Facebookvrienden worden met de verdachte

Over undercoverbevoegdheden op internet

Jan-Jaap Oerlemans*

Online undercoverbevoegdheden bieden de mogelijkheid onder dekmantel bewijs te verzamelen op internet. De anonimiteit en (potentieel) grensoverschrijdende toepassing bieden vanuit opsporingsperspectief belangrijke voordelen. Opsporingsambtenaren kunnen bijvoorbeeld onder dekmantel chatten met een verdachte of zichzelf toevoegen als 'vriend' aan het Facebookaccount van de verdachte.
Voor de toepassing van undercoveropsporingsbevoegdheden bestaat een gedetailleerd juridisch kader vanwege de Wet bijzondere opsporingsbevoegdheden (Wet BOB).[1] Deze wet is een nasleep van de IRT-affaire en bestaat onder andere ter regulering van controversiële undercover opsporingsmethoden, die eind jaren tachtig en negentig intensiever werden gebruikt ter bestrijding van de georganiseerde drugscriminaliteit (Commissie-Van Traa 1996).[2]
Met de Wet BOB zijn de volgende drie bijzondere opsporingsbevoegdheden met betrekking tot undercoveropsporingsmethoden in het Wetboek van Strafvordering (Sv) geïntroduceerd:
1. pseudokoop en pseudodienstverlening;
2. stelselmatige informatie-inwinning;
3. infiltratie.

Voor de toepassing van deze bijzondere opsporingsbevoegdheden in een online context is het van belang dat in de wetsgeschiedenis al in 1999 is opgemerkt dat opsporingsbevoegdheden, zoals observatie en infiltratie, onder gelijke voorwaarden in de digitale wereld kunnen

* Mr. dr. J.J. Oerlemans is als onderzoeker verbonden aan eLaw, het Centrum voor Recht en Digitale Technologie van de Universiteit Leiden.
1 *Stb.* 1999, 245.
2 De Wet BOB is gebaseerd op de aanbevelingen van de commissie-Van Traa.

doi: 10.5553/JV/016758502018044005007

worden toegepast.[3] De reikwijdte van undercoveropsporingsbevoegdheden is binnen een online context echter niet altijd duidelijk. De memorie van toelichting reflecteert heel summier op de concrete toepassing van de bijzondere opsporingsbevoegdheden in de 'digitale wereld', waarbij de context waarbinnen deze bevoegdheden worden ingezet snel verandert. In 1999 kon de wetgever bijvoorbeeld de ontwikkeling van sociale media nog niet overzien. Daarbij kan het onduidelijk zijn of het bestaand juridisch kader nieuwe toepassingen van bijzondere opsporingsbevoegdheden in een online context nog 'dekt'. De vraag is bijvoorbeeld in hoeverre de 'accountovername' als undercoveropsporingsmethode mag worden ingezet.
In dit artikel worden de mogelijkheden van online undercoveropsporingsbevoegdheden in kaart gebracht, aan de hand van de wet, literatuur en actuele jurisprudentie.[4] Het artikel is opgehangen aan de bespreking van de drie bijzondere opsporingsbevoegdheden van pseudokoop, stelselmatige informatie-inwinning en infiltratie in een online context. De tussenconclusie geeft antwoord op de vraag welke meerwaarde deze online undercoverbevoegdheden bieden voor de opsporing. Het artikel sluit af met een bespreking van het jurisdictievraagstuk bij de toepassing van online undercoverbevoegdheden, omdat er spanning bestaat tussen de praktische mogelijkheid grensoverschrijdend via internet op te sporen, terwijl het internationaal recht dit slechts onder strikte voorwaarden toelaat.

Pseudokoop

De bijzondere opsporingsbevoegdheid van een pseudokoop kan ook plaatsvinden op internet, zoals een online marktplaats, waarbij een undercoveragent de aankoop doet van een goed (zoals drugs of wapens) of gegeven[5] (zoals gestolen persoonsgegevens). De online

3 Zie *Kamerstukken II* 1998/99, 26671, 3, p. 36. Zie ook Siemerink 2000b.
4 Dit artikel bouwt voort op de resultaten van mijn proefschrift (Oerlemans 2017). Ter beperking van de omvang van het artikel wordt slechts de politiële inzet van de bijzondere opsporingsbevoegdheden besproken. Voor de inzet van burgers zijn andere bijzondere opsporingsbevoegdheden onder grotendeels gelijke voorwaarden van toepassing, maar gelden aanvullende specifieke regels op basis van de Aanwijzing opsporingsbevoegdheden (*Stcrt.* 2014, 24442). Dit artikel concentreert zich op de relevante bepalingen in het Sv en de reikwijdte van deze bevoegdheden in een online context.
5 Sinds 2006 kunnen door de bekrachtiging van de Wet computercriminaliteit II ook *gegevens* worden gekocht bij een pseudokoop, in plaats van alleen goederen. Zie *Kamerstukken II* 1998/99, 26671, 3, p. 36-37.

doi: 10.5553/JV/016758502018044005007

pseudokoop wordt in de strafrechtpraktijk veelvuldig toegepast (Kruisbergen & De Jong 2010, p. 216).[6] Gepubliceerde uitspraken laten bijvoorbeeld zien dat de bijzondere opsporingsbevoegdheid in artikel 126i Sv wordt toegepast voor de aankoop van drugs, vuurwapens, vuurwerk en gestolen goederen op Marktplaats.nl en van ivoor van bedreigde diersoorten via internet.[7]

