheden ten behoeve van de fictieve onderneming van de opsporingsambtenaar.[74] Deze indringendere vorm van stelselmatige informatie-inwinning is gebonden aan zwaardere voorwaarden, zo dient er bijvoorbeeld voor de toepassing van deze bevoegdheid een machtiging te worden verkregen van de rechter-commissaris.

De lokpuber

Met de implementatie van de Wet computercriminaliteit III kunnen opsporingsambtenaren zich ook voordoen als minderjarige (als 'lokpuber') en chatten met andere internetgebruikers in opsporingsonderzoeken naar verdachten van grooming en ontucht. Eerder heeft een dergelijke undercoveroperatie tot vrijspraak geleid, omdat voor de delictsomschrijving was vereist dat met een *zestienminner* wordt afgesproken (zie uitgebreid Schermer et al., 2016).[75]

De tekst van artikel 248e Sr (oud) (grooming) en artikel 248a Sr (oud) (ontucht) werd aangepast, waardoor het helder is dat ook van grooming en ontucht sprake kan zijn als een meerderjarige opsporingsambtenaar of zelfs een computerprogramma met de verdachte onder dekmantel communiceert.

Er is ook kritiek gekomen op de wetswijziging. Zo twijfelt De Hingh (2018) aan de noodzaak en wenselijkheid van de strafbaarstelling van grooming met virtuele creaties. Met de wetswijziging wordt bovendien door een aanpassing in het materieel strafrecht een nieuwe opsporingsmethode mogelijk gemaakt. Daarbij is de grens met het uitlokkingsverbod precair (zie Ölçer, 2014). Opsporingsambtenaren kunnen rekening houden met het uitlokkingsverbod

73 *Kamerstukken II* 2022/23, 36327, nr. 3, p. 690-692.
74 *Kamerstukken II* 2022/23, 36327, nr. 3, p. 692.
75 Zie Hof Den Haag 25 juni 2013, ECLI:NL:GHDHA:2013:2302.

door de communicatie met een minderjarige niet zelf te starten, maar af te wachten tot iemand contact met hen legt voor seksuele doeleinden.[76]

Infiltratie

Infiltratieoperaties onderscheiden zich van stelselmatige inwinning in de zin dat bij infiltratieoperaties wordt *geparticipeerd* in een criminele organisatie met als doel bewijsmateriaal over strafbare feiten te verzamelen.[77] 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 dat met de opsporingsmethode inzicht kan worden verkregen in de modus operandi van de verdachten.[78] Voor de uitvoering worden in principe medewerkers van het team 'Werken onder Dekmantel' van de politie ingezet.[79]

Een infiltratieoperatie mag, kort gezegd, alleen worden gestart nadat een bevel is verkregen van een officier van justitie in opsporingsonderzoeken naar misdrijven zoals omschreven in artikel 67 Sv. Bovendien moet sprake zijn van een ernstige schending van de rechtsorde en het onderzoek moet de inzet van de BOB-bevoegdheid 'dringend vorderen'.[80] Als intern controlemechanisme dient de officier van justitie toestemming te vragen aan het College van procureurs-generaal, dat daartoe door de Centrale Toetsingscommissie (CTC) wordt geadviseerd.

In de nieuwe regeling in het gemoderniseerde Wetboek van Strafvordering dient, nadat het College van procureurs-generaal toestemming voor de toepassing van de infiltratiebevoegdheid heeft gegeven, er een machtiging van een rechter-commissaris te worden verkregen. Hier is veel voor te zeggen, gezien de voorkeur van het Straatsburgse Hof voor de betrokkenheid van een rechter bij deze indringende opsporingsbevoegdheid (Koops & Oerlemans, 2019b).[81]

76 Zie ook *Kamerstukken I* 2016/17, 34372, nr. D, p. 27.

77 Zie *Kamerstukken II* 1996/97, 25403, nr. 3, p. 28-29. Zie ook de brief van de minister van Veiligheid en Justitie van 8 oktober 2014 over het juridische verschil tussen 'informanten' en 'individuen die infiltreren binnen een opsporingsonderzoek', *Kamerstukken II* 2014/15, 29279, nr. 208.

78 Zie *Kamerstukken II* 1996/97, 25403, nr. 3, p. 28.

79 Zie de Aanwijzing opsporingsbevoegdheden, *Stcrt.* 2014, 24442.

80 Zie artikel 126h Sv.

81 Zie EHRM 24 juni 2008, nr. 74355/01, ECLI:CE:ECHR:2008:0624JUD007435501 (*Milinienè t. Litouwen*), EHRM 4 november 2010, nr. 18757/06, ECLI:CE:ECHR:2010:1104JUD001875706 (*Bannikova t. Rusland*) en EHRM 23 okto-

Dergelijke waarborgen in infiltratieoperaties zijn daarnaast belangrijk, omdat met deze bevoegdheid niet alleen een zeer ingrijpende inbreuk op het privéleven van de verdachte wordt gemaakt, maar ook op het privéleven van andere betrokkenen. Verder bestaan er bij dergelijke undercoveroperaties risico's omtrent de integriteit en beheersbaarheid van de opsporing. In sommige gevallen mogen in het traject namelijk (vooraf afgestemde) strafbare feiten worden gepleegd en bestaat daardoor het risico dat agenten het verkeerde pad op gaan (ook wel *going rogue* genoemd) (Kruisbergen & De Jong, 2010). Dat geldt ook voor online undercoveroperaties. Daarbij kan bijvoorbeeld worden verwezen naar de Amerikaanse opsporingsambtenaar die na de inbeslagname van de digitale portemonnee van de eigenaar van Silk Road zonder toestemming ook bitcoins naar zichzelf overmaakte om bij te verdienen.[82]

Casus: Operatie Bayonet (Hansa Market)

Operatie 'Bayonet' vormt een uitstekend voorbeeld van de toepassing van infiltratie als opsporingsbevoegdheid in een digitale context. Van 20 juni tot 20 juli 2017 nam de Nederlandse politie de online handelsplaats 'Hansa Market' over.[83]

Hansa Market was begin 2017 een populaire darknet market, voornamelijk gericht op drugshandel. De absolute nummer één was echter 'AlphaBay', een darknet market waar niet alleen drugs, maar ook andere illegale goederen zoals vuurwapens beschikbaar waren.[84] Op enig moment was AlphaBay maar liefst tien keer zo groot dan het fameuze 'Silk Road'. Begin 2017 maakten Amerikaanse opsporingsdiensten AlphaBay ontoegankelijk. In samenwerking met het Nederlandse THTC en in coördinatie met Europol ging 'Operation Bayonet' van start. De Amerikanen gaven na de ontoegankelijkheidsmaking van AlphaBay geen uitgebreide persconferentie, maar lieten de darknet market-gebruikers in verwarring

ber 2014, nr. 54648/09, ECLI:CE:ECHR:2014:1023JUD005464809 (*Furcht t. Duitsland*), *EHRC* 2015/1, m.nt. F.P. Ölçer.

82 Reuters, 'US undercover agent jailed for six years for Silk Road Bitcoin theft', *BBC News*, 20 oktober 2015.

83 H. Modderkolk, 'Zo nam de Nederlandse politie een online drugsmarkt over', *Volkskrant.nl*, 19 augustus 2017.

84 Zie persbericht FBI, 'Darknet Takedown. Authorities Shutter Online Criminal Market AlphaBay', 20 juli 2017.

over wat er was gebeurd. Veel kopers en verkopers verplaatsten zich, zoals verwacht, naar de nummer 2 van darknet markets: Hansa Market. De migratie van gebruikers naar andere markten wordt ook wel het 'waterbedeffect' genoemd (Van Wegberg & Verburgh, 2018). Op Hansa Market steeg het aantal bezoekers van 1000 naar 8000 per dag.[85]

De Nederlandse politie kreeg en hield voor ongeveer een maand de controle over de Hansa Market. Daartoe werd de inhoud van de servers van de Hansa Market gekopieerd en overgeplaatst van Litouwen naar een datacentrum in Nederland. Als de *administrators* van de markt runde de Nederlandse politie onder leiding van het OM en in samenwerking met buitenlandse opsporingsinstanties de drugsmarkt. Tijdens deze overname vonden in totaal meer dan 27.000 transacties plaats en werd een schat aan informatie verzameld, waaronder de informatie van 20.000 gebruikers en 10.000 thuisadressen. Deze gegevens zijn verstrekt aan Europol en van daaruit verder gedistribueerd naar opsporingsinstanties in andere landen. Ook de communicatie tussen het personeel en gebruikers van de darknet market en de financiële administratie is in kaart gebracht. Deze informatie kan belastende informatie opleveren voor verdere vervolging.[86]

De operatie had ook duidelijk tot nevendoel om gedigitaliseerde criminaliteit te verstoren. Met de operatie werd aan darknet market-gebruikers duidelijk gemaakt dat zij niet anoniem waren. Bekende Nederlandse verkopers (*vendors*) zijn daarnaast door de Nederlandse politie met naam en toenaam genoemd (zie figuur 9.5).

