3 Formeel strafrecht & ICT

Bert-Jaap Koops & Jan-Jaap Oerlemans[1]

Formeel strafrecht betreft de opsporing en vervolging van strafbare feiten, alsmede de tenuitvoerlegging van straffen. Opsporingsmethoden die een meer dan geringe inmenging met de rechten en vrijheden van de betrokken met zich meebrengen worden doorgaans in het Wetboek van Strafvordering (hierna: Sv) genormeerd.
Het opsporingsproces naar computergerichte en computergerelateerde criminaliteit ziet er anders uit dan het klassieke opsporingsproces in de fysieke wereld. Dit komt doordat computerdelicten zich grotendeels in een online context afspelen en het opsporingsproces dientengevolge ook. Toch geldt sinds halverwege de jaren negentig van de vorige eeuw het adagium: "wat offline geldt, geldt ook online".[2] Om deze reden is het juridisch opsporingskader van toepassing bij de inzet van bevoegdheden in een online context ongeacht of het computerdelicten of andere delicten betreft. Zo kan bijvoorbeeld bij moordzaken de zoekgeschiedenis op een computer de vereiste 'voorbedachte rade' opleveren,[3] en kunnen bij drugszaken via een smartphone verstuurde privéberichten over de prijslijsten van drugs en 'aanbiedingen van de maand' belangrijk bewijs opleveren.[4] Het gaat bij ICT-gerelateerde opsporingsbevoegdheden dus om computercriminaliteit in ruime zin (zie paragraaf 1.2).

In dit hoofdstuk beschrijven en analyseren wij de ICT-gerelateerde opsporingsbevoegdheden. Het hoofdstuk beoogt meer duidelijkheid te geven over de toepassing,

---

1 Bert-Jaap Koops is hoogleraar regulering van technologie bij TILT – Tilburg Institute for Law, Technology, and Society (TILT) van de Universiteit van Tilburg. Jan-Jaap Oerlemans is als onderzoeker verbonden aan eLaw, het centrum voor Recht en Digitale Technologie van de Universiteit Leiden. Dit hoofdstuk bouwt voort op de versie van dit hoofdstuk uit de tweede, herziene druk (2007) van Bert-Jaap Koops en Ybo Buruma. Ybo Buruma, raadsheer in de Hoge Raad en voormalig hoogleraar straf- en strafprocesrecht aan de Radboud Universiteit Nijmegen, heeft toestemming gegeven voor dit hergebruik. Daarnaast zijn verschillende delen in dit hoofdstuk gebaseerd op Oerlemans 2017a en Oerlemans 2017b.

2 Zie *Kamerstukken II* 1997/98, 25880, 1, p. 1 (nota Wetgeving elektronische snelweg).

3 Zie bijvoorbeeld Hof Arnhem 4 mei 2012, ECLI:NL:GHARN:2012:BW4764 (bewijs van moord mede op basis van zoekwoorden als "Walther PPK", "Walther PPK onderhoud", "dood" en "kogel door het hoofd"), Rb. Noord-Holland 4 november 2016, ECLI:NL:RBNHO:2016:9098 (onderbouwing van voorbedachte raad door digitale aantekeningen van de verdachte over het slachtoffer en zoekgeschiedenis). en Rb. Rotterdam 16 mei 2017, ECLI:NL:RBROT:2017:4101 (poging tot moord door middel van brandstichting, met veelzeggende zoektermen als "met terpentine overgieten", "terpentine verdampt", "oorzaak uitgebrande slaapkamer", "terpentine brand" en "man steekt dakloze die aan het slapen is in brand").

4 Zie Rb. Noord-Nederland 9 maart 2017, ECLI:NL:RBNNE:2017:843 en Rb. Midden-Nederland 3 januari 2017, ECLI:NL:RBMNE:2017:93.

reikwijdte en juridische basis van digitale opsporingsmethoden. De analyse is daarbij beperkt tot het opsporingsonderzoek, waarbij met name de *vergaring* van gegevens wordt genormeerd. De normering van het *verwerken* van persoonsgegevens door de opsporingsinstanties valt buiten het bestek van dit hoofdstuk.[5]
Dit hoofdstuk begint met een korte introductie van het opsporingsonderzoek en de normering van opsporingsmethoden in het strafprocesrecht (paragraaf 3.1). Daarna komen eerst de opsporingsbevoegdheden aan bod die over het algemeen gericht zijn op het vergaren van reeds bestaande (opgeslagen) gegevens: de bevoegdheden met betrekking tot doorzoeking, beslag en onderzoek in computers, inclusief aanpalende en steunbevoegdheden als de netwerkzoeking, het ontsleutelbevel, '*notice-and-takedown*' en ontoegankelijkmaking (paragraaf 3.2), alsmede de bevoegdheden tot het vorderen van gegevens (paragraaf 3.3). Vervolgens komen bijzondere opsporingsbevoegdheden aan bod, die over het algemeen gericht zijn op het vergaren van nog niet reeds ergens vastgelegde gegevens: de telecommunicatietap (paragraaf 3.4), direct afluisteren (paragraaf 3.5) en stelselmatige observatie en locatiebepaling (paragraaf 3.6). Daarna behandelen we opsporingsbevoegdheden die een hybride karakter hebben, in de zin dat ze zowel van toepassing kunnen zijn op historische (reeds ergens vastgelegde) als toekomstige (nog niet reeds ergens vastgelegde) gegevens: het van afstand binnendringen in geautomatiseerde werken – oftewel hacken – (paragraaf 3.7) en het onderzoek van gegevens in publiek toegankelijke bronnen, met name internet (paragraaf 3.8). Waar deze laatste bevoegdheid een passieve is, in de zin dat geen interactie plaatsvindt met personen om informatie te genereren, zijn er ook mogelijkheden voor gegevensgaring door online interactie, oftewel undercoveroperaties zoals pseudokoop en dienstverlening, stelselmatige inwinning van informatie en infiltratie (paragraaf 3.9). Het hoofdstuk sluit af met een korte discussie van digitaal bewijs (paragraaf 3.10) en een blik op de toekomst, waaronder het project Modernisering Strafvordering (paragraaf 3.11).

3.1 Het opsporingsonderzoek

Opsporingsbevoegdheden worden tijdens een opsporingsonderzoek ingezet teneinde bewijs te verzamelen over een strafbaar feit. Op deze wijze tracht de politie, onder leiding van het Openbaar Ministerie, achter de waarheid te komen over het vermoeden van een strafbaar feit.
Opsporing is "het onderzoek in verband met strafbare feiten onder gezag van de officier van justitie met als doel het nemen van strafvorderlijke beslissingen" (artikel 132a Sv). De officier van justitie is de leider van het opsporingsonderzoek; lichte opsporingsbevoegdheden kunnen door politieambtenaren zelf worden uitgevoerd, maar voor de meeste bevoegdheden is een bevel van de officier van justitie nodig. Voor zeer

5 Zie daarover de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens, en het wetsvoorstel ter implementatie van Richtlijn 2016/680/EU, *Kamerstukken II* 2017/18, 34889, 1-3.

ingrijpende bevoegdheden behoeft de officier toestemming van de rechter-commissaris.[6]
Een opsporingsonderzoek vangt meestal aan bij een redelijk vermoeden van schuld bij een strafbaar feit.[7] Bij misdrijven die in georganiseerd verband worden gepleegd, is het mogelijk een opsporingsonderzoek te starten bij betrokkenheid van het plegen van misdrijven in georganiseerd verband.[8] Het is ook mogelijk bij aanwijzingen van terroristische misdrijven een opsporingsonderzoek te starten en bijzondere opsporingsbevoegdheden in te zetten.[9] In de plannen tot de modernisering van het Wetboek van Strafvordering met betrekking tot het opsporingsonderzoek wordt beoogd slechts één titel in het Wetboek van Strafvordering op te nemen en de huidige repetitieve en mede daardoor onoverzichtelijke regeling in de 126-serie te vereenvoudigen.[10] In dit hoofdstuk wordt alleen de juridische grondslag van de inzet van opsporingsbevoegdheden bij een redelijk vermoeden van schuld bij een strafbaar feit genoemd.