De online pseudokoop biedt opsporingsautoriteiten de mogelijkheid na te gaan wie het pakketje met het goed of de gegevens verzendt en waar het wordt afgeleverd. Als de verdachte de verzending van het pakketje zelf heeft verzorgd, dan geeft hij of zij mogelijk identificerende gegevens vrij. Een pakketje met drugs kan bijvoorbeeld vingerafdrukken bevatten of DNA-materiaal (via een postzegel), op basis waarvan verder onderzoek kan plaatsvinden. Bij de aankoop van goederen of gegevens via internet gaat soms online communicatie vooraf. Tijdens deze communicatie is het wellicht mogelijk identificerende gegevens van een verdachte te achterhalen, zoals een naam, telefoonnummer en/of e-mailadres. Deze gegevens bieden mogelijkheden voor andere opsporingshandelingen, zoals het vorderen van gegevens bij aanbieders van communicatiediensten.

De opsporingsbevoegdheid van de pseudokoop mag worden toegepast nadat een bevel van een officier van justitie is afgegeven een goed of gegevens aan te kopen in opsporingsonderzoeken met betrekking tot misdrijven zoals omschreven in artikel 67 Sv. Hoewel een algemeen verbod tot uitlokking altijd al 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'.[8] Indien een persoon een vermoedelijk illegaal goed of gegevens op internet

6 De pseudoverkoop of -dienstverlening wordt – op basis van gepubliceerde uitspraken – in een online context bijna nooit toegepast (zie alleen Hof Amsterdam 31 mei 2013, ECLI:NL:GHAMS:2013:2090). Deze opsporingsmethode wordt daarom buiten beschouwing gelaten.

7 Zie bijv. Rb. Roermond 4 maart 2009, ECLI:NL:RBROE:2009:BH4757 (online pseudokoop van gestolen goederen op Marktplaats.nl), Rb. Zutphen 28 januari 2011, ECLI:NL:RBZUT:2011:BP2308 (online pseudokoop van illegale wapens), Rb. Oost-Brabant 6 mei 2013, ECLI:NL:RBOBR:2013:BZ9467 (online pseudokoop van illegaal vuurwerk), Rb. Rotterdam 8 mei 2014, ECLI:NL:RBROT:2014:3504 (online pseudokoop van drugs op Silk Road), Rb. Overijssel 18 april 2016, ECLI:NL:RBOVE:2016:1323 (online pseudokoop van ivoor van bedreigde diersoorten), Rb. Rotterdam 11 augustus 2017, ECLI:NL:RBROT:2017:6830 (aankoop vuurwapen op het 'dark web') en Rb. Den Haag 17 mei 2018, ECLI:NL:RBDHA:2018:5775 (online pseudoaankoop creditcardgegevens van LizardSquad-verdachte).

8 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, 18757/06, *EHRC* 2011/9, m.nt. Ölçer (*Bannikova t. Rusland*) over uitlokking in de context van art. 6 EVRM. Zie ook *Kamerstukken II* 1996/97, 25403, 3, p. 31.

doi: 10.5553/JV/016758502018044005007

aanbiedt en een opsporingsambtenaar koopt vervolgens het aangeboden goed of gegeven, dan zal van uitlokking niet snel sprake zijn. De opsporingshandelingen in undercoveroperaties moeten zorgvuldig worden geverbaliseerd, zodat ter zitting kan worden nagegaan of er sprake is van uitlokking en of het recht op een eerlijk proces van artikel 6 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) niet is geschonden.

Stelselmatige informatie-inwinning

Via internet kunnen opsporingsambtenaren onder dekmantel *interacteren* met een verdachte en personen in diens omgeving. Deze interacties vinden bijvoorbeeld plaats in de vorm van communicatie op chatkanalen, online discussie- of handelsfora of door 'vrienden' te worden met de verdachte (of diens vrienden) op sociale media.
De bijzondere opsporingsbevoegdheid van stelselmatige informatie-inwinning kan bij bovengenoemde voorbeelden van toepassing zijn. Het is voor de bevoegdheid kenmerkend dat een actieve interventie in het leven van de verdachte plaatsvindt; het gaat verder dan louter het (passief) observeren van gedrag van personen of zaken.[9] In cybercrimezaken is de undercoveropsporingsmethode bijzonder waardevol, omdat een *nickname* en andere '*online handle*', zoals een e-mailadres, belangrijke digitale sporen zijn op basis waarvan bewijs kan worden verzameld.[10]
De wetgever heeft bij de Wet BOB expliciet aangegeven dat stelselmatige informatie-inwinning ook op internet kan worden toegepast.[11] De toepassing van stelstelmatige informatie-inwinning in een online context is bijzonder interessant, omdat opsporingsambtenaren met dezelfde anonimiteit als andere internetgebruikers met betrokkenen in een opsporingsonderzoek kunnen interacteren. Ook is het – praktisch gezien – mogelijk grensoverschrijdend via internet op te treden (daarover meer in de laatste paragraaf over jurisdictie). In deze paragraaf worden de vier mogelijke toepassingen van de bevoegdheid van

9 Zie *Kamerstukken II* 1996/97, 25403, 3, p. 35.
10 Zie uitgebreid Oerlemans 2017, p. 30-36.
11 Zie *Kamerstukken II* 1996/97, 25403, 3, p. 34. Zie ook *Kamerstukken II* 1998/99, 26671, 3, p. 37.

doi: 10.5553/JV/016758502018044005007

stelselmatige informatie-inwinning besproken. Eerst wordt nog het juridisch kader kort uiteengezet.