85 Zie ook persbericht OM, 'Ondergrondse Hansa Market overgenomen en neergehaald', 20 juli 2017.

86 Zie o.a. A. Greenberg, 'Operation Bayonet: Inside the Sting That Hijacked an Entire Dark Web Drug Market', *Wired*, 3 augustus 2018.

Figuur 9.5 Screenshot getoonde afbeelding bij Hansa-operatie

Veel criminelen moesten als gevolg van de Hansa-operatie afscheid nemen van de nickname die ze al lange tijd gebruikten en waarmee ze een bepaalde reputatie hadden opgebouwd. Ze moesten als het ware 'opnieuw' beginnen, wat ook als een verstorend effect kan worden gezien. De politie hoopt dat met deze operatie de verkopers stoppen met de verkoop van drugs op online drugsmarkten (Oerlemans & Van Wegberg, 2019). Naast een aantal aanhoudingen hield de Nederlandse politie ongeveer vijftig *knock & talk*-gesprekken om kopers en verkopers af te schrikken van het gebruik van de online drugsmarkten (zie ook hoofdstuk 10 over het gebruik van knock & talk als interventie bij cybercriminaliteit). Van Wegberg en Verburgh (2018) leggen in hun artikel overtuigend uit hoe door middel van meer technisch-criminologisch onderzoek het mogelijk is om de gevolgen en effectiviteit van dergelijke operaties tot in detail in kaart te brengen.

Een van de verkopers op Hansa Market is op 3 juli 2019 door de rechtbank Rotterdam tot vijf jaar gevangenisstraf veroordeeld voor het witwassen van bitcoins voor in totaal meer dan 800.000 euro; ook had de verdachte samen met anderen meer dan 22.000 drugsbestellingen afgeleverd.[87]

87 De drugs werden verstopt in speciaal met 3D-printers geprinte verpakkingen zoals make-updoosjes. Twee medeverdachten zijn ook veroordeeld, zie Rb. Rotterdam 4 juli 2019, ECLI:NL:RBROT:2019:6049 en ECLI:NL:RBROT:2019:6050.

De rechtbank legt in het vonnis uit dat onder het bevel van een officier van justitie de infiltratiebevoegdheid van artikel 126h Sv rechtmatig is ingezet. Ook is volgens de rechtbank geen sprake van uitlokking. De rechtbank past daarbij de gebruikelijke toets toe of de verkopers en kopers door het onderzoeksteam door de overname niet tot andere strafbare feiten zijn gebracht, dan die waarop hun opzet reeds was gericht. Met de geruisloze overname van Hansa Market heeft het onderzoeksteam de bestaande situatie in zoverre ongewijzigd voortgezet. Niet is gebleken dat verkopers (of kopers) door de overname, dan wel door het handelen van het onderzoeksteam, zijn gebracht tot het begaan van andere strafbare feiten dan waarop hun opzet reeds van tevoren was gericht. Het toelaten van nieuwe verkopers en het aanbieden van een korting bij personen bij wie al het opzet bestond om te handelen in verdovende middelen op deze specifieke en verborgen website, passen volgens de rechtbank eveneens in dit kader en kunnen dan ook niet worden gekwalificeerd als uitlokking.[88]

9.5 Opsporingsmethoden en de uitdaging van versleuteling

De versleuteling van gegevens is essentieel om onbevoegden niet de kans te geven om kennis te nemen van gegevens. Bij gebruikmaking van cryptografie worden gegevens, kort gezegd, door middel van een wiskundig algoritme omkeerbaar onleesbaar gemaakt.[89] Met behulp van een sleutel kunnen gegevens vervolgens weer leesbaar worden gemaakt.[90] Cryptografie is een essentiële techniek om vertrouwelijk met anderen te communiceren (Arnbak, 2015). Voor een deel zit er versleuteling in de apparaten waarvan wij dagelijks gebruikmaken. Denk bijvoorbeeld aan de standaard versleuteling op mobiele telefoons en laptops voor beveiliging en het bezoeken van websites die zijn beveiligd met het ssl-protocol (zichtbaar als https:// i.p.v. http://).

Het gebruik van cryptografie heeft tegelijkertijd een keerzijde. Het levert namelijk problemen op voor opsporingsinstanties bij het aftappen van telecommunicatie (gegevens in transport), het doen van onderzoek in computers en bij het kennis willen nemen van mogelijk belastende gegevens (gegevens in opslag). Al sinds het begin van de jaren negentig spreken opsporingsinstanties de verwachting uit dat de opsporing ineffectief wordt (*going dark*)

88 Zie ook Rb. Rotterdam 3 juli 2019, ECLI:NL:RBROT:2019:5339, *Computerrecht* 2019/178, m.nt. J.J. Oerlemans.

89 De gegevens worden, anders gezegd, omgezet in *cipher text*.

90 De gegevens worden omgezet in *plain text*.

door crimineel cryptogebruik. Tijdens de eerste 'cryptowar' van halverwege de jaren negentig werden maatregelen voorgesteld, zoals het vereisen van een vergunning voor het gebruik van cryptografie en het beschikbaar stellen van de cryptosleutels (*key escrow*) aan de overheid ten behoeve van de nationale veiligheid en opsporing (Koops, 1999). Varianten van deze voorstellen zijn in enkele landen geïmplementeerd, maar hebben geen mondiale uitwerking gekregen (Koops & Oerlemans, 2019b).

Inmiddels is versleuteling in opsporingsonderzoeken gemeengoed geworden. Dat is voor een belangrijk deel te wijten aan mobiele telefoons die in beslag worden genomen in opsporingsonderzoeken. Op die telefoons zit vrijwel altijd een vorm van encryptie. Andere vormen van encryptie waarmee de opsporing zich geconfronteerd ziet, zijn versleutelde chatdiensten, vergrendelde devices anders dan mobiele telefoons (bijvoorbeeld laptops), versleutelde e-maildiensten en cryptotelefoons. Volgens een recent onderzoek naar het probleem van versleuteling in de opsporing komt encryptie het meest voor bij georganiseerde (drugs)criminaliteit, cybercriminaliteit en opsporingsonderzoeken naar seksueel materiaal van minderjarigen (Jansen et al., 2023).

Sinds 2014 pleitten – in het bijzonder Amerikaanse – vertegenwoordigers van opsporingsinstanties voor de wettelijke verplichting om handhavingsinstanties toegang te geven tot onversleutelde informatie. Een tweede cryptowar is daarmee van start gegaan. Overheden pleiten daarbij over het algemeen niet meer tot het afschaffen of verbieden van bepaalde cryptografie. Het ligt meer voor de hand dat op de een of andere wijze een 'achterdeurtje' in systemen moet worden gebouwd om de versleuteling ongedaan te kunnen maken. Een belangrijk bezwaar is dat de ICT-infrastructuur hier echter inherent onveilig van wordt, omdat ook andere actoren dan goedwillende overheidsinstanties misbruik kunnen maken van de achterdeur, zoals de autoriteiten van buitenlandse mogendheden en technisch zeer vaardige criminelen (Bellovin et al., 2013).[91] Vooralsnog zijn (met name Amerikaanse) elektronische communicatiedienstaanbieders, zoals Facebook en Apple, niet verplicht om communicatieverkeer te ontsleutelen voor opsporingsinstanties. Koops en Kosta (2018) verklaren dit door te stellen dat beleidsmakers zich mogelijk realiseren dat het inbouwen van achterdeuren een doodlopende weg is en dat steeds meer landen hackbevoegdheden invoeren, waarmee met een meer op maat gesneden wijze toegang kan worden verkregen tot de systemen waarmee betrokkenen communiceren.