3.1.1 *Het strafvorderlijk legaliteitsbeginsel*

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 een grondslag in de wet voorhanden zijn voor bewijsgaringsactiviteiten van opsporingsambtenaren. Artikel 3 van de Politiewet 2012 (hierna: Polw) (jo.141-142 Sv) volstaat als grondslag voor opsporingsactiviteiten die slechts een geringe inmenging met de rechten en vrijheden van de betrokken individuen met zich meebrengen en geen risico voor de integriteit van het opsporingsonderzoek vormen.[11] In artikel 3 Polw jo. 141-142 Sv staat de algemene taakstelling van politieagenten beschreven, waaronder "de daadwerkelijke handhaving van de rechtsorde" waar ook het opsporingsonderzoek onder valt.
Opsporingsmethoden die een meer dan geringe inmenging op de rechten en vrijheden van de betrokken individuen met zich meebrengen of de integriteit van het opsporingsonderzoek in gevaar kunnen brengen, moeten in detail worden gereguleerd. Deze norm wordt afgeleid uit de memorie van toelichting bij de Wet bijzondere opsporingsbevoegdheden (Wet BOB) en uit jurisprudentie over de inzet van opsporingsmetho-

6 *Kamerstukken II* 1996/97, 25403, 3, p. 99: "Het vereiste van een machtiging van de rechter-commissaris is gereserveerd voor de meest in de grondrechten van burgers ingrijpende opsporingsbevoegdheden, te weten het opnemen van vertrouwelijke communicatie met een technisch hulpmiddel en de telefoontap".
7 Zie artikel 27 Sv.
8 Zie Titel V van het Eerste Boek van het Wetboek van Strafvordering.
9 Zie Titel VB van het Eerste Boek van het Wetboek van Strafvordering.
10 Zie p. 10 van de memorie van toelichting bij het Conceptwetsvoorstel Boek 2 (2017).
11 *Kamerstukken II* 1996/97, 25403, 3, p. 110 en 115.

den.[12] 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.[13]

De inzet van bevoegdheden is steeds toegestaan voor bepaalde categorieën strafbare feiten, bijvoorbeeld voor alle misdrijven, of voor misdrijven met een maximumgevangenisstraf van ten minste één jaar, of van acht jaar. Veelgebruikt is de categorie misdrijven genoemd in artikel 67, eerste lid, Sv, dat wil zeggen misdrijven waarvoor voorlopige hechtenis is toegestaan. Meestal zijn dat misdrijven met ten minste vier jaar gevangenisstraf als maximum, maar de categorie omvat ook specifiek genoemde delicten waarop een lagere maximumstraf staat. Sinds de Wet computercriminaliteit II worden bijna alle computermisdrijven met een lagere strafbedreiging dan vier jaar genoemd in artikel 67, eerste lid, Sv, zodat daarvoor veel bevoegdheden kunnen worden ingezet. De meest ingrijpende bevoegdheden kunnen alleen worden ingezet als er een misdrijf is dat – gezien zijn aard of de samenhang met andere door de verdachte begane[14] misdrijven – een ernstige inbreuk op de rechtsorde oplevert.[15]

3.1.2 *De IRT-affaire en de Wet bijzondere opsporingsbevoegdheden*

De moderne manier van regulering van opsporingsmethoden vindt haar achtergrond in de IRT-affaire uit de jaren negentig van de vorige eeuw. In de jaren negentig werkten verschillende politiekorpsen in ons land samen in 'Interregionale Recherche Teams'. Deze teams richtten zich op georganiseerde misdaad waarbij vaak drugshandel in het spel was. Geïnspireerd door de Amerikaanse opsporingspraktijk maakte het team gebruik van innovatieve opsporingsmethoden, onder meer van de zogenoemde 'groei-infiltrant'.[16] 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

12 Zie Fokkens & Kirkels-Vrijman 2009 en Borgers 2015. Deze standaard werd voor het eerst vastgesteld in de *Zwolsman*-zaak in 1995 (HR 19 december 1995, ECLI:NL:HR:1995:ZD0328, *NJ* 1996/249, m.nt. Schalken). In deze zaak maakte de Hoge Raad duidelijk dat het doorzoeken van vuilniszakken op straat niet een zodanig ernstige privacy-inmenging met zich meebrengt dat een bijzondere opsporingsbevoegdheid voor de opsporingsmethoden voorhanden moet zijn. De standaard is later bevestigd in de wetsgeschiedenis en andere arresten van de Hoge Raad. Zie bijvoorbeeld *Kamerstukken II* 1996/97, 25403, 3, p. 110 en 115 en HR 20 januari 2009, ECLI:NL:HR:2009:BF5603, *NJ* 2009/225, m.nt. Borgers, HR 13 november 2012, ECLI:NL:HR:2012:BW9338, *NJ* 2013/413, m.nt. Borgers en HR 1 juli 2014, ECLI:NL:HR:2014:1562, *NJ* 2015/115, m.nt. P.H.P.H.M.C. van Kempen.

13 Zie ook HR 12 april 1897, *W* 6954, (*Muilkorf*-arrest). In dit arrest gaf de Hoge Raad aan dat een regeling van de opsporing van strafbare feiten in een plaatselijke verordening in strijd is met de wet. Alleen de formele wetgever mag regels van strafprocesrecht opstellen.

14 Vanwege de onschuldpresumptie moet dit naar wij aannemen worden gelezen als: 'vermoedelijk begane'.

15 In de rechtspraak wordt het criterium 'ernstige inbreuk op de rechtsorde' ook wel aangenomen bij delicten die aanzienlijk minder ernstig zijn dan de in de wetgeschiedenis genoemde moord, drugshandel, mensenhandel en dergelijke. Zie Blom 2007.

16 Zie uitgebreid Nadelmann 1993, Nadelmann 1995 en Fijnaut & Marx 1995.

aan het opsporingsonderzoek en om zicht te blijven houden op de criminele organisatie.[17]
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 sommige opsporingsmethoden opriepen, maar ook omdat slechts weinig leidinggevenden bij de bevoegde instanties op de hoogte waren van de activiteiten.[18] Naar aanleiding van deze controverse werd een Parlementaire Enquêtecommissie Opsporingsmethoden ingesteld onder leiding van Van Traa. De Commissie-Van Traa schreef een uitgebreid rapport over het gebruik van de undercover opsporingsmethoden en deed aanbevelingen om deze opsporingsmethoden in het Wetboek van Strafvordering te reguleren.[19]
De aanbevelingen werden grotendeels overgenomen en leidden tot de Wet bijzondere opsporingsbevoegdheden.[20] Zoals in paragraaf 3.1.1 al werd gesteld, is het van belang dat in de wetsgeschiedenis al is opgemerkt dat opsporingsbevoegdheden, zoals stelselmatige observatie en infiltratie, onder gelijke voorwaarden in de digitale wereld kunnen worden toegepast.[21] Met andere woorden, met het aannemen van de Wet BOB heeft de Nederlandse wetgever expliciet ervoor gekozen dat de bijzondere opsporingsbevoegdheden ook in een online context toepasbaar zijn onder dezelfde voorwaarden als in een offline context. Daarbij moet echter wel worden bedacht dat de wetgever bij de totstandkoming van de Wet BOB het toenmalige internet voor ogen had, dat een veel beperkter bereik en gegevensomvang kende dan tegenwoordig het geval is.

In de memorie van toelichting van de Wet BOB werd opgemerkt dat "technische ontwikkelingen van invloed kunnen zijn op de toepassing van opsporingsmethoden". Het Wetboek van Strafvordering moet worden aangepast, indien de toepassing van deze nieuwe opsporingsmethoden – of in geval van gebruik van bestaande methoden in een nieuwe context – een meer dan geringe inmenging met rechten en vrijheden met zich meebrengt of een risico voor de integriteit voor de opsporingsonderzoeken vormt.[22]

---

17 Zie uitgebreid *Kamerstukken II* 1995/96, 24072, 10-11 (rapport-Van Traa), p. 72-164.
18 Zie *Kamerstukken II* 1995/96, 24072, 10-11 (rapport-Van Traa), p. 427-428.
19 Daarnaast zijn ook andere aanbevelingen gedaan die betrekking hebben op het recht op een eerlijk proces van verdachten, bijvoorbeeld met betrekking tot het opmaken van een proces-verbaal en de notificatie. Bovendien zijn aanbevelingen gedaan omtrent de organisatie van het opsporingsbestel. In deze studie wordt slechts ingegaan op het recht op privacy in relatie tot de normering van opsporingsmethoden.
20 *Stb.* 1999, 245, 27 mei 1999. De Wet BOB is in werking getreden op 1 februari 2000. Zie Buruma 2001, p. 33-130 voor een overzicht van opsporingsbevoegdheden die destijds werden geïntroduceerd.
21 Zie *Kamerstukken II* 1998/99, 26671, 3, p. 36.
22 *Kamerstukken II* 1996/97, 25403, 3, p. 12. Strikt genomen wordt in de memorie van toelichting alleen gesproken van een geringe inbreuk op het recht op privacy. Door de jaren heen is helder geworden dat ook andere rechten en vrijheden van belang zijn bij de toets of opsporingsmethoden in detail gereguleerd moeten worden als bijzondere opsporingsbevoegdheden. Zie ook de aanbeveling van de Raad van Europa (Recommendation Rec (2005)10) aan lidstaten over "*special investigation techniques*" met betrekking tot ernstige misdrijven (inclusief terrorisme): *"Considering that special investigation techniques are numerous, varied and constantly evolving and their common characteristics are their cover nature and the fact that their application could interfere with fundamental rights and freedoms*".