Juridisch kader

De juridische basis voor de interactie met verdachten in een opsporingsonderzoek onder dekmantel is artikel 3 van de Politiewet 2012 of artikel 126j Sv als de opsporingsmethode door een opsporingsambtenaar wordt uitgevoerd. Artikel 3 Polw 2012 voldoet voor zover de opsporingsmethode niet op stelselmatige wijze wordt toegepast. Artikel 126j Sv vormt de basis voor de inzet van de bijzondere opsporingsbevoegdheid van 'stelselmatige informatie-inwinning'.
Er is sprake van stelselmatigheid als een 'min of meer volledig beeld van bepaalde aspecten van iemands privéleven' wordt verkregen.[12] Uit de memorie van toelichting kunnen vijf factoren worden afgeleid om te bepalen of een opsporingsmethode op *stelselmatige* wijze wordt toegepast. Dit zijn: (1) de duur, (2) de plaats, (3) de intensiteit, (4) de frequentie en (5) het gebruik van een technisch hulpmiddel.[13] Deze factoren lijken oorspronkelijk geformuleerd voor stelselmatige observatie en niet expliciet voor stelselmatige informatie-inwinning. Toch kan worden aangenomen dat deze factoren ook voor deze bijzondere opsporingsbevoegdheid zijn geformuleerd.[14] Welke grondslag ook wordt toegepast, het is van belang dat opsporingsinstanties de opsporingshandelingen voldoende vastleggen (mogelijk met behulp van software), zodat de verdediging en rechter kunnen nagaan of van stelselmatigheid sprake is en het uitlokkingsverbod niet wordt geschonden.
Voor de toepassing van de bijzondere opsporingsbevoegdheid is een bevel van een officier van justitie vereist. Artikel 126j Sv kan worden ingezet bij de opsporing van elk misdrijf voor een (verlengbare) periode van drie maanden. De inzet is daarmee niet beperkt tot opsporingsonderzoeken naar bepaalde delicten. In het kader van het project Modernisering Strafvordering zijn er plannen om de toepassing van de bijzondere opsporingsbevoegdheid te beperken tot mis-

12 Zie *Kamerstukken II* 1996/97, 25403, 3, p. 26-27.
13 Zie *Kamerstukken II* 1996/97, 25403, 3, p. 26-27 en *Kamerstukken II* 1998/99, 26671, 7, p. 46.
14 Zie ook Rb. Den Haag 10 december 2015, ECLI:NL:RBDHA:2015:14365, *Computerrecht* 2016/46, m.nt. J.J. Oerlemans en Hof Den Haag 25 mei 2018, ECLI:NL:GHDHA:2018:1248 (*Context*).

doi: 10.5553/JV/016758502018044005007

drijven met ten minste een maximale gevangenisstraf van een jaar.[15] De inzet van de bijzondere opsporingsbevoegdheid kan ingrijpend zijn voor de betrokkene in het opsporingsonderzoek, 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' door de undercoveragent (zie ook Kruisbergen & De Jong 2012, p. 51). Daarnaast bestaan er bij undercoveroperaties bepaalde risico's omtrent de integriteit van het onderzoek. Extra waarborgen zijn op hun plaats om bijvoorbeeld het risico te beperken dat een undercoveragent zich met criminele activiteiten bezighoudt die verder gaan dan oorspronkelijk met een officier van justitie zijn afgesproken. In mijn proefschrift heb ik zelfs de betrokkenheid van een rechter-commissaris bij de toepassing van stelselmatige informatie-inwinning aanbevolen, onder verwijzing naar jurisprudentie van het Straatsburgse Hof, dat ook de betrokkenheid van een rechter bij undercoverbevoegdheden prefereert (Oerlemans 2017, p. 241).[16]

Online communiceren met de verdachte

Opsporingsambtenaren kunnen met de inzet van de bijzondere opsporingsbevoegdheid van stelselmatige informatie-inwinning onder dekmantel communiceren met verdachten op bijvoorbeeld een chatkanaal, online forum of online marktplaats. Met behulp van anonimiseringstechnieken kan het IP-adres van de politieorganisatie worden verhuld en onder een nickname (pseudoniem) met dezelfde anonimiteit als andere internetgebruikers worden gecommuniceerd. Cybercriminelen communiceren bijvoorbeeld veel met elkaar in chatkanalen, via online forums of via chatprogramma's zoals Jabber. Opsporingsinstanties kunnen daar handig op inspelen. In de praktijk moet op grond van de Aanwijzing opsporingsbevoegdheden overigens in de meeste gevallen de unit 'Werken Onder Dekmantel' (WOD) worden ingezet. Uiteraard is ook bij deze afdeling voldoende kennis van de subcultuur op internet noodzakelijk om voldoende overtuigend over te komen (Siemerink 2000a, p. 145).