91 EHRM 13 februari 2024, nr. 33696/19, ECLI:CE:ECHR:2024:0213JUD003369619 (*Podchasov t. Rusland*), *EHRC-Updates.nl*, m.nt. J.H.L. Banning, par. 77.

Jansen et al. (2023) stellen in hun onderzoek ook wel de vraag wat encryptie écht anders maakt voor het opsporingswerk. Het beschermen en verkrijgen van informatie is altijd al onderdeel geweest van het zogenoemde kat-en-muisspel tussen politie en criminelen. Uiteindelijk, zo stellen de onderzoekers, vraagt digitalisering van politie en haar partners meebewegen en aanpassen aan wat er op hen afkomt.

In deze paragraaf worden beide vormen van versleuteling (versleuteling in opslag en versleuteling in transport) kort behandeld. Daarna wordt aangegeven op welke wijze de hackbevoegdheid ook in Nederland wordt ingezet om met de uitdaging van versleuteling in cybercriminaliteitszaken om te gaan.

9.5.1 Versleuteling in opslag

Bij versleuteling van gegevens in opslag kunnen het hele apparaat, een harde schijf of individuele bestanden versleuteld worden. Via internet is gratis versleutelsoftware verkrijgbaar en versleuteling is vaak een standaardoptie bij mobiele telefoons, laptops, harde schijven en USB-sticks. Deze versleuteling is heel sterk, waarbij naar verluidt opsporingsinstanties de grootste moeite hebben de bestanden te kraken, oftewel de opgeslagen inhoud op computers weer leesbaar te maken (Europol, 2015a; Mevis et al., 2016).[92] Binnen de bevoegdheid om een apparaat (zoals een iPhone) in beslag te nemen, valt ook de bevoegdheid om kennis te nemen van de opgeslagen gegevens en de beveiliging – voor zover mogelijk – ongedaan te maken.

Het omzeilen van encryptie kan door het vinden van de sleutel, het raden van de sleutel, het afdwingen van de sleutel, het exploiteren van een lek in de encryptiesoftware, het verkrijgen van toegang tot leesbare tekst als het apparaat in gebruik is en door het lokaliseren van een kopie van de leesbare tekst. Voor het technisch kraken – ofwel toegang krijgen tot een computersysteem met behulp van forensische hulpmiddelen – is adequate soft- en hardware nodig. Het kraken wordt veelal uitbesteed aan een andere partij of afdeling, zoals het NFI (Jansen et al., 2023).

In sommige gevallen is het ook mogelijk een opgeslagen reservekopie van een telefoon of harde schijf bij een bedrijf te vorderen.[93] De Nederlandse regering heeft hierover opgemerkt dat het in de praktijk echter niet altijd

92 Zie ook *Kamerstukken II* 2015/16, 34372, nr. 3, p. 7-8.

93 Zie ook P. Rosenzweig, 'iPhones, the FBI, and Going Dark', *Lawfareblog.com*, 4 augustus 2015.

mogelijk is om de benodigde gegevens te vorderen als het bedrijf in het buitenland gevestigd is. In dat geval zijn rechtshulpverzoeken noodzakelijk, die tot grote vertragingen kunnen leiden.[94] Zonder een rechtshulpverdrag is het ook mogelijk dat opsporingsautoriteiten met lege handen komen te staan (zie verder paragraaf 9.6 over jurisdictie).

Ontsleutelingsbevel

In zowel de jaren negentig als tijdens de wetsbehandeling van de Wet computercriminaliteit III is het onderwerp van discussie geweest of een 'ontsleutelingsbevel' kan worden afgegeven aan de verdachte, onder dreiging van een gevangenisstraf. Bij het gedwongen afgeven van een wachtwoord of pincode moet de verdachte gedwongen een 'geestesinspanning' leveren, wat op gespannen voet staat met het nemo-teneturbeginsel, het zwijgrecht en de verklaringsvrijheid. Deze fundamentele rechten worden afgeleid uit het recht op een eerlijk proces van artikel 6 EVRM (Van Toor, 2019). Beide keren vond de regering de maatregel uiteindelijk niet wenselijk, mede omdat iemand dwingen een wachtwoord ter ontsleuteling van gegevens af te geven te zeer op gespannen voet staat met het beginsel niet mee te hoeven werken aan de eigen veroordeling (het nemo-teneturbeginsel) (Koops & Oerlemans, 2019b).

De bevoegdheid tot het dwingen tot een ontgrendeling van de biometrische beveiliging – dat wil zeggen: beveiliging op basis van biometrische gegevens zoals een vingerafdruk en irisscan – is echter inmiddels door de Hoge Raad erkend.[95] Zowel de verdachte als niet-verdachte personen dienen hierbij lichte dwang te dulden. Deze bevoegdheid is in het kader van de modernisering van het Wetboek van Strafvordering gecodificeerd in artikel 558 Sv en is bij de Innovatiewet Strafvordering ingevoerd.[96]

Verder is in artikel 125k Sv wel een ontsleutelingsbevel opgenomen voor anderen dan verdachten, zoals systeembeheerders. Deze bevoegdheid kan slechts worden toegepast bij een doorzoeking of in het kader van het vorderen van vastgelegde gegevens. De verplichting tot ontsleuteling geldt alleen voor zover de geadresseerde daartoe in staat is. De persoon hoeft geen technische voorzieningen aanwezig te hebben om te kunnen ontsleutelen; van hem of haar kan slechts worden verlangd dat het signaal in de vorm waarin dit is aangeboden ontsleutelt, voor zover hij of zij (nog) over de sleutel beschikt (Koops & Oerlemans, 2019b). In het gemoderniseerde Wetboek van Strafvor-

94 Zie *Kamerstukken II* 2015/16, 34372, nr. 3, p. 9.
95 HR 9 februari 2021, ECLI:NL:HR:2021:202.
96 *Stb.* 2022, 276.

dering wordt het ontsleutelingsbevel buiten de gevallen van een doorzoeking ook mogelijk gemaakt na de inbeslagneming van een gegevensdrager.[97]

9.5.2 Versleuteling in transport

Bij de telecommunicatietap geldt dat het versleutelen van gegevens de inhoud in principe onleesbaar maakt voor justitie. In de laatste tien jaar is dit vooral een probleem gebleken met betrekking tot het leesbaar maken van privéberichten die via populaire programma's, zoals WhatsApp, worden verstuurd en de toepassing van versleuteling van internetverkeer naar websites (Oerlemans, 2012).

Opsporingsinstanties kunnen op grond van artikel 126m Sv met de inzet van de bijzondere opsporingsbevoegdheid van een telecommunicatietap gegevens aftappen en later uitlezen of uitluisteren. Gezien de ernstige privacy-inbreuk die daarbij plaatsvindt, zijn daarvoor een bevel van een officier van justitie en een machtiging van een rechter-commissaris noodzakelijk. Een tap is alleen mogelijk bij misdrijven waarvoor voorlopige hechtenis is toegelaten en die een ernstige inbreuk op de rechtsorde opleveren. Een tapbevel wordt gegeven voor ten hoogste vier weken, maar dit kan telkens met een termijn van ten hoogste vier weken worden verlengd.

In de standaardsituatie tapt de aanbieder van openbare telecommunicatie het netwerkverkeer. Aanbieders van openbare telecommunicatie zijn op basis van artikel 13.2 Telecommunicatiewet verplicht mee te werken aan een tapbevel en hebben daarvoor een tapinfrastructuur ingericht (Koops & Oerlemans, 2019b). De opsporingsambtenaar kan echter eventueel ook zelf de bevoegdheid uitvoeren door tapapparatuur te plaatsen. In de regel wordt een tap bij aanbieders geplaatst op een specifiek telefoonnummer (of ander identificerend nummer van een telefoon, zoals een zogenoemd IMEI-nummer). Vervolgens wordt het hele gesprek opgenomen en worden andere gegevens, zoals locatiegegevens, naar de politie doorgestuurd. Ook het netwerkverkeer dat van en uit een mobiele telefoon gaat, kan worden afgetapt.