Het is aan de wetgever daarop de wet aan te passen, dus niet aan de rechter en zeker niet aan opsporingsinstanties, en zo een juridische basis voor nieuwe opsporingsmethoden te creëren.[23] Verschillende malen heeft de Nederlandse wetgever dat al gedaan, bijvoorbeeld met de Wet vorderen gegevens in 2005, de Wet computercriminaliteit II in 2006 en de Wet computercriminaliteit III in 2018.

3.1.3 *Relativering van vormverzuimen*

Wanneer de autoriteiten onrechtmatig verkregen bewijs op een presenteerblaadje krijgen aangeboden, maar geen betrokkenheid hebben bij de onregelmatigheden, is er geen probleem voor het bewijs, zo blijkt bijvoorbeeld in de zaak van de babyfoon.[24] In deze zaak luisterden de buren van de verdachte gesprekken af via een babyfoon en namen deze op een cassettebandje op. Dit cassettebandje gaven zij eigener beweging aan de politie, en dit kon gewoon als bewijs worden gebruikt binnen het strafproces.
Wanneer opsporingsautoriteiten wel zelf betrokken zijn bij onregelmatigheden in de bewijsverkrijging, kan het materiaal in veel gevallen toch worden gebruikt als bewijs. Slechts als de bewijsgaring op een grove nalatige wijze is gebeurd, leidt het vormverzuim tot bewijsuitsluiting of niet-ontvankelijkheid (artikel 359a Sv). Lichte overtredingen van vormvoorschriften in het vooronderzoek leiden in de regel enkel tot het vaststellen van het vormverzuim of strafvermindering. De vormverzuimen waarop artikel 359a Sv betrekking heeft, kunnen voortvloeien uit de schending van wettelijke normen, verdragsbepalingen (zoals het EVRM) of ongeschreven normen.[25]
De Hoge Raad heeft in jurisprudententie de lat voor sancties op vormverzuimen hoog gelegd, door deze te 'relativeren'.[26] De verdachte moet sowieso in een verdedigingsbelang worden geschaad dat door het geschonden vormvoorzicht wordt beschermd. Dit wordt de *Schutznorm* genoemd. Het Europees Hof voor de Rechten van de Mens is overigens ook terughoudend bij de toetsing van procedures voor bewijsuitsluiting. Dat betekent dat het aan de lidstaten is om te bepalen welke gevolgen aan bijvoorbeeld illegaal tappen of illegaal direct afluisteren worden verbonden.[27]
De normering van ingrijpende opsporingsmethoden biedt burgers bescherming tegen willekeur van toepassing van overheidsmacht. Het biedt de burger rechtszekerheid en het geeft duidelijkheid aan opsporingsinstanties hoe ver ze kunnen gaan. De relativering van vormverzuimen heeft als nadeel dat zij geen prikkel biedt aan opsporingsin-

23 Zie Corstens & Borgers 2014, p. 19. Wel wordt door onder andere Borgers (2015) voorgesteld dat overwogen zou kunnen worden zogenoemde 'lichte opsporingsmethoden' die op basis van artikel 3 Politiewet kunnen worden ingezet, verder te reguleren in Algemene Maatregelen van Bestuur (AMvB's). Zie ook Contourennota 2015, p. 10-11.
24 HR 14 januari 2003, ECLI:NL:HR:2003:AE9038, *NJ* 2003/288, m.nt. YB.
25 Corstens & Borgers 2014, p. 816.
26 Zie bijvoorbeeld HR 19 februari 2013, ECLI:NL:HR:2013:BY5321, *NJ* 2013/308, m.nt. B.F. Keulen, HR 3 februari 2015, ECLI:NL:HR:2015:193 en HR 4 oktober 2016, ECLI:NL:HR:2016:2247. Zie zeer uitvoerig over het onderwerp Kuiper 2014 en Embregts 2003.
27 Zie bijvoorbeeld: *EHRM 12 mei 2000, NJ 2002/180, m.nt. Sch (Khan); zie ook EHRM 25 september 2001, NJ 2003/670, m.nt. EJD (PG en JH t. UK).*

stanties om zich aan alle voorschriften te houden en om niet te gemakkelijk de grenzen van de wet op te zoeken met nieuwe opsporingsmethoden. Het is begrijpelijk dat de Hoge Raad onregelmatigheden in het opsporingsonderzoek niet ten goede wil laten komen aan de verdachte als diens belang niet door de desbetreffende onregelmatigheid is geschaad; in principe zijn daarvoor andere wegen voorhanden, zoals onrechtmatige-daadsacties en tuchtrecht. De vraag is echter of in de praktijk wel voldoende andere sanctiewegen worden bewandeld die afdoende prikkels bieden om onregelmatigheden in de opsporing te voorkomen. Volgens ons kan onder omstandigheden ook bewijsuitsluiting nodig zijn, mede gelet op de "positive duty on the State to take reasonable and appropriate measures to secure the applicants' rights under Article 8", zoals het EHRM de staatstaak omschrijft.[28] Onzes inziens is het dan ook een terechte keuze van de wetgever om bij het gemoderniseerde wetboek een 'normatief richtsnoer' te bieden in de vorm van een iets striktere bepaling over de omgang met onrechtmatig verkregen bewijs.[29]
Zolang de huidige lijn van omgang met onrechtmatig verkregen bewijs echter wordt voortgezet, kan het Nederlandse opsporingsonderzoek worden gekenschetst als een pragmatisch georiënteerd systeem waarin misdaadbestrijding zwaarder lijkt te wegen dan rechtsbescherming.[30]

3.1.4 *Verkennend onderzoek*

Ter voorbereiding van een opsporingsonderzoek kan een 'verkennend onderzoek' worden aangevangen (artikel 126gg Sv). Volgens artikel 126gg Sv kan de officier van justitie bevelen dat opsporingsambtenaren een onderzoek instellen met als doel voorbereiding van opsporing, indien aanwijzingen bestaan dat binnen verzamelingen van personen misdrijven worden gepleegd waarvoor voorlopige hechtenis is toegelaten en die een ernstige inbreuk op de rechtsorde opleveren. Bij dergelijk onderzoek gaat het om grotere, lossere verzamelingen, bijvoorbeeld mensen die in een bepaalde branche werken. Daarbij kan gebruik worden gemaakt van bestaande, al dan niet in registers opgeslagen gegevens. In 2001 is een tweede lid ingevoegd: "Indien dit noodzakelijk is voor de uitvoering van het onderzoek kan de officier van justitie bepalen dat artikel 9, eerste lid, van de Wet bescherming persoonsgegevens met betrekking tot het onderzoek niet van toepassing is op daarbij nader aan te geven openbare registers die bij wet zijn ingesteld".[31] Artikel 9 lid 1 Wbp ziet op doelbinding: persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.

28 EHRM 2 oktober 2001, nr. 36022/97 (*Hatton e.a. t. Verenigd Koninkrijk*).
29 Zie concept-wetsvoorstel voor Boek 4, voorgesteld artikel 4.3.2.6 lid 3: "Indien opsporingsambtenaren onrechtmatig hebben gehandeld, kan het belang van een goede rechtsbedeling meebrengen dat de resultaten worden uitgesloten als bewijs teneinde te bevorderen dat in overeenstemming met de geschonden norm wordt gehandeld". Zie nader Samadi 2018.
30 Koops 2016, p. 54.
31 *Stb.* 2001, 180.

Bij het verkennend onderzoek zal rekening moeten worden gehouden met de mogelijkheid dat van *data mining* gebruik wordt gemaakt, dat wil zeggen van het bevragen en met elkaar in verband brengen van verschillende systemen over een op voorhand onbepaalde groep van personen.[32] Ter illustratie: men zou uit een fiscaal register een lijst kunnen genereren van 'ieder voor wie premies worden ingehouden in Nederland maar die woonachtig is in België of in Spanje'; het aldus door *data mining* verkregen nieuwe, tijdelijke register kan dan zelf weer worden vergeleken met de index van de subjecten en hun contacten van de Criminele Inlichtingen Eenheid. Vanuit het oogpunt van persoonsgegevensbescherming zijn hier de nodige haken en ogen aan verbonden.
Specifiek voor de voorbereiding van opsporing van terroristische misdrijven zijn twee *data mining*-gerelateerde bevoegdheden ingevoerd om het verkennend onderzoek te faciliteren.[33] De officier van justitie kan op basis van artikel 126ii Sv voor een verkennend terrorismeonderzoek identificerende gegevens vorderen die niet voor persoonlijk gebruik worden verwerkt, alsmede gebruikersgegevens van telecomaanbieders.[34] Hij kan tevens op basis van artikel 126hh Sv, met machtiging van de rechter-commissaris, aan iedereen schriftelijk vorderen geautomatiseerde gegevensbestanden te verstrekken. Geheimhouders kunnen zich verschonen.[35] Het doel van de verstrekking van gegevensbestanden is bewerking door justitie, die overigens "op een zodanige wijze [wordt] uitgevoerd dat de bescherming van de persoonlijke levenssfeer van personen zo veel mogelijk wordt gewaarborgd" (lid 3). Relevante resultaten van het *data minen* kunnen enkel worden gebruikt voor het onderzoek zelf (lid 5 onder a), inclusief de opsporing van terroristische misdrijven (lid 6); dit suggereert dat zij niet mogen worden gebruikt voor de opsporing van andere misdrijven. Niet-relevante resultaten en de oorspronkelijke gegevens moeten worden vernietigd (lid 5 onder b), tenzij ze nodig zijn voor latere controle van de *data mining*; ze mogen alleen voor dergelijke controle worden gebruikt (lid 7).