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

16 Zie bijv. EHRM 24 juni 2008, 74355/01 (*Milinienè/Litouwen*), EHRM 4 november 2010, 18757/06, *EHRC* 2011/9, m.nt. Ölçer (*Bannikova/Rusland*) en EHRM 23 oktober 2014, 54648/09, *EHRC* 2015/1, m.nt. F.P. Ölçer (*Furcht/Duitsland*).

doi: 10.5553/JV/016758502018044005007

De accountovername als opsporingsmethode

Een bijzonder interessante toepassing van de opsporingsmethode is de 'accountovername'. Uit jurisprudentie blijkt bijvoorbeeld dat Zwitserse opsporingsautoriteiten het account van een Zwitserse zedenverdachte hebben overgenomen.[17] De Zwitsers hebben daarmee vervolgens ingelogd op het peer-to-peerprogramma GigaTribe.[18] Via GigaTribe is contact gelegd met een Nederlandse GigaTribe-gebruiker en zijn via het programma bestanden met kinderpornografie uitgewisseld. Het is denkbaar dat de opsporingsmethode van de accountovername ook in Nederland wordt toegepast. Omdat in de *GigaTribe*-zaak de Zwitserse autoriteiten het bewijs hadden verzameld en hebben overgedragen aan de Nederlandse autoriteiten, is op grond van het vertrouwensbeginsel de opsporingsmethode niet aan de Nederlandse wetgeving getoetst.[19]

Het kan bijzonder waardevol zijn door de ogen van de verdachte of informant op besloten internetomgevingen rond te kijken en bewijs te verzamelen ten behoeve van een opsporingsonderzoek. In een online context is het daarmee mogelijk bewijs te verzamelen uit besloten netwerken, forums, accounts en andere plekken waar degene toegang toe heeft, van wie het account wordt overgenomen. Uiteraard mag bij de accountovername (en overige undercoveropsporingsmethoden) geen uitlokking plaatsvinden; de verdachte mag er niet toe worden bewogen een strafbaar feit te plegen dat hij niet voornemens was. Bij de *GigaTribe*-zaak lijkt daar bijvoorbeeld geen sprake van te zijn, omdat de desbetreffende GigaTribe-gebruikers bewust kinderpornobestanden met elkaar uitwisselden en de verdachte niet is bewogen tot het uitwisselen van de illegale bestanden nadat is gecommuniceerd met een opsporingsambtenaar onder dekmantel.

Naar mijn mening is de accountovername als opsporingsmethode mogelijk met toepassing van de bijzondere opsporingsbevoegdheid van stelselmatige informatie-inwinning als een verdachte of informant vrijwillig meewerkt en zijn inloggegevens met opsporingsautoriteiten

17 Zie Rb. Noord-Nederland 27 juli 2017, ECLI:NL:RBNNE:2017:2882, *Computerrecht* 2018/6, m.nt. J.J. Oerlemans en Rb. Amsterdam 22 november 2017, ECLI:NL:RBAMS:2017:8564.

18 GigaTribe is eigenlijk een '*friend-to-friend*'-programma, omdat het alleen verbindt met toegevoegde contacten van de gebruiker.

19 Zie Rb. Noord-Nederland 27 juli 2017, ECLI:NL:RBNNE:2017:2882.

doi: 10.5553/JV/016758502018044005007

deelt.[20] Opsporingsambtenaren kunnen vervolgens kennisnemen van informatie in deze besloten omgevingen en daarbij gegevens overnemen. Met de inzet van undercoverbevoegdheid kunnen zij onder dekmantel uit naam van die verdachte of informant communiceren met betrokkenen in het opsporingsonderzoek. Als daarbij een strafbaar feit wordt gepleegd, zoals het delen van kinderpornomateriaal als in bovengenoemde zaak, moet de BOB-bevoegdheid van infiltratie worden toegepast. Zonder informatie hierover in een openbare richtlijn van het Openbaar Ministerie of jurisprudentie waarbij de rechtmatigheid van de opsporingsmethode aan de Nederlandse wetgeving wordt getoetst, kan niet met 100% zekerheid worden gesteld dat deze toepassing inderdaad onder Nederlandse wetgeving mogelijk is. Het is uiteraard van belang dat afspraken worden gemaakt over hoe ver de opsporingsautoriteiten mogen gaan uit naam van degene die zijn account beschikbaar heeft gesteld.

De lokpuber

Na implementatie van de Wet computercriminaliteit III[21] kunnen opsporingsambtenaren zich ook voordoen als minderjarige (de 'lokpuber') en chatten met andere internetgebruikers. Deze opsporingsmethode kan waardevol zijn bij de opsporing van het delict grooming en ontucht.
Grooming is kort gezegd de strafbare gedraging waarbij een meerderjarige via internet met een minderjarige een afspraak maakt om seks te hebben.[22] Eerder heeft een dergelijke undercoveroperatie tot vrijspraak geleid, omdat voor de delictsomschrijving is vereist dat daadwerkelijk met een *minderjarig persoon* wordt afgesproken.[23] De tekst van artikel 248e (grooming) en artikel 248a van het Wetboek van Strafrecht (Sr) (ontucht) wordt nu aangepast, waardoor het volstrekt helder