Uit een WODC-onderzoek blijkt dat de aftapbaarheid van communicatie sterk is verminderd in de afgelopen tien jaar (Odinot et al., 2012). Dat is met name ingegeven door de omslag van communicatie met de telefoon naar communicatie via internet. Zoals gezegd is het niet altijd mogelijk bij versleuteld internetverkeer de inhoud van het verkeer uit te lezen. Populaire program-

97 *Kamerstukken II* 2022/23, 36327, nr. 3, p. 588-589.

ma's zoals WhatsApp worden ook wel aangeduid als Over The Top (OTT)-diensten en worden (vooralsnog) niet gezien als aanbieders van openbare telecommunicatienetwerken of -diensten die onder de Telecommunicatiewet een tapinfrastructuur moeten bouwen om aan de 'taplast' te voldoen. Deze (veelal Amerikaanse) diensten zijn dus ook niet verplicht mee te werken aan een Nederlands bevel tot inzet van de bijzondere opsporingsbevoegdheid van een telecommunicatietap (Oerlemans, 2012).[98]

Overigens kan het tappen van telecommunicatie ondanks het probleem van versleuteling voor opsporingsinstanties alsnog nuttige informatie opleveren. Hoewel de inhoud van gegevens niet kan worden uitgelezen, kunnen wel de zogenoemde metagegevens (ook wel: verkeersgegevens) worden geanalyseerd zoals welke nummers met elkaar op welk tijdstip bellen en vanaf welke locatie.

In het gemoderniseerde Wetboek van Strafvordering kan op grond van artikel 2.8.13 Sv het tapbevel worden gegeven voor ten hoogste acht weken, waarbij telkens een verlenging met twee maanden mogelijk is.[99] Net zoals in de huidige bepaling is bij het gemoderniseerde wetsvoorstel een machtiging van de rechter-commissaris vereist voor de toepassing van de tapbevoegdheid. De aanbieder van telecommunicatie is verplicht niet slechts de inhoud van het communicatieverkeer te verstrekken, maar ook de verkeersgegevens af te geven. Nieuw is daarnaast de betredingsbevoegdheid in de situatie waarin telecommunicatie wordt opgenomen zonder medewerking van de aanbieder van telecommunicatie. In een dergelijke situatie kan de officier van justitie bepalen dat ter uitvoering van het vastleggen van telecommunicatie een besloten plaats of woning wordt betreden.

9.5.3 De hackbevoegdheid

De gedachten over de introductie van de hackbevoegdheid van de Nederlandse regering zijn terug te voeren op een Kamerbrief uit 2009. Daarin werd gezegd dat: 'het opsporen van cybercrime door anonimiseringstechnieken en encryptie "extreem gecompliceerd" is geworden'.[100]

98 Brief van de minister van Justitie en Veiligheid van 20 mei 2020, 2893215 (Rijksoverheid.nl).

99 *Kamerstukken II* 2022/23, 36327, nr. 3, p. 702-707.

100 Zie *Kamerstukken II* 2008/09, 28684, nr. 232, p. 2-3.

De hackbevoegdheid kan voor deze problematiek eventueel een oplossing bieden. Met de implementatie van de Wet computercriminaliteit III is op 1 maart 2019 de hackbevoegdheid als bijzondere opsporingsbevoegdheid geïntroduceerd. De bevoegdheid werd destijds noodzakelijk geacht als mogelijke oplossing voor de problemen van (1) anonimiteit, (2) versleuteling en (3) *cloud computing* in opsporingsonderzoeken (Oerlemans, 2017b).

Met de inzet van de hackbevoegdheid verschaffen opsporingsinstanties heimelijk en op afstand toegang tot een computer (het 'geautomatiseerde werk') waar de verdachte gebruik van maakt. Door 'op de bron' in te breken kunnen opsporingsambtenaren, doorgaans met behulp van software, communicatie onderscheppen en uitlezen, voordat de versleuteling in werking treedt. Met behulp van bijvoorbeeld een keylogger worden toetsaanslagen geregistreerd. Het is daarmee ook mogelijk ingevoerde inlognamen, wachtwoorden, URL's en e-mails te registreren. Met een andere functionaliteit kan een microfoon worden aangezet, waarmee bijvoorbeeld een gesprek kan worden afgeluisterd (Oerlemans, 2011). Net als de malware die criminelen gebruiken, heeft de software ook bepaalde functionaliteiten die van pas kunnen komen voor opsporingsinstanties, zoals het maken van screenshots (om te kijken wat op een computer van de verdachte staat), het aanzetten van een camera (ter identificatie van de computergebruiker) en het aanzetten van een GPS-functionaliteit (ter lokalisering van het apparaat).[101]

Tijdens het parlementaire debat richtte veel kritiek zich op het gebruik van kwetsbaarheden bij de toepassing van de bevoegdheid. Het idee is dat het hacken van apparaten met het gebruik van onbekende kwetsbaarheden (zogenoemde *zero-days*) meer onveiligheid dan veiligheid voor de maatschappij met zich brengt. De redenering is dat opsporingsautoriteiten een belang hebben bij het in stand houden van onbekende kwetsbaarheden in apparaten, waardoor apparaten onveilig blijven. Aangezien deze kwetsbaarheden niet bekend zijn bij de fabrikant van hardware of software, kan het beveiligingsprobleem niet worden opgelost. Deze onbekende kwetsbaarheden kunnen dus worden misbruikt door kwaadwillenden, totdat het beveiligingsprobleem wordt opgelost. Uiteindelijk heeft deze discussie geleid tot het aangenomen amendement 'Recourt/Telligen', waarbij een verplichting is geïntroduceerd om onbekende kwetsbaarheden te melden die bij de politie bekend zijn geworden bij toepassing van de hackbevoegdheid.[102] Slechts bij een zwaarwegend opsporingsbelang kan, na akkoord van het centraal aanspreekpunt bij het Landelijk Parket,

101 Zie ook *Kamerstukken II* 2015/16, 34372, nr. 3, p. 19-25.
102 *Kamerstukken II* 2016/17, 30372, nr. 14.

worden besloten een rechter-commissaris toestemming te vragen om de melding van de onbekende kwetsbaarheid uit te stellen (Koops & Oerlemans, 2019b).[103]

Uit een evaluatierapport van de hackbevoegdheid blijkt nu dat de hackbevoegdheid met name wordt ingezet bij mobiele telefoons die bij de verdachte in gebruik zijn. Het gaat daarbij vooral om opsporingsonderzoeken naar traditionele criminaliteit, zoals moord en doodslag (Van Uden et al., 2022). De hackbevoegdheid wordt ongeveer dertig keer per jaar ingezet en daarbij wordt met name gebruikgemaakt van commerciële hacksoftware (ook wel *spyware* genoemd). De Inspectie Justitie en Veiligheid houdt toezicht op de bevoegdheid en geeft bijvoorbeeld aan dat in 2022 in 25 zaken met commerciële software is gewerkt. De politie heeft geen inzicht in de werking hiervan. Voor zowel de politie als de Inspectie is deze software een *black box* (Inspectie, 2022). Het blijkt daarbij lastig aan procedurele regels te voldoen die zijn opgenomen in lagere regelgeving. Het Parket van de Hoge Raad rapporteerde op zijn beurt in 2022 (Procureur-Generaal bij de Hoge Raad der Nederlanden, 2022) dat 'de wijze waarop het Openbaar Ministerie ten aanzien van de onderzochte gevallen toepassing heeft gegeven aan de bevoegdheid tot het uitvoeren van onderzoek in een geautomatiseerd werk [...] grosso modo [voldoet] aan de wettelijke voorschriften. In beginsel is in de onderzochte zaken voldaan aan beginselen van proportionaliteit en subsidiariteit.' Er is nog nauwelijks jurisprudentie met bewijsoverwegingen over de inzet van de hackbevoegdheid en het gebruik van commerciële hacksoftware in opsporingsonderzoeken.