Het verkennend onderzoek ziet op de *voorbereiding* van opsporingsonderzoek; zelf is het dat nog niet, waardoor nog geen gebruik mag worden gemaakt van bijzondere opsporingsbevoegdheden of van dwangmiddelen. Een voorstel tot een verkennend onderzoek wordt voorgelegd aan de hoofdofficier van justitie en deze legt het op zijn beurt voor aan de hoofdofficier van het landelijk parket en in voorkomende gevallen aan het College van Procureurs-Generaal.
Over het algemeen zal er, naar de systematiek van de Wet bijzondere opsporingsbevoegdheden, bij verkenningen op internet meestal sprake zijn van een zogenoemde

32 Over *data mining* en opsporing, zie uitgebreid Sietsma 2006.
33 *Stb.* 2006, 580, inwerkingtreding 1 februari 2007.
34 Artikel 126ii gebruikt de oude terminologie van openbare telecommunicatie.
35 Opvallend is dat alleen professionele verschoningsgerechtigden zich kunnen verschonen, maar niet de personen bedoeld in artikel 217 en 219, dus naar de letter van de wet moeten zij wel gegevensbestanden overhandigen waarmee zij zichzelf of naasten belasten van enig strafbaar feit. Artikel 126hh Sv is hierin verstrekkender dan de normale gegevensvordering van artikel 126nd Sv.

(van het verkennend onderzoek te onderscheiden) projectvoorbereiding. Daarvan is sprake wanneer bij de politie aanwezige informatie wordt gegroepeerd, geordend en eventueel gecompleteerd ter voorbereiding van een te beginnen (verkennend, strafrechtelijk financieel of opsporings-)onderzoek. Daarbij kan gezocht worden in publiek toegankelijke internetbronnen, binnen de grenzen die daarvoor gelden (zie paragraaf 3.8).

3.2 Doorzoeking, inbeslagname en onderzoek van gegevens in computers

In cybercrime-onderzoeken speelt digitaal bewijs een cruciale rol. In veel gevallen moet bewezen worden dat de verdachte ten tijde van het plegen van een misdrijf 'achter het toetsenbord' zat. Door middel van digitaal forensisch onderzoek kan worden nagegaan wie de gebruikers van een computer zijn en wat deze gebruikers op specifieke datums en tijdstippen hebben gedaan. Ook kunnen gewiste sporen in veel gevallen weer boven water worden gehaald, wat bijvoorbeeld in kinderpornografiezaken van belang kan zijn.[36]
Ook bij niet-cybercrimezaken speelt digitaal bewijs echter in toenemende mate een belangrijke rol. Smartphones bijvoorbeeld bevatten veel informatie die in uiteenlopende zaken van belang kan zijn, als sturingsinformatie of als mogelijk bewijs.
In deze paragraaf ligt de nadruk op digitaal bewijs in de vorm van gegevens die opgeslagen liggen op gegevensdragers die vatbaar zijn voor onderzoek en/of inbeslagname door opsporingsambtenaren. Meestal zijn deze gegevensdragers computers en smartphones waar een verdachte gebruik van maakt. Steeds meer zal digitaal bewijs ook opgeslagen liggen op 'slimme apparaten', zoals met internet verbonden thermostaten, lampen, koelkasten en auto's.
In dit verband verdient opmerking dat het Wetboek van Strafvordering geen definities bevat van 'gegevens' of 'geautomatiseerd werk'; wetssystematisch gezien gelden de definities uit Sr niet als zodanig voor Sv, zodat hier een theoretische lacune bestaat.[37] In de praktijk zijn er evenwel geen problemen door het ontbreken van een aparte definitiebepaling in het Wetboek van Strafvordering: de begrippen worden kennelijk gehanteerd in de betekenis zoals die in het Wetboek van Strafrecht wordt gegeven.[38] Met de ruime definitie in Sr (zie paragraaf 2.2) vallen ook 'slimme apparaten' (evenals tamelijk 'domme', zolang ze maar op enige wijze gegevens verwerken) onder 'geautomatiseerd werk'.

36 Zie bijvoorbeeld Rb. Breda, 22 februari 2006, ECLI:NL:RBBRE:2006:AV2996, Rb. 's-Hertogenbosch, 27 januari 2009, ECLI:NL:RBSHE:2009:BH0895, Rb. Den Haag, 2 maart 2012, ECLI:NL:GHSGR:2012:BW1046, Rb. Zeeland-West-Brabant 24 juni 2013, ECLI:NL:RBZWB:2013:6323 en Rb. Noord-Holland 19 maart 2015, ECLI:NL:RBNNE:2015:1302.

37 Wiemans 2004a, p. 238-240.

38 *Handelingen I* 30 mei 2006, 30-1352. De minister zegde hier toe bij de algemene herziening van het Wetboek van Strafvordering te zullen bezien of er aanleiding is gelijkluidende definities in Sv op te nemen. In het Conceptwetsvoorstel Boek 2 (2017) worden inderdaad definities opgenomen, gelijkluidend aan die in Sr.

In deze paragraaf beperken we ons bij de voorbeelden grotendeels tot computers, smartphones, USB-sticks en harde schijven, die in de praktijk op dit moment nog het meest van belang zijn in de opsporing.
Allereerst wordt het juridisch kader voor de doorzoeking geschetst, zowel de klassieke doorzoeking ter inbeslagneming van gegevensdragers als de doorzoeking ter vastlegging van gegevens (paragraaf 3.2.1). Vervolgens wordt nader ingegaan op de regeling van inbeslagname van gegevensdragers (ook buiten doorzoeking) en het onderzoek van daarop opgeslagen gegevens. Daarbij de problematiek van onderzoek van smartphones bij aanhouding apart belicht (paragraaf 3.2.2). Vervolgens wordt de aanpalende bevoegdheid van de 'netwerkzoeking' besproken, die relevant is omdat gegevens steeds vaker liggen opgeslagen in de *cloud* of op andere aangesloten computers en netwerken (paragraaf 3.2.3). Een belangrijke steunbevoegdheid is het bevel tot ongedaan maken van beveiliging (paragraaf 3.2.4), terwijl het onder omstandigheden ook belangrijk kan zijn om gegevens ontoegankelijk te maken (paragraaf 2.3.5). Een variant op dat laatste is het bevel aan derden om gegevens ontoegankelijk te maken, wat met name bij internetgegevens relevant is: het zogenoemde '*notice-and-takedown*'-bevel (paragraaf 3.2.6). We sluiten de paragraaf af met een samenvattend overzicht (paragraaf 3.2.7).

3.2.1 *De doorzoeking en daaraan gerelateerde bevoegdheden*

Tijdens een doorzoeking zijn de autoriteiten bevoegd in de te doorzoeken ruimtes aangetroffen computers te onderzoeken, waarbij relevante gegevens mogen worden gekopieerd. In het Wetboek van Strafvordering staan verschillende regelingen voor de doorzoeking. In geval van ontdekking op heterdaad of bij verdenking van een misdrijf waarvoor voorlopige hechtenis mogelijk is, is de officier van justitie bevoegd elke plaats te doorzoeken, behoudens woningen zonder toestemming van de bewoner en behoudens kantoren van professionele verschoningsgerechtigden (artikel 96c jo. 218 Sv). Verder kan de rechter-commissaris ambtshalve of op vordering van de officier van justitie elke plaats (dus ook de zojuist uitgezonderde plaatsen) doorzoeken (artikel 110 Sv).[39] Daartoe is sinds 2000 geen verlof van de rechtbank meer nodig. Bij dringende noodzakelijkheid, als het optreden van de rechter-commissaris niet kan worden afgewacht, kan de (hulp)officier van justitie ook, met machtiging van de rechter-commissaris (bijvoorbeeld gegeven via de mobiele telefoon), woningen en geheimhoudersplaatsen doorzoeken (artikel 97 Sv). Ten slotte kunnen opsporingsambtenaren bij heterdaad of verdenking van een misdrijf waarvoor voorlopige hechtenis is toegelaten, ter inbeslagneming voertuigen (met uitzondering van woongedeelten) doorzoeken (artikel 96b Sv).