20 Zie mijn annotatie bij Rb. Noord-Nederland 27 juli 2017, ECLI:NL:RBNNE:2017:2882 in *Computerrecht* 2018/6. De commissie-Koops (2018) merkt in haar rapport op dat opsporingsambtenaren soms ook actief inloggen op een account van een verdachte, waarbij de inloggegevens zijn verkregen na de inbeslagname van een gegevensdrager. De commissie stelt voor deze opsporingsbevoegdheid mogelijk te maken door deze onder de reikwijdte van de netwerkzoeking onder te brengen. In het hier besproken geval komt daar nog bij dat onder het account van de betrokkene met anderen wordt gecommuniceerd, waardoor de inzet van een undercoverbevoegdheid voor de hand ligt.
21 De Wet computercriminaliteit III is op 26 juni 2018 door de Eerste Kamer aangenomen.
22 Grooming is strafbaar gesteld in art. 248e Sr.
23 Zie Hof Den Haag 25 juni 2013, ECLI:NL:GHDHA:2013:2302.

doi: 10.5553/JV/016758502018044005007

wordt dat ook van grooming en ontucht sprake kan zijn als een meerjarige opsporingsambtenaar of zelfs een computerprogramma met de verdachte onder dekmantel communiceert, vanwege de toevoeging in de delictsomschrijving:

> 'of iemand zich, al dan niet met een technisch hulpmiddel, waaronder een virtuele creatie van een persoon die de leeftijd van achttien jaren nog niet heeft bereikt, voordoet als een persoon die de leeftijd van achttien jaren nog niet heeft bereikt'.[24]

In de memorie van toelichting van de Wet computercriminaliteit III wordt opgemerkt dat de inzet van de lokpuber plaatsvond op basis van de algemene taakstellende bepalingen van opsporingsambtenaren, dat wil zeggen artikel 3 Polw jo. artikel 141-142 Sv.[25] Hierbij sluit de wetgever kennelijk aan bij de lokfiets, die volgens jurisprudentie kan worden neergezet op basis van artikel 3 Polw.[26] Toch is het de vraag of de 'lokpuber' en 'lokfiets' over één kam kunnen worden geschoren. Bij de lokfiets ontstaat weinig zicht op het privéleven van de verdachten of derden. Terwijl bij de lokpuber en webcamseks het gespreksonderwerp intiem (seksueel) van aard is. Bovendien worden persoonsgegevens of een opname opgeslagen in politiesystemen ter bewijsvoering van grooming of webcamseks. Bij grooming is bovendien mogelijk sprake van een langere duur van het gesprek of een hogere frequentie van gesprekken. De vraag is of de grondslag van artikel 3 Polw dan wel voldoet. Voor de zekerheid kan daarom beter de bijzondere opsporingsbevoegdheid van stelselmatige informatie-inwinning worden ingezet.

24 Uit het citaat blijkt tevens dat de aanpassing ook is geïnspireerd door de actie van Terres des Hommes met het 'Sweetie project', waarmee met een virtueel meisje webcamseks aan de kaak is gesteld (zie uitgebreid Schermer e.a. 2016). Zie voor kritiek op de formulering van deze nieuwe strafbaarstelling o.a. De Hingh 2018 en over de precaire grens met het uitlokkingsverbod ook Ölçer 2014, p. 18.

25 *Kamerstukken II* 2015/16, 34372, 3, p. 72. In dezelfde zin *Kamerstukken II* 2016/17, 34372, 6, p. 115.

26 Zie HR 28 oktober 2008, ECLI:NL:HR:2008:BE9817 (*lokfiets*) en HR 23 januari 2018, ECLI:NL:HR:2018:62.

doi: 10.5553/JV/016758502018044005007

Facebookvrienden worden met de verdachte

Kunnen opsporingsambtenaren ook 'Facebookvrienden' worden met de verdachte? Het antwoord op deze vraag luidt bevestigend, zo blijkt uit de '*Context*-zaak'.[27] In deze zaak hebben opsporingsambtenaren 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.
In de *Context*-zaak hadden de opsporingsambtenaren het bevel van de officier van justitie voor stelselmatige informatie-inwinning pas later tijdens de undercoveroperatie verkregen. De rechters waren echter van mening dat al vóór het aanmaken van een profiel het bevel tot stelselmatige informatie-inwinning noodzakelijk was.[28] Dit is mijns inziens terecht, omdat bij het toevoegen van een nepprofiel aan het profiel van een verdachte er een grote kans is dat een 'min of meer volledig beeld van bepaalde aspecten van iemands privéleven' wordt verkregen. De inschatting of daarvan sprake is, moet voorafgaand aan de inzet van de opsporingsmethode plaatsvinden. Op Facebookprofielen zetten mensen in de regel veel privégegevens online, zoals foto's, geboortedatum, interesses en informatie over relaties. Daarnaast is het gehele online sociale netwerk van de betrokkene met betrekking tot die dienst zichtbaar. Daarom wordt al snel bij de inzet van het BOB-middel op Facebook aan het criterium voldaan.
Uit de *Context*-zaak bleek ook dat er sprake was van gebrekkige vastlegging van de opsporingshandelingen.[29] Hier kan nog een les uit worden getrokken voor toekomstige zaken: de verslaglegging van dit type opsporingshandelingen in strafzaken is essentieel.