Voorwaarden voor de inzet

De hackbevoegdheid is geregeld in artikel 126nba Sv. Voor de inzet van deze bijzondere opsporingsbevoegdheid is een bevel van een officier van justitie, een machtiging van een rechter-commissaris en een verplicht advies van de CTC van het OM vereist. De hackbevoegdheid mag alleen worden ingezet in opsporingsonderzoeken naar misdrijven als omschreven in artikel 67 Sv en de artikelen die worden genoemd in het Besluit onderzoek in een geautomatiseerd werk, voor zover het onderzoek dat dringend vordert en het misdrijf een ernstige inbreuk op de rechtsorde oplevert.[104] In het bevel moet de officier

103 Zie artikel 126ffa Sv. Zie ook *Kamerstukken I* 2016/17, 34372, D, p. 20-21. De staatssecretaris geeft aan dat de politie geen onbekende kwetsbaarheden zal inkopen, maar hij sluit niet uit dat van onbekende kwetsbaarheden gebruik wordt gemaakt door de software die de politie aanschaft om de hackbevoegdheid uit te voeren.

104 *Stb.* 2018, 340.

van justitie aangeven welke functionaliteiten van de software noodzakelijk zijn om in te zetten om het doel te bereiken, en zich afvragen of de inzet daarvan proportioneel en subsidiair is.[105]

De hackbevoegdheid kan ook wel worden omschreven als een 'paraplubevoegdheid', omdat naast het heimelijk binnendringen ook andere bevoegdheden mogen worden ingezet (Oerlemans, 2011). Na het toegang verschaffen tot het geautomatiseerde werk mogen opsporingsinstanties de volgende vijf opsporingshandelingen uitvoeren:

1. de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of van de gebruiker, zoals de identiteit of locatie, en de vastlegging daarvan;
2. de uitvoering van een bevel tot stelselmatige observatie;
3. de uitvoering van een bevel tot het aftappen en opnemen van communicatie of opnemen van vertrouwelijke communicatie;
4. de vastlegging van gegevens die in het geautomatiseerde werk zijn of worden opgeslagen;
5. de ontoegankelijkheidsmaking van gegevens.[106]

In het gemoderniseerde Wetboek van Strafvordering is de hackbevoegdheid opgenomen in artikel 2.8.16 Sv. Afgezien van een wijziging van de geldigheidsduur (namelijk van vier weken naar acht weken) en de terminologie is de bepaling inhoudelijk grotendeels hetzelfde gebleven.[107]

9.6 Jurisdictie en grensoverschrijdende digitale opsporing

Jurisdictie verwijst naar de rechtsmacht van een staat of een ander regelgevend orgaan om wetten te maken, toe te passen en uit te voeren met betrekking tot het gedrag van personen, binnen de grenzen van het internationale recht (Mann, 1964; Shaw, 2008). Jurisdictie wordt gezien als het grootste probleem in opsporingsonderzoeken naar cybercriminaliteit (UNODC, 2013; Oerlemans, 2017a). Het zorgt ervoor dat in veel gevallen geen bewijs kan worden vergaard in het buitenland of dat de verdachte niet succesvol in Nederland kan worden vervolgd.

105 Zie artikel 126nba lid 2 sub d Sv.
106 Zie ook uitgebreid *Kamerstukken II* 2015/16, 34372, nr. 3, p. 21-31.
107 *Kamerstukken II* 2022/23, 36327, nr. 3, p. 715-717.

In deze paragraaf wordt het probleem van jurisdictie bij de bewijsgaring in opsporingsonderzoeken naar cybercriminaliteit nader toegelicht. Daarbij worden de kernbegrippen uitgelegd en wordt de problematiek geschetst bij de unilaterale toepassing van digitale opsporingsbevoegdheden. Ook worden enige internationale ontwikkelingen op een rijtje gezet die voor een gedeeltelijke oplossing moeten dienen voor het jurisdictieprobleem.

9.6.1 Wetgevende jurisdictie

Voordat er een opsporingsonderzoek wordt gestart, moeten opsporingsinstanties namens de staat rechtsmacht hebben, ook wel 'wetgevende jurisdictie' genoemd. De wetgevende jurisdictie van een staat wordt in beginsel bepaald door het 'territorialiteitsbeginsel'. Het territorialiteitsbeginsel houdt in dat een staat rechtsmacht kan aannemen over een element van een strafgedraging binnen het territorium van die staat. Het gaat dus over de vraag in hoeverre opsporingsinstanties van een staat een opsporingsonderzoek naar een strafbaar feit starten als bijvoorbeeld een strafbaar feit op het territorium van die staat door een dader van een andere staat wordt gepleegd.

Bij opsporingsonderzoeken naar computercriminaliteit is het (ondanks dat cybercriminaliteit grensoverschrijdend is) doorgaans niet problematisch om rechtsmacht aan te nemen op grond van het territorialiteitsbeginsel, omdat (eenvoudig gesteld) schade op het territorium door een delict ofwel het gebruik van een computer op het territorium van een staat voor het plegen van een computermisdrijf al voldoende kan zijn om rechtsmacht aan te nemen in cybercriminaliteitszaken, ongeacht de locatie waar het delict wordt gepleegd (Oerlemans, 2019a; Van der Net, 2000). Daarnaast zijn er nog diverse andere gronden om jurisdictie aan te nemen in cybercriminaliteitszaken (zie verder Oerlemans, 2019a).

9.6.2 Handhavingsjurisdictie en rechtshulp

Veel problematischer dan de wetgevende jurisdictie is de handhavingsjurisdictie, oftewel de jurisdictie om overheidsmacht uit te oefenen in opsporingsonderzoeken naar cybercriminaliteit. Hoe een staat zijn opsporing reguleert en (organisatorisch) inricht, valt onder de soevereiniteit van een staat. Opsporing is een exclusieve taak van een staat (Schmitt, 2017). Dit vormt de achtergrond waarom het niet is toegestaan om in het buitenland opsporingshandelingen te verrichten. Handhavingsjurisdictie is met andere woorden

'territoriaal beperkt'.[108] Op dit principe gelden twee uitzonderingen, namelijk (1) dat opsporing op buitenlands territorium mag plaatsvinden met toestemming van de betrokken staat of (2) als voor de grensoverschrijdende inzet een verdragsbasis bestaat.

Via het klassieke systeem van rechtshulp kunnen staten elkaar formeel verzoeken bewijs te vergaren. Een staat kan verzoeken dat de buitenlandse lokale opsporingsinstanties de opsporingshandeling uitvoeren, maar kan ook verzoeken de opsporingshandeling in het buitenland zelf uit te voeren (wat veel minder vaak voorkomt). Deze afspraken kunnen telkens eenmalig zijn (een ad-hocverzoek) of structureel in (rechtshulp)verdragen worden vastgelegd. Nederland kent heel veel bilaterale en multilaterale verdragen waarin grensoverschrijdende bewijsgaringsactiviteiten zijn geregeld (Koers, 2001). Ook bestaan er op Europees niveau belangrijke rechtshulpverdragen voor de opsporingspraktijk.[109]

Op het gebied van cybercriminaliteit is het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (het Cybercrimeverdrag) om drie redenen belangrijk.[110] Ten eerste harmoniseert het Cybercrimeverdrag belangrijke strafbaarstellingen zoals computervredebreuk, ddos-aanvallen, het bezitten, vervaardigen en verspreiden van malware en (virtuele) kinderpornografie. Ten tweede verplicht het verdrag tot het implementeren van opsporingsbevoegdheden in nationale wetgeving met betrekking tot het vorderen en veiligstellen van gegevens. Gezien het belang van de mogelijkheid een IP-adres te traceren en vervolgens gebruikersgegevens en verkeersgegevens te vorderen bij online service providers, is het noodzakelijk dat

108 Dit principe uit het internationaal recht is bevestigd in de belangrijke zaak *SS Lotus* (*Frankijk t. Turkije*) (1927), *PCIJ Reports*, Series A, nr. 10, p. 18-19: 'The first and foremost restriction imposed by international law upon a State is that - failing existence of a permissive rule to the contrary - it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention.'