39 Afgezien van de 'gewone' doorzoeking biedt het Wetboek van Strafvordering ook de mogelijkheid van een doorzoeking in het kader van een strafrechtelijk financieel onderzoek (vergelijk artikel 126b Sv).

Vastleggen van gegevens op een computer

Zoals gezegd zijn de autoriteiten tijdens de doorzoeking bevoegd computers te doorzoeken en daarbij relevante gegevens te kopiëren. Die benadering was een uitgangspunt van de wetgever bij de Wet computercriminaliteit. De wetgever vond dat voor computeronderzoek tijdens een doorzoeking geen zelfstandige bevoegdheid nodig was: als men bevoegd is te doorzoeken, waarbij bijvoorbeeld kasten opgebroken en doorzocht mogen worden, is men daarmee ook bevoegd om een computer aan te zetten en te onderzoeken. En evenals autoriteiten kopieën van vingerafdrukken mogen maken bij een doorzoeking, mogen zij kopieën maken van aangetroffen computergegevens.

Van inbeslagneming van vastgelegde gegevens kan door de aard van digitaal opgeslagen gegevens echter geen sprake zijn. Dat is van belang omdat de klassieke doorzoekingsbevoegdheden strekken tot *inbeslagneming* van voorwerpen of stukken, hetgeen dus niet mogelijk is voor gegevens (die immers geen goed zijn, zie paragraaf 1.5.2).[40] Aangezien gegevens niet in beslag genomen kunnen worden, kon er theoretisch geen reguliere doorzoeking worden aangevraagd als justitie alleen beoogde een computer te doorzoeken en gegevens te kopiëren. In de praktijk kon natuurlijk altijd een doorzoeking ter inbeslagneming van een gegevens*drager* plaatsvinden, maar dat verdiende geen schoonheidsprijs. In navolging van de Commissie-Mevis heeft de wetgever dit (theoretische) probleem bij de Wet bevoegdheden vorderen gegevens opgelost door een zelfstandige bevoegdheid in te voeren tot "doorzoeken van een plaats ter vastlegging van gegevens die op deze plaats op een gegevensdrager zijn opgeslagen of vastgelegd" (artikel 125i Sv)[41] De doorzoeking ter vastlegging van gegevens is mogelijk onder dezelfde voorwaarden als de reguliere doorzoeking; artikel 125i Sv verwijst daartoe naar de artikelen 96b, 96c, 97 en 110. Het voorstel van Wiemans om in plaats van deze vrij ingewikkelde verwijzingsbepaling een veel simpeler bepaling in de betekenissentitel op te nemen dat onder 'doorzoeking ter inbeslagneming' ook 'doorzoeking ter vastlegging van gegevens' wordt verstaan, is helaas niet overgenomen door de wetgever.[42]

Onzes inziens geldt nog steeds de oude (door de wetgever in 1993 bedoelde) situatie dat bij een klassieke doorzoeking ter inbeslagneming (dus op basis van artikel 96b e.v. Sv) ook computers onderzocht en gegevens vastgelegd kunnen worden. In de praktijk wordt echter veelal zowel een doorzoeking ter inbeslagneming als een doorzoeking ter vastlegging van gegevens aangevraagd. Een veronderstelling die in de praktijk lijkt te leven is dat gegevens alleen gezocht en vastgelegd kunnen worden op basis van artikel 125i, en niet (ook) op basis van artikel 96b e.v. Deze veronderstelling berust onzes inziens op een misverstand ten aanzien van de wetsgeschiedenis: artikel 125i Sv is niet

40 *Kamerstukken II* 1989/90, 21551, 3, p. 11-13 en (enigszins) kritisch daarover Van Dijk & Keltjens 1995, p. 225-226.

41 Zie ook Commissie-Mevis 2001, p. 88-90 en 100; *Kamerstukken II* 2001/01, 28366, 1, p. 28; Wiemans 2004a, p. 234-238. NB Tot 1 januari 2006 bevatte artikel 125i-oud Sv de (niet-gerelateerde) bevoegdheid van de r-c tot gegevensvordering (zie paragraaf 3.3.1).

42 Wiemans 2004a, p. 236-237. Hij uit kritiek op de volgorde van de artikelvermelding, die niet correspondeert met de volgorde van functionarissen, en op het opnemen van de clausule "in het belang van het onderzoek" die bij de doorzoekingsbepalingen zelf niet is geëxpliciteerd.

ingevoerd met de bedoeling exclusief de vastlegging van gegevens bij doorzoekingen te regelen, maar als aanvullende basis, met name voor gevallen waarin justitie op voorhand niet van plan is (ook) dragers in beslag te nemen maar (alleen of primair) gegevens vast te leggen.

Bescherming van communicatie op gegevensdragers

Opgeslagen gegevens kunnen communicatie betreffen. Artikel 114 Sv (bescherming van brieven en andere poststukken) is daarop niet van toepassing, vanwege de fysieke terminologie ('in beslag genomen'). Voor doorzoeking bij aanbieders van openbare telecommunicatie is daarom in 2006 een specifieke bepaling ingevoerd met een vergelijkbare strekking als artikel 114: van bij telecomaanbieders opgeslagen berichten (zoals e-mail of voicemail) mag slechts met machtiging van de rechter-commissaris worden kennisgenomen, en alleen voor zover de berichten van of voor de verdachte zijn, op de verdachte betrekking hebben, of voorwerp uitmaken van het strafbare feit (artikel 125la Sv).[43] De bepaling geldt (om ons onbekende redenen) volgens de wettekst echter alleen voor berichten aangetroffen bij een doorzoeking *ter vastlegging van gegevens*, niet bij een reguliere doorzoeking ter inbeslagneming, waarbij volgens ons immers ook computers doorzocht en gegevens gekopieerd mogen worden. Merkwaardig is ook dat de wettekst hier de oude formulering van telecomaanbieders gebruikt, namelijk aanbieders van openbare telecommunicatie, terwijl de verkeersgegevens- en tapbevoegdheden (zie paragraaf 3.2.3 en 3.4) sinds de Wet computercriminaliteit II spreken van aanbieders van communicatiediensten (waaronder besloten telecommunicatie). Hierdoor bestaat een verschil in de regimes voor onderschepping van opgeslagen berichten bij besloten en openbare telecommunicatie, terwijl de regimes voor onderschepping van stromende berichten gelijk zijn; de ratio van dit verschil is onduidelijk.

Verder geldt de communicatiebescherming vermoedelijk alleen zo lang de berichten onderweg zijn, dat wil zeggen ressorteren onder een communicatievervoerder. Bij een doorzoeking anders dan bij een dergelijke vervoerder zijn artikel 114 lid 2 en artikel 125la Sv daarom sowieso niet van toepassing. Vermoedelijk geldt echter evenmin artikel 102a Sv, dat voor inzage van brieven machtiging van de rechter-commissaris vereist.[44] Maar ook al zou artikel 102a Sv van toepassing zijn bij de doorzoeking, dan is dit beperkt tot fysieke brieven; elektronische post, faxen, voicemail, opnames van gesprekken en dergelijke mogen daarom tijdens een doorzoeking ook door lagere autoriteiten ingezien en overgenomen worden. Het verschil in rechtsbescherming bij een doorzoeking tussen opgeslagen fysieke communicatie (brieven) en opgeslagen elektronische communicatie lijkt ons achterhaald en zou door de wetgever opgeheven moeten worden.[45]

43 Ingevoerd bij de Wet bevoegdheden vorderen gegevens, *Stb*. 2005, 390.
44 Koops 2003a.
45 Zie nader Koops 2003a.

Overige waarborgen

Bij de doorzoeking (zowel ter inbeslagneming als ter vastlegging van gegevens) bestaan verder diverse vormen van rechtsbescherming. Er mag geen onderzoek plaatsvinden naar gegevens die zijn ingevoerd door of vanwege beroepsmatige geheimhouders, tenzij met hun toestemming (artikel 125l jo. 218 Sv), vergelijkbaar met artikel 98 Sv dat bepaalt dat brieven en geschriften van geheimhouders niet zonder hun toestemming mogen worden onderzocht.[46] Dit geldt zowel voor doorzoekingen bij de geheimhouders zelf als elders. Een onderzoek in een bij een geheimhouder inbeslaggenomen computer hoeft niet op voorhand beperkt te worden tot bestanden die volgens de geheimhouder niet onder zijn verschoningsrecht vallen, mede omdat "computerbestanden zich naar hun aard niet eenvoudig lenen voor afzonderlijk onderzoek"; de gehele computer mag dus worden onderzocht, mits "op een wijze waarbij het verschoningsrecht (...) niet in het gedrang komt".[47] Kwalijk is wel dat voor de doorzoeking ter vastlegging van gegevens artikel 125i Sv verwijst naar artikel 98 Sv ("brieven en andere geschriften") en niet naar het speciaal op gegevens toegesneden artikel 125l Sv.[48] Niettemin is artikel 125l gewoon van toepassing, het is immers algemeen geredigeerd voor elk onderzoek in een geautomatiseerd werk.