27 Rb. Den Haag 10 december 2015, ECLI:NL:RBDHA:2015:14365, *Computerrecht* 2016/46, m.nt. J.J. Oerlemans en Hof Den Haag 25 mei 2018, ECLI:NL:GHDHA:2018:1248 (*Context*).
28 Zie Rb. Den Haag 10 december 2015, ECLI:NL:RBDHA:2015:14365, r.o. 5.26-5.27. Zie de bevestiging van deze zaak in het arrest van Hof Den Haag 25 mei 2018, ECLI:NL:GHDHA:2018:1248 (*Context*).
29 Zie Rb. Den Haag 10 december 2015, ECLI:NL:RBDHA:2015:14365, r.o. 5.27. Het maken van een proces-verbaal is hier verplicht, omdat de opsporingshandelingen mogelijk relevant tijdens het proces kunnen zijn. De vormverzuimen hebben niet geleid tot een sanctie. Het vormverzuim is daarmee dus 'gerelativeerd'.

doi: 10.5553/JV/016758502018044005007

Infiltratie

Infiltratieoperaties onderscheiden zich van stelselmatige inwinning in de zin dat bij infiltratieoperaties wordt *geparticipeerd* in een criminele organisatie teneinde bewijsmateriaal over strafbare feiten te verzamelen.[30] Het is daarbij mogelijk dat (geautoriseerde) strafbare feiten worden gepleegd. De Nederlandse wetgever gaf in de memorie van toelichting van de Wet BOB aan dat door middel van infiltratieoperaties bewijs kan worden verzameld over de strafbare feiten die in georganiseerd verband worden gepleegd (of worden gepland) en met de opsporingsmethode inzicht kan worden verkregen in de modus operandi van de verdachten.[31] Een infiltratieoperatie mag 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.[32] Als intern controlemechanisme moet ook de Centrale Toetsingscommissie van het Openbaar Ministerie verplicht advies geven over de inzet van infiltratieoperaties.
Infiltratieoperaties kunnen ook in een online context worden ingezet, zoals op online fora of handelswebsites waarbij het vermoeden bestaat dat strafbare feiten in georganiseerd verband worden gepleegd. Het ligt bijvoorbeeld voor de hand dat bij de eerder in dit nummer beschreven *Hansa-operatie* de bijzondere opsporingsbevoegdheid van infiltratie is ingezet. Het is daarbij spannend om te zien hoe rechters omgaan met het doorlaten van de drugs of de uitgestelde inbeslagneming daarvan; door het runnen van de website wordt immers drugshandel gefaciliteerd, hetgeen een van de gevoeligheden bij de IRT-affaire was.
Uit gepubliceerde jurisprudentie blijkt dat opsporingsinstanties eerder hebben geprobeerd in de hiërarchie van een online drugsmarktplaats op te klimmen door middel van een online infiltratieoperatie.[33] De opsporingsambtenaren hadden in deze zaak onder andere het doel de

30 Zie *Kamerstukken II* 1996/97, 25403, 3, p. 28–29. Zie ook de brief van de minister van Veiligheid en Justitie van 8 oktober 2014 (nr. 571620) over het juridische verschil tussen 'informanten' en 'individuen die infiltreren binnen een opsporingsonderzoek'.
31 Zie *Kamerstukken II* 1996/97, 25403, 3, p. 28.
32 Zie art. 126h Sv.
33 Rb. Midden-Nederland 9 oktober 2014, ECLI:NL:RBMNE:2014:4790 en ECLI:NL:RBMNE:2014:4792. Vermoedelijk ging het hier om de online marktplaatsen '*Black Market Reloaded*' en '*Utopia*'. Zie ook ANP, 'OM wil tot zeven jaar cel voor internetdealers', Nu.nl 23 september 2014.

doi: 10.5553/JV/016758502018044005007

positie van 'moderator' te verwerven. Moderators managen de dagelijkse taken van een forum en controleren de naleving van interne regels door de gebruikers van een forum. In die positie kan een goed beeld van de gebruikers van het criminele forum worden verkregen. Ter uitvoering van de operatie werd de bijzondere opsporingsbevoegdheid van infiltratie ingezet. Het is de opsporingsambtenaren uiteindelijk niet gelukt zelf moderator te worden op het forum. Zij wisten echter wel het vertrouwen te winnen van een van de moderators op het forum. Door middel van een pseudokoop werden drugs aangekocht (de moderator verkocht zelf ook drugs) en voor de aflevering werd een afspraak in de fysieke wereld gemaakt. Na de aankoop van de drugs is de verdachte gevolgd tot zijn woonhuis door een observatieteam, waarvoor de bijzondere bevoegdheid van systematische observatie was ingezet. De verdachte werd later gearresteerd. De advocaat van de verdachte protesteerde tegen het feit dat de operatie zowel in de fysieke wereld als 'virtueel' had plaatsgevonden. De rechter keurde deze hybride toepassing van de bijzondere opsporingsbevoegdheid van infiltratie goed.[34] Toch is het opvallend dat maar één zaak over de toepassing van een online infiltratie beschikbaar is. Meer jurisprudentie is noodzakelijk om de reikwijdte van de toepassing van de bijzondere opsporingsbevoegdheid in een online context voldoende te bepalen.