109 Zie bijvoorbeeld Richtlijn 2014/41/EU van het Europees Parlement en de Raad van 3 april 2014 betreffende het Europees onderzoeksbevel in strafzaken, *Publicatieblad van de Europese Unie* 2014, L 130/1, geïmplementeerd op 17 mei 2017, *Stb.* 2017, 23 en Overeenkomst, door de Raad vastgesteld overeenkomstig artikel 34 van het Verdrag betreffende de Europese Unie, betreffende de wederzijdse rechtshulp in strafzaken tussen de lidstaten van de Europese Unie, *Publicatieblad van de Europese Unie* 2000, C 197/3.

110 Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (*Trb.* 2002, 18).

staten in hun nationale wetgeving in deze mogelijkheid voorzien. Ten derde draagt het verdrag bij aan de mogelijkheid tot een snelle bewijsgaring met behulp van rechtshulp. Het verdrag schrijft voor dat elke verdragsstaat een contactpunt creëert voor rechtshulpverzoeken in cyberzaken, dat 24 uur per dag, zeven dagen in de week beschikbaar moet zijn (Kaspersen, 2007).

Het kernprobleem is echter dat het systeem van rechtshulp in cyberonderzoeken niet altijd werkt of te traag is (zie o.a. Koops & Goodwin, 2014; Oerlemans, 2019a; UNODC, 2013).[111] Als een staat niet bereid is om mee te werken aan een rechtshulpverzoek om bewijs te verzamelen, kunnen opsporingsinstanties van de onderzoekende staat simpelweg met lege handen komen te staan (Stigall, 2013).

Tegen deze achtergrond is jarenlang gewerkt aan nieuwe internationale afspraken. Dit leidde op 17 november 2021 tot de goedkeuring van het Tweede Aanvullend Protocol bij het Cybercrimeverdrag. Deze aanvulling op het verdrag voorziet in een aantal instrumenten die de justitiële samenwerking en toegang tot elektronische gegevens moeten vergemakkelijken.[112] Zo wordt er een juridische basis gecreëerd voor rechtstreekse bevragingen van domeinnaaminformatie bij aanbieders van domeinnaamregistratiediensten.[113] Daarnaast wordt in artikel 7 de juridische basis gecreëerd voor de rechtstreekse bevraging van gebruikersgegevens bij dienstaanbieders. Dit vormt een afwijking van het traditionele principe in het internationaal recht waarbij *staten* beslissen of zij opsporingshandelingen binnen hun territorium goedkeuren, in plaats van bedrijven. De nieuwe regelingen kunnen bijdragen aan strafrechtelijke onderzoeken door het versnellen en eenvoudiger maken van de identificatie van internetgebruikers op basis van kenmerken uit elektronische communicatie, zoals een IP-adres, of het lokaliseren van internetgebruikers of geautomatiseerde werken op basis van internetverkeersgegevens (Van der Ham, 2024).

Bijna tegelijkertijd heeft de Europese Commissie wetgeving gemaakt over het verkrijgen van gegevens van internetdienstverleners (ISP's) in strafzaken (het *e-evidence*-pakket genoemd) (Boonstra, 2023). De regeling werd noodzakelijk geacht, omdat elektronische dienstverleners te maken hebben met een gefragmenteerd stelsel van regelingen voor het vorderen van gegevens en het vergaren van deze vorm van digitaal bewijs van elektronische dienstverleners

111 Zie ook *Kamerstukken II* 2015/16, 34372, nr. 3, p. 49.

112 Nederland heeft het protocol op 12 mei 2022 ondertekend.

113 Artikel 6 van het Tweede Aanvullend Protocol bij het Cybercrimeverdrag.

volgens het huidige stelsel van rechtshulp – waaronder het Europees onderzoeksbevel – (te) veel tijd kost (Ligeti & Robinson, 2021). De nieuwe regelgeving moet opsporingsinstanties de instrumenten geven direct vorderingen voor openbaarmaking of bewaring van gebruikersgegevens, verkeersgegevens en inhoudelijke gegevens te sturen naar elektronische dienstverleners (in plaats van naar centrale rechtshulpinstellingen van staten) (Tosza, 2024). In 2023 hebben het Europees Parlement en de Raad van Ministers ingestemd met de richtlijn en verordening.[114] Naar verwachting duurt het nog enkele jaren voordat de wetgeving naar aanleiding van het Tweede Aanvullend Protocol bij het Cybercrimeverdrag en de Europese wetgeving in Nederland zijn geïmplementeerd (Van der Ham, 2024). Toch is het belangrijk deze wetgeving kort te bespreken.

De regeling is van toepassing op elektronische dienstverleners die een of meer ondernemingen binnen de Europese Unie hebben of als er een 'substantiële connectie met de Europese Unie' bestaat, bijvoorbeeld vanwege substantieel veel klanten in lidstaten of het specifiek richten van activiteiten richting bewoners van EU-lidstaten. Als niet wordt voldaan aan de 'productiebevelen', staat daarop een boete van maximaal 2% van hun jaaromzet.[115] Elektronische dienstverleners kunnen zich tegen vorderingen verzetten als daar een grondslag voor is in hun eigen wetgeving, op grond van weigeringsgronden die zijn opgenomen in de verordening.[116] De voorgestelde regeling bevat ook enkele waarborgen ter bescherming van de persoonlijke levenssfeer. De belangrijkste daarvan is dat verkeers- en inhoudsgegevens slechts opgevraagd mogen worden voor strafbare feiten waarop in het uitvaardigende land een maximumvrijheidsstraf van ten minste drie jaar staat of voor specifieke cyber- en terrorismegerelateerde strafbare feiten (Van der Ham, 2024).[117] Ook bestaat er een notificatiemechanisme bij de verstrekking van verkeers- en inhoudelijke gegevens.

114 Richtlijn (EU) 2023/1544 van het Europees Parlement en de Raad van 12 juli 2023 tot vaststelling van geharmoniseerde regels inzake de aanwijzing van aangewezen vestigingen en de aanstelling van wettelijke vertegenwoordigers ten behoeve van de vergaring van elektronisch bewijsmateriaal in strafprocedures, *Publicatieblad van de Europese Unie* 2023, L 191/181. Verordening (EU) 2023/1543 van het Europees Parlement en de Raad van 12 juli 2023 betreffende het Europees verstrekkingsbevel en het Europees bewaringsbevel voor elektronisch bewijsmateriaal in strafzaken en de tenuitvoerlegging van vrijheidsstraffen als gevolg van een strafprocedure, *Publicatieblad van de Europese Unie* 2023, L 191/118.

115 Artikel 15 lid 1 Verordening (EU) 2023/1543.

116 Artikel 12 Verordening (EU) 2023/1543.

117 Artikel 5 lid 4 en overweging 40 en 41 Verordening (EU) 2023/1543.

Het belangrijkste kritiekpunt van deze regeling is dat de verantwoordelijkheid voor de bescherming van fundamentele rechten nu grotendeels wordt gelegd bij de internet service provider en de autoriteit die het bevel uitvaardigt. De vraag is of zij zich voldoende geroepen voelen de rechten van de betrokken individuen te verdedigen, zeker als het de inwoners van een ander land betreffen. De verwachting is dat de internetdienstverleners vooral reageren als het bevel tot verstrekking van gegevens incompleet en onvoldoende duidelijk is (Tosza, 2024).

9.6.3 Unilaterale digitale opsporing

Bij unilaterale digitale opsporing worden opsporingsmethoden toegepast zonder toepassing van het systeem van rechtshulp of een specifieke verdragsbasis. Dat is internationaalrechtelijk niet toegestaan, maar toch vindt unilaterale digitale opsporing in de praktijk plaats, omdat het internet praktisch gezien geen territoriale beperkingen kent en opsporingsinstanties niet met lege handen willen blijven.