Verder bestaat er, als gegevens bij een doorzoeking worden vastgelegd (of ontoegankelijk gemaakt, zie onder), een notificatieplicht aan betrokkenen. Dat wil zeggen dat de verdachte (tenzij die via de processtukken toch al op de hoogte geraakt), de verantwoordelijke voor de gegevensverwerking (in de zin van de AVG) en de rechthebbende van de plaats waar de doorzoeking plaatsvond (artikel 125m Sv) van de doorzoeking op de hoogte moeten worden gebracht.[49] Tot slot moeten bij een doorzoeking vastgelegde gegevens worden vernietigd zodra ze niet meer van belang zijn voor het onderzoek; ze kunnen wel worden bewaard voor een ander onderzoek of in een register zware criminaliteit (artikel 125n Sv). Waar de notificatieplicht vergelijkbaar is met die voor bijzondere opsporingsbevoegdheden als de tap en direct afluisteren (zie artikel 126bb Sv), wijkt de vernietigingsplicht daarvan af: BOB-gegevens moeten namelijk bewaard worden tot twee maanden na afloop van de zaak (artikel 126cc Sv). Het bevreemdt enigszins dat overhandigde gegevens (artikel 126nc e.v. Sv) via de BOB-regeling bewaard moeten worden, terwijl door de politie zelf vastgelegde gegevens volgens artikel 125n vernietigd moeten worden zodra ze niet meer van belang zijn. Een ander kritiekpunt is ook hier dat artikel 125n zich beperkt tot gegevens vastgelegd bij een

46 Duijst-Heesters 2005 wijst erop dat deze bepaling achterhaald is, nu medische dossiers in toenemende mate ook niet-geschreven gegevens bevatten, zoals video's en scans. Wij gaan ervan uit dat onder 'geschriften' in dit verband ook (niet-tekstuele) elektronische bestanden moeten worden verstaan. Vgl. HR 10 april 2018, ECLI:NL:HR:2018:553 over gevorderde camerabeelden die onder het verschoningsrecht kunnen vallen. Zie ook uitgebreid Vellinga-Schootstra 2017.

47 HR 20 februari 2007, ECLI:NL:HR:2007:AZ3564.

48 Wiemans 2004a, p. 236-237.

49 Wiemans 2004a, p. 184-187, beveelt aan de notificatie uit te breiden met situaties buiten de doorzoeking, bijvoorbeeld bij vastlegging of gebruik van gegevens bij onderzoek aan een inbeslaggenomen voorwerp.

doorzoeking, en dus niet ziet op gegevens die zijn overgenomen uit bijvoorbeeld een inbeslaggenomen computer.[50]

3.2.2 *Onderzoek aan inbeslaggenomen gegevensdragers; de 'smartphone-problematiek'*

In Nederland worden gegevensdragers als voorwerpen beschouwd die binnen een opsporingsonderzoek vatbaar zijn voor inbeslagname.[51] De inbeslagnemingsbevoegdheid brengt met zich mee dat voor de waarheidsvinding onderzoek mag worden gedaan aan inbeslaggenomen voorwerpen.[52] Sporen op het voorwerp mogen worden veiliggesteld; de inhoud mag worden onderzocht op relevant bewijsmateriaal. Dat geldt, bij gebreke van een specifieke regeling die anders zou bepalen, ook voor computers.[53] Indien de gegevensdragers in beslag zijn genomen bij een doorzoeking, kan worden betoogd dat dit afdoende wordt genormeerd door de bovengeschetste regeling van doorzoeking (hoewel onzes inziens bijvoorbeeld het onderzoek aan een smartphone die in een doorzochte auto is gevonden dan wel is ondergenormeerd). Er zijn echter ook gevallen van beslag buiten de doorzoeking, bijvoorbeeld (bij voor de hand aangetroffen computers) tijdens een schouw of betreding van plaatsen en vooral in het kader van aanhouding of staandehouding (artikel 52-54 jo. 95 en 96 Sv). Indien in die gevallen onderzoek wordt gedaan aan inbeslaggenomen gegevensdragers, zoals smartphones, tablets of laptops, kan een grote hoeveelheid gegevens, veelal van uiteenlopende aard, worden aangetroffen. De rechttoe-rechtaan-toepassing van de oude doctrine dat onderzoek aan een inbeslaggenomen voorwerp besloten ligt in de beslagregeling zelf, botst met het idee dat gegevensdragers bijzondere bescherming binnen strafvordering verdienen, vanwege de hoeveelheid en gevoelige aard van de gegevens die op de gegevensdragers liggen opgeslagen. Het EHRM heeft in verschillende uitspraken ook gewezen op de ernstige privacy-inmenging die plaatsvindt bij de inbeslagname en het uitlezen van gegevensdragers. Het Straatsburgse Hof prefereert daarom de betrokken-

50 Wiemans 2004a, p. 249. Met de Wet computercriminaliteit III is artikel 126cc Sv uitgebreid met een nieuw lid 6 dat een vergelijkbare regeling treft als artikel 125n Sv, voor gevallen waarin gegevens "zijn vastgelegd tijdens een onderzoek in een geautomatiseerd werk". De algemene formulering suggereert dat dit alle situaties betreft waarin gegevens uit een (bijvoorbeeld inbeslaggenomen) computer worden vastgelegd, maar de plaatsing in de titel over bijzondere opsporingsbevoegdheden en de toelichting suggereren dat de wetgever met "onderzoek in een geautomatiseerd werk" enkel doelt op de hackbevoegdheid van artikel 126nba Sv. Vgl. *Kamerstukken II* 2015/16, 34372, 3, p. 60 ("In dit wetsvoorstel wordt tevens de bevoegdheid voorgesteld van onderzoek in een geautomatiseerd werk [i.e., artikel 126nba Sv]. Indien bij de doorzoeking ter vastlegging van gegevens of het onderzoek in een geautomatiseerd werk gegevens worden aangetroffen met betrekking tot welke of met behulp waarvan het strafbare feit is begaan, kan de officier van justitie op grond van het voorgestelde artikel 126cc, vijfde en zesde lid, Sv bepalen dat die gegevens ontoegankelijk worden gemaakt").

51 Zie voor een uitgebreide analyse van het juridisch kader over de inbeslagname van gegevensdragers en de daarop opgeslagen gegevens: Wiemans 2004.

52 Corstens & Borgers 2014, p. 541.

53 *Ibid.* HR 29 maart 1994, *NJ* 1994/577, m.nt. Sch bepaalde reeds dat "voor de waarheidsvinding onderzoek mag worden gedaan aan inbeslaggenomen voorwerpen ten einde gegevens voor het strafrechtelijk onderzoek ter beschikking te krijgen en in computers opgeslagen gegevens daarvan niet zijn uitgezonderd".

heid van een rechter(-commissaris) bij de inbeslagname en het uitlezen van de gegevensdragers.[54]

Vooral ten aanzien van onderzoek aan bij aanhouding inbeslaggenomen smartphones is in dit verband een levendige discussie ontstaan in de literatuur,[55] mede gevoed door uiteenlopende rechtspraak. De voorlopige uitkomst van deze rechtsontwikkeling wordt gevormd door het zogenoemde "smartphone-arrest" van de Hoge Raad. In feite gaat het om drie arresten die de Hoge Raad op 4 april 2017 heeft gewezen in zaken over de inbeslagname en het uitlezen van gegevens op een smartphone.[56] In één zaak doorzocht een opsporingsambtenaar de inhoud van een smartphone, specifiek: één WhatsApp-gesprek. Dit gesprek viste hij eruit, printte het en voegde het toe aan het strafdossier. De Hoge Raad overweegt in het arrest of de regeling in artikel 94 Sv jo. 95 Sv en 96 Sv voor de inbeslagname van een gegevensdrager door opsporingsambtenaren een voldoende grondslag is. Daartoe besluit de Hoge Raad dat indien bij de doorzoeking van een gegevensdrager een "min of meer volledig beeld wordt verkregen van bepaalde aspecten van het persoonlijk leven van de gebruiker", minstens een bevel van een officier van justitie of een machtiging van een rechter-commissaris is vereist. Bestaande doorzoekingsregelingen waarbij al een bevel van een officier van justitie of een daarbij komend bevel van de rechter-commissaris is vereist, worden voldoende geacht.[57] Wel geeft de Hoge Raad aan dat onderzoek door de rechter-commissaris op zijn plaats is in die gevallen waarin op voorhand is te voorzien dat de inbreuk op de persoonlijke levenssfeer zeer ingrijpend zal zijn.[58] Volgens de Hoge Raad is de algemene bevoegdheid voor inbeslagname door opsporingsambtenaren voldoende als de met het onderzoek samenhangende inbreuk op de persoonlijke levenssfeer als beperkt kan worden beschouwd.[59] Als voorbeeld geven de hoogste rechters aan dat "dit het geval zou kunnen zijn indien het onderzoek slechts bestaat uit het raadplegen van een gering aantal bepaalde op de elektronische gegevensdrager of in het geautomatiseerde werk opgeslagen of beschikbare gegevens".