Tussenconclusie

Online undercoverbevoegdheden bieden een meerwaarde voor de opsporing, omdat zij naast de fysieke undercoveroperaties de mogelijkheid bieden ook in een online context onder dekmantel bewijs te verzamelen. In dit artikel is nagegaan welke toepassingsmogelijkheden er zijn met betrekking tot de pseudokoop, stelselmatige informatie-inwinning en infiltratie.
De verstrekte voorbeelden van de inzet van de bijzondere opsporingsbevoegdheden in dit artikel hebben voornamelijk betrekking op opsporingsonderzoeken naar cybercriminaliteit. In reguliere opspo-

34 Zie Rb. Midden-Nederland 9 oktober 2014, ECLI:NL:RBMNE:2014:4790 en ECLI:NL:RBMNE:2014:4792. Siemerink (2000b, p. 144) gaf in 2000 al aan dat deze hybride toepassing veel zal voorkomen. Net als in het normale leven beginnen interacties soms op internet en kunnen deze leiden tot ontmoetingen in de fysieke wereld.

doi: 10.5553/JV/016758502018044005007

ringsonderzoeken (geen cybercrime) waarbij verdachten online actief zijn, biedt de toepassing van online undercoverbevoegdheden echter ook additionele mogelijkheden ten opzichte van de bevoegdheden die in de fysieke wereld kunnen worden toegepast.
In cybercrimezaken kunnen online undercoveroperaties een effectief opsporingsmiddel zijn om bewijs te verzamelen met een online handle als digitaal spoor, zoals een nickname, e-mailadres of profiel op sociale media. Onder de omstandigheid dat verdachten consistent gebruik maken van anonimiseringstechnieken die het IP-adres verhullen van het netwerk waar zij gebruik van maken, is de toepassing van online undercoveropsporingsmethoden een van de weinige middelen om bewijs te verzamelen in opsporingsonderzoeken met betrekking tot cybercriminaliteit.
Een bijkomend voordeel van de *online* toepassing van undercover-opsporingsbevoegdheden is dat opsporingsambtenaren net zo anoniem kunnen communiceren als de betrokkenen van het opsporingsonderzoek, zonder (direct) lijflijk risico en zonder de bureaustoel te hoeven verlaten, met een wereldwijd bereik van de opsporingsmethode. Dat wereldwijde bereik levert echter wel een jurisdictievraagstuk op, dat in de volgende paragraaf wordt geadresseerd.

Het jurisdictievraagstuk

Opsporingsbevoegdheden, inclusief undercoveropsporingsbevoegdheden, mogen niet over de territoriale grenzen worden toegepast zonder toestemming van de betrokken staat of verdragsbasis.[35] Nederland heeft vele bilaterale en multilaterale verdragen met andere staten afgesloten, waarin onder andere rechtshulp wordt geregeld. Over de toelaatbaarheid van de grensoverschrijdende *online* toepassing van undercoverbevoegdheden wordt daarin met geen woord gerept. Dit roept de vraag op in hoeverre opsporingsambtenaren de bovengenoemde bijzondere opsporingsbevoegdheden unilateraal (dus zonder

35 Zie de *S.S. 'Lotus'*-zaak (*Frankrijk/Turkije*), *PCIJ Reports*, Series A, nr. 10, 7 september 1927, 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.' Zie ook 'Rule 11' uit de Tallinn Manual 2.0 (Schmidt 2017, p. 66).

doi: 10.5553/JV/016758502018044005007

toestemming van een betrokken staat) en grensoverschrijdend mogen toepassen.

In de praktijk worden online undercoveroperaties dikwijls unilateraal uitgevoerd. De eerder in dit nummer beschreven *Hansa*-zaak is daar een voorbeeld van. Naar goed gebruik worden de autoriteiten van de betrokken staat van de operatie op de hoogte gesteld en vaak wordt het bewijsmateriaal aan de betrokken autoriteiten overgedragen, zodat zij zelf handhavend kunnen optreden. Uit nieuwsberichten en jurisprudentie blijkt ook dat Amerikaanse autoriteiten via internet Nederlandse ingezetenen hebben benaderd en pseudokopen op online handelsplaatsen hebben uitgevoerd (zie bijvoorbeeld Kreling & Modderkolk 2016; Lensink & Vuijst 2013).[36] Het is niet helemaal duidelijk of de Amerikanen wisten dat het Nederlandse ingezetenen waren die zij benaderden. Als een drugsverkoper bijvoorbeeld van de anonimiseringsdienst TOR gebruik maakt en zijn handel op een online drugsmarktplaats in de Engelse taal aanbiedt, dan is zijn IP-adres en daarmee – na de vordering van gebruikersgegevens – het woonadres van de abonneehouder niet vast te stellen. In deze situatie is het verdedigbaar dat een undercoveroperatie unilateraal wordt uitgevoerd, omdat de opsporingsautoriteiten van de onderzoekende staat dan niet redelijkerwijs kunnen vaststellen waar de verdachte zich bevindt (Oerlemans 2017, p. 338). Opsporingsautoriteiten bewegen zich echter internationaalrechtelijk gezien op glad ijs als ze gericht een buitenlandse ingezetene via internet benaderen en op unilaterale wijze undercoverbevoegdheden toepassen.