Elk van de opsporingsmethoden die in dit hoofdstuk zijn beschreven, kunnen unilateraal worden ingezet en krijgen daarmee een 'extraterritoriaal karakter'. Dan doet zich het probleem van de territoriale beperking van handhavingsjurisdictie in verschillende mate voor. Denk daarbij bijvoorbeeld aan online undercoveroperaties, waarbij onder dekmantel bijvoorbeeld in de Engelse taal wordt gecommuniceerd met een verdachte met een bepaalde nickname. Vindt op dat moment opsporing in het buitenland plaats? En zo ja, in welk land? Moet de betrokken staat in kennis worden gesteld van de opsporingshandeling? Dit probleem en deze vragen worden aan de hand van een casus geïllustreerd.

Casus: David S.

De Amerikaanse 'Secret Service' verdacht de Nederlandse David S. van creditcardfraude.[118] In het kader van het opsporingsonderzoek heeft de Secret Service via het account van een andere verdachte met David S. gecommuniceerd.[119] Ook hebben Secret Service-agenten creditcards

118 *United States v. David Schrooten*, Case No. CR12-85-RSM, W.D. Washington, 11 juni 2012.

119 H. Lensink & F. Vuijst, 'Geen krediet voor David S.', *Vrij Nederland*, 15 april 2013.

gekocht van David S., die op internet actief was onder de nickname 'Fortezza' (Schrooten & Vuijst, 2016). Fortezza bood gestolen creditcards aan op online handelsplaatsen en heeft vermoedelijk ook andere marktplaatsen gehackt om creditcardgegevens te bemachtigen. Dit leidde onder andere tot een tegenreactie waarbij – door vermoedelijk Russische cybercriminelen – onder andere de naam en school waar David S. naartoe ging, bekend werd gemaakt ('doxing').[120]

Op een zeker moment vloog David S. naar zijn Roemeense vrienden. Hij werd op het vliegveld in Roemenië gearresteerd en direct uitgeleverd aan de Verenigde Staten. Hij bekende, maakte een deal met de Amerikaanse autoriteiten en werd veroordeeld.[121] Na een tijd in Amerikaanse gevangenissen te hebben doorgebracht, heeft hij succesvol een beroep kunnen doen op een procedure waarbij hij zijn straf mocht uitzitten in Nederland.[122] Een paar weken na de gevangenisstraf in Nederland werd hij weer vrijgelaten.

De zaak leidde tot een smeekbede van David voor een terugkeer naar Nederland, maar ook tot Kamervragen en consternatie in de Nederlandse politiek.[123] Kamerleden vroegen zich af of Amerikaanse opsporingsinstanties zonder toestemming opsporingshandelingen in Nederland hadden uitgevoerd. De minister antwoordde dat er géén opsporingshandelingen in Nederland waren uitgevoerd en heeft zich ingespannen om David S. terug te krijgen naar Nederland om hier zijn straf uit te zitten.[124]

120 B. Krebs, 'Feds Arrest "Kurupt" Carding Kingpin?', *Krebson security blog*, 12 juni 2012.

121 Persbericht U.S. Department of Justice, 'Dutch Citizen Sentenced to 12 Years in Prison for Computer Hacking Scheme that Stole and Sold Credit Card Info', 1 februari 2013.

122 H. Lensink, 'Minister wil terugkeer hacker David S. bespoedigen', *Vrij Nederland*, 15 april 2013.

123 Zie antwoorden op Kamervragen over de uitlevering van een Nederlandse hacker aan de Verenigde Staten door Roemenië van 1 augustus 2012, *Aanhangsel Handelingen II* 2011/12, nr. 3028.

124 Beantwoording Kamervragen over het bericht 'FBI-agenten hacken mee met Nederlandse politie' en de detentieomstandigheden van de betrokkene in de VS van 16 april 2013, *Aanhangsel Handelingen II* 2012/13, nr. 2001.

Toch kan het niet anders dan dat er opsporingshandelingen in Nederland zijn uitgevoerd door Amerikaanse opsporingsinstanties, vanwege de stelselmatige informatie-inwinning en de pseudokoop die in dit opsporingsonderzoek hebben plaatsgevonden (Oerlemans, 2017a). Het is echter onduidelijk of de Amerikanen wisten dat de persoon achter de nickname 'Fortezza' in Nederland woonde. Op basis van het onderzoek in publiek toegankelijke bronnen en een geldopname bij Western Union in Den Haag was lokalisering van de verdachte in theorie goed mogelijk (Schrooten & Vuijst, 2016).

Bovenstaande zaak maakt duidelijk dat extraterritoriale opsporing twee effecten kan hebben, namelijk: 1) het maakt mogelijk een inbreuk op de territoriale soevereiniteit van een staat en 2) het bedreigt de rechtszekerheid van de verdachten in een opsporingsonderzoek.

Voor de grensoverschrijdende inzet van de hackbevoegdheid is een speciale regeling gemaakt, waarbij onder bepaalde omstandigheden de bijzondere opsporingsbevoegdheid buiten het Nederlands territorium mag worden ingezet. In de Aanwijzing staat dat als met een redelijke inspanning niet kan worden vastgesteld wat de locatie van geautomatiseerd verwerkte gegevens is, wordt gehandeld alsof de gegevens in Nederland zijn opgeslagen.[125] Daarvan kan blijkens de aanwijzing ook sprake zijn als niet langer kan worden gewacht op een reactie of er geen reactie van het land is te verwachten op een rechtshulpverzoek. Ook kan hiervan bijvoorbeeld sprake zijn bij het gebruik van anonimiseringssoftware of opslag van gegevens in de cloud. Het criterium van de 'redelijke inspanning' wordt in de Aanwijzing omschreven als: 'de tijd en moeite voor het vaststellen van een specifieke geografische locatie in een reële verhouding tot de noodzakelijkheid van "onverwijld" optreden, de tijdsdruk en de doorlooptijd van het onderzoek'. Het is denkbaar dat deze norm in de praktijk ook wordt gebruik in de toepassing van andere digitale opsporingsbevoegdheden.[126]

Afhankelijk van de indringendheid van de opsporingsmethode die plaatsvindt of de gevolgen daarvan, kan grensoverschrijdende digitale opsporing tot poli-

125 Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv, *Stcrt.* 2019, 10277.

126 Zie voor een vergelijkbaar gebruik van het criterium: Rb. Rotterdam 22 februari 2019, ECLI:NL:RBROT:2019:2712.

tieke en diplomatieke spanningen leiden (Oerlemans, 2017a). Het valt buiten het bestek van dit boek om de mogelijke extraterritoriale effecten van alle digitale opsporingsmethoden en betrokken regels te bespreken.[127] Wel is het belangrijk om zich bewust te zijn dat wat technisch kan (unilateraal digitaal opsporen), niet altijd juridisch is toegestaan, ethisch wenselijk is of verstandig is vanuit politiek of diplomatiek perspectief.

9.7 Verstoring en de brede bestrijding van cybercriminaliteit

Aangezien de klassieke opsporing[128] en vervolging van verdachten vaak complex is door de uitdagingen van anonimiteit, versleuteling en jurisdictie, komt het niet altijd – of zelfs vaak niet – tot een succesvolle opsporing en vervolging van verdachten van cybercriminaliteit (Ruiter et al., 2023; Van den Eeden et al., 2021; Van der Wagen et al., 2019).

Waar het opsporen en/of vervolgen van cybercriminelen niet haalbaar is of onvoldoende effectief blijkt, is *verstoring* van criminele processen een alternatieve of aanvullende methode om schade voor burgers en bedrijven te beperken. Deze aanpak richt zich bijvoorbeeld op de criminele verdienmodellen die achter de verschillende vormen van cybercriminaliteit schuilgaan (Van den Eeden et al., 2021).[129] Het wordt ook wel de 'brede bestrijding' van cybercriminaliteit genoemd, omdat het – naast opsporing – ook ziet op het tegenhouden van daders, het stoppen van het strafbare feit of het anderszins beschermen van de belangen van slachtoffers (Bonnes & Divendal, 2024). Met verstoring worden concrete drempels opgeworpen in het crime script van daders, zoals deze naar voren kwamen in hoofdstuk 3 en 4.