Op het geformuleerde criterium van de Hoge Raad kan kritiek worden geuit. Het is de vraag of gemiddelde burgers het wel als een "beperkte inbreuk op hun recht op privacy" ervaren als hun smartphone in beslag wordt genomen en een bericht wordt uitgelezen of als handmatig in de foto's wordt gezocht om een enkele voor het delict relevante foto eruit te vissen.[60] Toch biedt het arrest enigszins meer bescherming aan

54 Zie bijvoorbeeld EHRM 30 september 2014, nr. 8429/05 (*Prezhdarovi t. Bulgarije*), paragraaf 49 en EHRM 30 mei 2017, nr. 32600/12 (*Trabajo Rueda t. Spanje*), paragraaf 45.

55 Zie onder andere Gritter 2016, Mevis, Verbaan & Salverda 2016, Koops, Conings & Verbruggen 2016 en Van den Bosch 2016.

56 HR 4 april 2017, ECLI:NL:HR:2017:584, ECLI:NL:HR:2017:588 en ECLI:NL:HR:2017:592, *NJ* 2017/230, m.nt. Kooijmans. De drie arresten zijn grotendeels gelijkluidend en verschillen alleen enigszins in de toepassing op de specifieke casus; meestal wordt gemakshalve alleen verwezen naar de zaak met ECLI-nummer 592 – de cassatie van een vooruitstrevende uitspraak van Hof Arnhem-Leeuwarden (ECLI:NL:GHARL:2015:2954, *Computerrecht* 2015/127, nr. 4, p. 210-215, m.nt. J.J. Oerlemans).

57 Zie HR 4 april 2017, ECLI:NL:HR:2017:592, r.o. 3.4.

58 Zie HR 4 april 2017, ECLI:NL:HR:2017:592, r.o. 3.6.

59 Zie HR 4 april 2017, ECLI:NL:HR:2017:592, r.o. 3.6.

60 Zie bijvoorbeeld Hof Arnhem-Leeuwarden 14 juli 2017, ECLI:NL:GHARL:2017:6069.

betrokkenen met betrekking tot de inbeslagname van gegevensdragers, vergeleken met de huidige wettelijke regeling.
Daarnaast creëert het arrest onzekerheid, omdat nu bij elke inbeslagname van een smartphone of andere gegevensdrager door de verdediging beargumenteerd kan worden dat een meer dan beperkte, of zelfs een zeer ingrijpende, inbreuk op de persoonlijke levenssfeer wordt gemaakt bij het uitlezen van de gegevensdrager.[61] Zo'n argumentatie is niet onterecht: het is bepaald niet eenduidig hoe het criterium van de Hoge Raad moet worden toegepast: wanneer is er sprake van een geringe, een meer dan geringe en een zeer ingrijpende inbreuk? De factoren die worden genoemd bij een beperkte inbreuk – een "beperkt aantal" en "bepaalde" – kunnen in de praktijk uiteenlopend worden uitgelegd.
Ook roept de formulering die de Hoge Raad gebruikt voor wanneer er in elk geval sprake kan zijn van een meer dan geringe inbreuk vragen op: "in het bijzonder (...) wanneer het gaat om onderzoek van alle in de elektronische gegevensdrager of het geautomatiseerde werk opgeslagen of beschikbare gegevens met gebruikmaking van technische hulpmiddelen".[62] Het lijkt ons wel een *voldoende* voorwaarde voor een meer dan geringe inbreuk dat *alle* gegevens *geautomatiseerd* worden doorzocht, maar zeker geen *noodzakelijke* voorwaarde. Ook bij handmatig zoeken in bijvoorbeeld alle foto's op een smartphone, of bij het geautomatiseerd doorzoeken van alle WhatsApp-berichten op bepaalde (maar mogelijk tamelijk algemene) trefwoorden, lijkt ons al snel sprake te zijn van een meer dan geringe inbreuk. Het risico bestaat dat de rechtspraak de formule van het geautomatiseerd onderzoeken van alle gegevens te gemakkelijk zal hanteren om te betogen dat geen sprake is van een meer dan geringe inbreuk. Een ander risico is dat vooral wordt gekeken naar het resultaat, dat wil zeggen de uiteindelijk overgenomen en in het dossier terechtkomende gegevens, en niet zozeer naar alle zoekhandelingen die zijn voorafgegaan aan het vinden en overnemen van het resultaat. Als slechts één of enkele bestanden worden overgenomen, kan de rechter allicht snel concluderen dat uit die enkele bestanden geen min of meer volledig beeld ontstaat van bepaalde aspecten van verdachtes privéleven; dat wil echter niet per se zeggen dat het doorzoeken van de smartphone geen meer dan geringe inbreuk heeft opgeleverd. Wanneer een groter aantal bestanden handmatig wordt bekeken, of wanneer met vrij algemene zoektermen in bepaalde mappen of apps geautomatiseerd wordt gezocht, kan dusdanig veel informatie in beeld komen bij de opsporingsambtenaar dat er wel degelijk sprake is van een meer dan geringe privacy-inbreuk, ook als slechts enkele zoekresultaten relevant blijken en worden overgenomen. Op dit moment (medio 2018) is het nog onvoldoende duidelijk welke lijn(en) de rechtspraak post-smartphone-arrest gaat trekken. Wel lijkt ons duidelijk dat dit onderwerp niet geheel aan de jurisprudentie kan worden overgelaten en dat de wetgever een regeling moet treffen, die zowel het opsporingsbelang van (snel) in smartphones kunnen kijken als het belang van rechtsbescherming voldoende tegemoetkomt. Het zal nog de nodige jaren duren voor een

61 Zie Royer & Oerlemans 2017.
62 HR 4 april 2017, ECLI:NL:HR:2017:592, r.o. 3.4.

gemoderniseerd Wetboek van Strafvordering in werking kan treden; het valt te hopen dat de wetgever eerder duidelijkheid zal scheppen over de smartphone-problematiek. Wij onderstrepen daarbij de noodzaak bijzondere bescherming te geven aan gegevensdragers die naar hun aard veel en velerlei gegevens bevatten, door vooraf, tijdens het uitlezen en achteraf bij het onderzoeken van de gegevens extra wettelijke waarborgen te creëren.[63]

Specifieke aandachtspunten

Bij het onderzoek aan inbeslaggenomen gegevensdragers spelen nog enkele punten, die in het bestek van dit hoofdstuk slechts kort aangestipt kunnen worden. Ten eerste de vraag of, en zo ja in hoeverre, ook berichten die pas na inbeslagneming op de smartphone binnenkomen, nog onder het onderzoek aan een inbeslaggenomen voorwerp vallen. Strikt genomen kan dat niet de bedoeling van de regeling zijn: de doorzoekings- en beslagbevoegdheden gelden immers voor de toestand van plaatsen en voorwerpen zoals die op het moment van de zoeking en het beslag zijn. Het kan bijvoorbeeld niet de bedoeling zijn dat een doorzoeking van een woning nog een tijd wordt gerekt enkel en alleen om brieven of briefkaarten die de post nog moet bezorgen van de deurmat te kunnen meenemen. Zo ook zou een onderzoek aan een inbeslaggenomen smartphone niet mogen worden gerekt enkel en alleen om later binnenkomende berichten te kunnen opvangen; daarvoor is de regeling niet bedoeld. Wel kan worden betoogd dat bij een natuurlijke periode van onderzoek (niet elke smartphone zal immers in luttele minuten na beslag direct forensisch verantwoord kunnen worden onderzocht) binnenkomende berichten als onvoorziene bijvangst wel kunnen worden onderzocht en gebruikt voor het onderzoek. De scheidslijn tussen een natuurlijke en een gerekte periode is echter vaag en flexibel, en zal sterk van de omstandigheden afhangen. Ook hier is het wenselijk dat spoedig een wettelijke regeling wordt getroffen, aangezien deze situatie zich steeds meer zal voordoen.[64]

Een tweede aandachtspunt is de noodzaak een goede regeling te treffen omtrent de teruggave van de gegevensdragers of gegevens zelf, een beklagregeling en de bewaartermijn en vernietiging van de gegevens.[65] Voor de teruggave bestaat momenteel geen consistente lijn in de jurisprudentie. Het betreft een complexe problematiek, omdat het moeilijk zal zijn om voldoende tegemoet te komen aan zowel de belangen van betrokkenen om 'onschuldige' gegevens op inbeslaggenomen gegevensdragers terug te krijgen (als de drager zelf niet kan worden teruggegeven omdat deze bijvoorbeeld ook

63 Zie Koops, Conings & Verbruggen 2016, p. 77-82 en Royer & Oerlemans 2017.

64 Zie hierover ook Commissie-Koops 2018, p. 92-96. Vgl. Rb. Midden-Nederland 7 juni 2018, ECLI:NL:RBMNE:2018:2655, waarin de rechtbank oordeelt dat voor "onderzoek op een inbeslaggenomen telefoon naar berichten die zullen binnenkomen op het chatprogramma 'Telegram' (...) een beslissing van de rechter-commissaris op grond van artikel 101 Sv [is] vereist omdat deze berichten kunnen worden beschouwd als brieven die nog niet geopend zijn".