De opsporing en vervolging van personen worden namelijk gezien als de exclusieve taak van een staat (Schmidt 2017, p. 21). Het zonder toestemming overnemen van die taak is dan een schending van de soevereiniteit van de betrokken staat.[37] Dat kan gevolgen met zich meebrengen, bijvoorbeeld op diplomatiek gebied. In Nederland heeft de vermeende unilaterale opsporing van de Amerikanen geleid tot Kamervragen.[38] Ook vanuit het perspectief van de burger zijn vraagtekens te zetten bij unilaterale digitale opsporing. Opsporingsinstanties over de hele wereld kunnen praktisch gezien met toepassing van hun eigen

36 Zie bijv. Rb. Rotterdam 11 augustus 2017, ECLI:NL:RBROT:2017:6830.

37 Overigens kan de betrokken staat achteraf alsnog toestemming geven.

38 Zie het antwoord op Kamervragen over de uitlevering van een Nederlandse hacker aan de VS door Roemenië van 7 juli 2012, *Aanhangsel Handelingen II* 2011/12, 3160 en het antwoord op Kamervragen over 'FBI agenten hacken mee met Nederlandse politie en detentieomstandigheden VS' van 15 april 2013, *Aanhangsel Handelingen II* 2012/13, 2001.

doi: 10.5553/JV/016758502018044005007

lokale wetgeving – zowel voor de strafbaarstellingen als voor opsporingsbevoegdheden – via internet opsporen, terwijl deze buitenlandse wetgeving niet kenbaar is voor de verdachte. Dat is een rechtsstatelijk probleem. Juist die kennis over de omstandigheden en onder welke voorwaarden opsporingsautoriteiten hun zwaardmacht mogen uitoefenen, is een kernprincipe van het leven in een rechtsstaat (Oerlemans 2017, p. 297). De mogelijke schending van de soevereiniteit van de betrokken staat leidt overigens niet tot gevolgen voor het strafproces, omdat hiermee geen beschermd belang van de verdachte gemoeid is dat zou leiden tot de sanctie van een vormverzuim in de zin van artikel 359a Sv.[39]

Hirsch Ballin (2018) schreef recentelijk in *Ars Aequi* een interessant artikel waarin zij pleit voor de mogelijkheid tot unilaterale online opsporing. Dit is op het eerste gezicht radicaal vanuit internationaalrechtelijk perspectief, maar zij merkt in het artikel meteen op dat daarvoor internationale afspraken noodzakelijk zijn. Voor online undercoveroperaties is het misschien mogelijk tot een EU-verdrag te komen. Europol is in het 'Internet Organised Crime Threat Assessment' (IOCTA)-rapport (2016, p. 14) over de noodzaak daarvan in ieder geval helder:

> 'The difficulties faced by law enforcement operating lawfully in the Darknet are clear, with many jurisdictions restricted by national legislation. A harmonised approach to undercover investigations is required across the EU.'

Tot op heden zijn hier nog geen initiatieven op EU-niveau voor geweest. Het is een grote stap voor staten ook formeel digitale unilaterale vormen van opsporing toe te staan en daarover afspraken te maken met andere staten. De stormachtige ontwikkeling van cybercriminaliteit en de noodzakelijke inzet van digitale opsporingsbevoegdheden om bewijs te verzamelen laten hun echter geen keuze.

39 Met andere woorden: de 'Schutznorm' is niet van toepassing. Zie HR 7 maart 2000, *NJ* 2000/539, m.nt. Sch.

doi: 10.5553/JV/016758502018044005007

Literatuur

Commissie-Koops 2018
Commissie-Koops (Commissie modernisering opsporingsonderzoek in het digitale tijdperk), *Regulering van opsporingsbevoegdheden in een digitale omgeving*, s.l. 2018.

Commissie-Van Traa 1996
Commissie-Van Traa, *Inzake opsporing. Enquête opsporingsmethoden*, Den Haag: Sdu Uitgevers 1996.

Europol 2016
Europol, *Internet Organised Crime Threat Assessment (IOCTA)*, Den Haag: European Police Office 2016.

De Hingh 2018
A.E. de Hingh, 'Grooming in het wetsvoorstel Computercriminaliteit III. Over het verbod op sexchatten met kinderen, robots en politieambtenaren', *Computerrecht* 2018, afl. 4, p. 208-215.

Hirsch Ballin 2018
M.F.H. Hirsch Ballin, 'De rol van grenzen bij opsporing: grenzeloze inzet van opsporingsbevoegdheden?', *Ars Aequi* 2018, afl. 6, p. 462-467.

Kreling & Modderkolk 2016
T. Kreling & H. Modderkolk, 'De dealer die in de Amerikaanse val werd gelokt', *de Volkskrant* 7 juni 2016.

Kruisbergen & De Jong 2010
E.W. Kruisbergen & D. de Jong, *Opsporen onder dekmantel. Regulering, uitvoering en resultaten van undercovertrajecten*, Den Haag: WODC/Boom Juridische uitgevers 2010.

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

Lensink & Vuijst 2013
H. Lensink & F. Vuijst, 'Geen krediet voor David S.', *Vrij Nederland* 16 maart 2013.

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

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

Schermer e.a. 2016
B.W. Schermer, I.N. Georgieva, S. van der Hof & B.J. Koops, *Legal aspects of Sweetie 2.0*, Leiden/Tilburg: Center for Law and Digital Technologies (eLaw)/Tilburg Institute for Law Technology and Society (TILT) 2016.

doi: 10.5553/JV/016758502018044005007

Schmidt 2017
M.N. Schmitt (red.), *Tallinn Manual 2.0 on the international law applicable to cyber operations*, Cambridge: Cambridge University Press 2017.

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

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

doi: 10.5553/JV/016758502018044005007