In dit boek zijn al verschillende voorbeelden van deze bestrijdingsstrategieën en interventies voorbijgekomen. Denk bijvoorbeeld aan het verwijderen van strafbaar materiaal, het waarschuwen van deelnemers aan een cybercriminele chatgroep voor de strafbaarheid van hun handelen door middel van het plaatsen van een bericht of een *knock-and-talk*-actie of door middel van gerichte

127 Zie Oerlemans (2019a) voor een uitgebreide bespreking over de (on)mogelijkheden van grensoverschrijdende digitale opsporing.

128 Met klassieke opsporing bedoelen we het ophelderen van een gepleegd strafbaar feit, het identificeren van de verdachte, en het bewijs vergaren tegen de verdachte met het oog op het nemen van een vervolgingsbeslissing.

129 Zie o.a. de brief van de minister van Justitie en Veiligheid van 4 november 2022, 4268124 (Rijksoverheid.nl).

advertenties aan de doelgroep, het onklaar maken van een cybercriminele infrastructuur, en het informeren van slachtoffers via een webpagina zoals 'politie.nl/checkjehack'.

Vanuit juridisch perspectief is het onduidelijk in hoeverre bijzondere opsporingsbevoegdheden mogen worden ingezet als niet de vervolging voor het strafbare feit het doel is, maar het beëindigen van een strafbaar feit en andere vormen van preventie. Ook in de wetsvoorstellen voor de modernisering van het Wetboek van Strafvordering wordt geen melding gemaakt van een 'brede bestrijding' van cybercriminaliteit, maar er staat wel dat 'het nemen van strafvorderlijke beslissingen kan inhouden dat strafbare feiten worden gestopt'.[130] Hirsch Ballin en Oerlemans (2023) stellen dat deze acties in het kader van een brede bestrijding van cybercriminaliteit mogelijk zijn, maar alleen naast het doel van de klassieke opsporing.

Het probleem is onder meer dat politieoperaties die een brede bestrijding van cybercriminaliteit nastreven niet altijd tot strafzaken in Nederland leiden, waarbij een zittingsrechter de rechtmatigheid van de naleving van het Wetboek van Strafvordering toetst (Bonnes & Divendal, 2024; Oerlemans & Van Wegberg, 2019; Procureur-Generaal bij de Hoge Raad der Nederlanden, 2022; Van den Eeden et al., 2021). Dat vormt ook een toezichtsprobleem of 'toezichtshiaat' op de naleving van wet- en regelgeving, waaronder ook de Wet politiegegevens (Fedorova et al., 2022; Hirsch Ballin & Oerlemans, 2023; Schermer, 2022; Schermer & Galiç, 2022; Stevens, 2021).

Bovengenoemde auteurs doen om deze reden het voorstel tot (onderzoek naar) het instellen van een andere onafhankelijke instantie dan de strafrechter voor effectiever toezicht. Bonnes & Divendal (2024) stellen voor de mogelijkheid tot brede bestrijding van cybercriminaliteit expliciet te regelen in het Wetboek van Strafvordering, zodat dit duidelijkheid schept, evenals de mogelijkheid om de gegevens die worden verzameld in een opsporingsonderzoek ook voor andere doelen dan opsporing te verwerken. Deze suggesties hebben tot nog toe niet tot wetsvoorstellen van de wetgever geleid en zijn zoals opgemerkt geen onderdeel van de modernisering van het Wetboek van Strafvordering.

130 *Kamerstukken II* 2022/23, 36327, nr. 3, p. 95.

9.8 Tot besluit

In dit hoofdstuk zijn digitale opsporingsmethoden besproken aan de hand van de uitdagingen van anonimiteit, versleuteling en jurisdictie in cybercriminaliteitszaken. Daarbij zijn telkens voorgenomen wetswijzigingen naar aanleiding van de modernisering van het Wetboek van Strafvordering genoemd.

Volgens Schermer (2022) lossen we met deze aanpak van cybercriminaliteit echter 'de problemen uit 2017 op' en zijn ook wijzigingen voor de Wet politiegegevens noodzakelijk om het recht op privacy beter te beschermen.[131] Ook hebben we in de voorgaande paragraaf gesignaleerd dat verstoring en de 'brede aanpak van cybercriminaliteit' leiden tot juridische vragen en op risico's met betrekking tot de naleving van de Wet politiegegevens. Wij nodigen ook studenten en professionals uit om kritisch te reflecteren op de huidige wet- en regelgeving met het oog gericht op de praktijk.

Daarnaast blijkt uit onderzoek dat training en het algemene kennisniveau over digitale opsporing en cybercriminaliteit bij de politie moet worden verbeterd (Boekhoorn, 2020; Ruiter et al., 2023). Wetswijzingen leiden op zichzelf niet altijd tot de nodige verbetering, daarvoor zijn ook culturele en organisatorische veranderingen noodzakelijk. Het potentieel van digitale opsporing lijkt ook niet volledig benut; in elke strafzaak zal mogelijk digitaal bewijs te vinden zijn. Daarbij blijft de digitale opsporingspraktijk voortdurend in beweging, waarbij mede wordt ingespeeld op de technologische ontwikkelingen die ons leven ingrijpend veranderen.

In de toekomst worden bepaalde problemen in opsporingsonderzoeken naar cybercriminaliteit opgelost en treden andere problemen weer op de voorgrond. Multidisciplinair onderzoek kan eraan bijdragen hier zicht op te houden en de noodzaak van juridische, technische of organisatorische veranderingen aan te tonen.

131 A. van Soest, interview met hoogleraar Bart Schermer: 'Met de huidige aanpak van cybercrime lossen we de problemen uit 2017 op', *FTM.nl*, podcast, 29 januari 2023.

9.9 Discussievragen

1. In hoeverre zijn de genoemde digitale opsporingsmethoden in opsporingsonderzoeken naar cybercriminaliteit ook relevant voor conventionele strafzaken?
2. Wat vindt u van de stelling: 'In elk opsporingsonderzoek naar een ernstig misdrijf is digitaal forensisch onderzoek noodzakelijk'?
3. Stel dat u een inschatting moet maken van het percentage opsporingsonderzoeken naar cybercriminaliteit dat succesvol is in de zin van een strafoplegging of uitspraak. Wat zou dan uw inschatting zijn na het lezen van dit hoofdstuk?
4. In Nederland wordt een driedeling gemaakt bij het waarderen van de privacy-inbreuk bij het onderzoek van gegevens op inbeslaggenomen gegevensdragers. Wat vindt u van deze driedeling?
5. Wat zijn de voor- en nadelen van een bijzondere opsporingsbevoegdheid voor onderzoek in publiek toegankelijke bronnen?
6. Zijn locatiegegevens altijd privacygevoelig? Of alleen als deze langere tijd over een individu worden vastgelegd?
7. In hoeverre is een machtiging van een rechter-commissaris bij undercoveroperaties noodzakelijk?
8. Wanneer moeten Amerikaanse socialemediadiensten meewerken aan een bevel tot het verstrekken van gegevens van Nederlandse opsporingsinstanties?
9. Hebben personen die met 'cryptotelefoons' communiceren een minder grote verwachting van privacy dan personen die met reguliere mobiele telefoons communiceren?
10. Gaan de voorstellen uit de modernisering van het Wetboek van Strafvordering ver genoeg?
11. Wat vindt u van de stelling: 'Bij opsporing op internet is de territoriale beperking van het opsporingsonderzoek niet meer van toepassing'?
12. Moet het ook mogelijk zijn bijzondere opsporingsbevoegdheden in te zetten met het enige doel om te verstoren of slachtoffers van cybercriminaliteit te helpen?

9.10 Kernbegrippen

- Anonimiteit
- Bijzondere opsporingsbevoegdheden
- Brede bestrijding van cybercriminaliteit

- Datagedreven opsporing
- Digitaal bewijs
- Digitale opsporing
- Hackbevoegdheid
- Inbeslagname van gegevensdragers
- Infiltratie
- Jurisdictie
- (Onbekende) kwetsbaarheid
- Onderzoek in publiek toegankelijke bronnen
- Ontsleutelingsbevel
- Netwerkzoeking
- Privacy
- Spyware
- Stelselmatigheid
- Strafvorderlijk legaliteitsbeginsel
- Undercoverbevoegdheden
- Versleuteling
- Verstoren van cybercriminaliteit