65 Zie bijvoorbeeld EHRM 17 januari 2017, nr. 27153/07 (*Cacuci en S.C. Virra & Cont Pad S.R.L. t. Roemenië*) en EHRM 14 maart 2013, nr. 24117/08 (*Bernh Larsen Holding AS e.a. t. Noorwegen*), paragraaf 165 e.v. en EHRM 19 januari 2017, nr. 63638/14 (*Posevini t. Bulgarije*), paragraaf 92. Vgl. HR 24 januari 2017, *NJ* 2017/228, m.nt. T. Kooijmans.

kinderporno bevat) als aan de belangen van politie en justitie om 'schuldige' gegevens(-dragers) aan het verkeer te onttrekken en om niet overbelast te worden met verzoeken tot teruggave van willekeurig welke 'onschuldige' bestanden. Niettemin hopen wij dat ook hier de wetgever binnen afzienbare tijd een adequate regeling treft.[66]

3.2.3 *De netwerkzoeking*

De netwerkzoeking is een opsporingsbevoegdheid die het mogelijk maakt computers in aanliggende netwerken tijdens een doorzoeking te doorzoeken. Via een netwerkzoeking kunnen bijvoorbeeld andere computers (zoals laptops, pc's en mediaspelers) die zijn aangesloten op een intranet worden doorzocht. Ook is het mogelijk tijdens een doorzoeking van een kantoorpand door middel van een netwerkzoeking bijvoorbeeld de mailserver van het bedrijf in een datacentrum te doorzoeken. De bevoegdheid zal vaker worden ingezet nu steeds meer burgers en bedrijven documenten en e-mail opslaan en verwerken in de cloud. Het idee achter de regeling van de bevoegdheid is dat voor die extra doorzoeking niet nog eens een aparte inbeslagname- of doorzoekingsbevoegdheid behoeft te worden ingezet. De netwerkzoeking is wel beperkt tot extern opgeslagen gegevens "die redelijkerwijs nodig zijn om de waarheid aan de dag te brengen" (artikel 125j lid 1 Sv).
Ook geldt de beperking dat de netwerkzoeking niet verder mag reiken dan de externe systemen waartoe de reguliere gebruikers van de plek waar de doorzoeking plaatsvindt, gerechtigd zijn.[67] Uit de tamelijk ingewikkelde formulering van artikel 125j lid 2 Sv, waarin dit zogenoemde 'dubbele band-criterium' is vastgelegd, blijkt dat er zowel een feitelijke band moet bestaan tussen de persoon en de locatie waar de doorzoeking plaatsvindt (dus niet een netwerkzoeking vanaf de laptop van een toevallige bezoeker of de smartphone van een schoonmaker), als een juridische band (toestemming) tussen de persoon en de computer elders (dus geen netwerkzoeking in bijvoorbeeld gehackte computers, of in gedeelten van de externe server waar de gebruiker geen toegangsrechten voor heeft).
De opsporingsbevoegdheid mag alleen worden toegepast tijdens een doorzoeking van een plaats. De voorwaarden verschillen daarbij echter per locatie, wat een probleem oplevert qua rechtsbescherming van computers in besloten plaatsen, in het bijzonder de woning. Als een opsporingsambtenaar in een auto een laptop of smartphone aantreft, kan niet alleen dit apparaat worden onderzocht (wat, als in paragraaf 3.2.2 al gesteld, op zich al onvoldoende rechtsbescherming kent), maar ook met dit apparaat verbonden computers, zoals een computer in de woning van verdachte. Er bestaat hier een moeilijk te verdedigen verschil in behandeling tussen computers in de woning die bij een doorzoeking in de woning worden onderzocht, ten opzichte van dezelfde com-

66 Zie hierover Commissie-Koops 2018, p. 57-59, met verwijzing naar rechtspraak, waaronder Hof Den Haag 3 mei 2018, ECLI:NL:GHDHA:2018:1074, dat een beroep doet op EHRM-rechtspraak (onder andere EHRM 30 september 2014, nr. 8429/05 (*Prezhdarovi t. Bulgarije*), paragraaf 49-50).

67 *Kamerstukken II* 1989/90, 21551, 3, p. 27.

puters in de woning die worden onderzocht via een netwerkzoeking vanuit een in een voertuig of bedrijf aangetroffen apparaat.

Een substantieel probleem is de beperking van de zoekbevoegdheid tot de landsgrenzen, in verband met het territorialiteitsbeginsel: de Nederlandse justitie mag slechts netwerkzoeken in computers die zich in Nederland bevinden. Op internet of in de cloud is echter lang niet altijd duidelijk in welk land gegevens zich bevinden, en dus ook niet welk land om rechtshulp zou moeten worden gevraagd. In beginsel mag de netwerkzoeking zich echter niet uitstrekken tot computers indien redelijkerwijs bekend kan worden geacht dat deze zich in het buitenland bevinden, wat in het geval van een cloudzoeking vanuit Nederland al snel het geval zal zijn. Indien achteraf blijkt dat een netwerkzoeking desondanks plaatsvond buiten de landsgrenzen, zal gekeken moeten worden of de doorzoekende autoriteit redelijkerwijs mocht aannemen dat de computer zich in Nederland bevond; als dat zo is, zal het bewijs toch toelaatbaar kunnen zijn. Daarbij ligt het in de rede – vergelijkbaar met de bepaling over grensoverschrijdend tappen (zie paragraaf 3.4.5) – de buitenlandse staat in te lichten en om toestemming te vragen alvorens de gegevens als bewijs te gebruiken.
De orthodoxe interpretatie van het internationale recht zadelt de praktijk wel met grote problemen op, zodat het wenselijk is creatieve, verdedigbare alternatieve interpretaties te zoeken. In het kader van het project Modernisering Strafvordering is bijvoorbeeld gesteld dat de netwerkzoeking[68] ook kan strekken tot een doorzoeking van een webmailaccount (zoals Gmail) of een online opslagdienst (zoals Dropbox).[69] Dat is een meer vergaande toepassing van de netwerkzoeking dan oorspronkelijk in de jaren negentig werd voorgesteld.[70] Hoewel strikt genomen in strijd met het (huidige) internationale recht, valt er wel veel te zeggen voor een dergelijke hernieuwde interpretatie van het wetsartikel, vanuit het oogpunt dat opsporing in een digitale samenleving ook werkbaar moet zijn en met inachtneming van de nog immer trage procedures van internationale rechtshulp. Op dit vlak is dan ook veel in beweging; we verwijzen in dit verband verder naar hoofdstuk 4.

3.2.4 *Encryptie, toegangsbeveiliging en het bevel tot ongedaan maken van beveiliging*

De beveiliging van gegevens vormt een essentieel onderdeel van de bescherming van het maatschappelijk verkeer. Een van de doelstellingen van informatiebeveiliging is het waarborgen van de vertrouwelijkheid van gegevens. Dit kan op vele manieren worden bereikt, maar gaat vaak gepaard met gebruik van cryptografie, een van de belangrijkste technieken voor het verzekeren dat onbevoegden geen kennis kunnen nemen van ge-

68 Indien de inkijk in een Gmail-account zelfstandig, dus niet tijdens een doorzoeking, wordt ingezet, is sprake van een online doorzoeking. Dat is een toepassing van hacken als opsporingsbevoegdheid (zie paragraaf 3.7).
69 Zie p. 52-53 van de memorie van toelichting bij het Conceptwetsvoorstel Boek 2 (2017).
70 Zie over de netwerkzoeking en haar reikwijdte ook Conings & Oerlemans 2013.

gevens.[71] Bij gebruikmaking van cryptografie worden gegevens – kort gezegd – door middel van een wiskundig algoritme omkeerbaar onleesbaar gemaakt. Met behulp van een sleutel kunnen gegevens weer leesbaar worden gemaakt.[72]
Het gebruik van cryptografie levert echt problemen op voor opsporings- en nationale veiligheidsinstanties bij het aftappen van telecommunicatie (gegevens in transport) en het doen van onderzoek in computers (gegevens in opslag). Bij versleuteling van gegevens in opslag kan het gehele apparaat, een harde schijf of een individueel bestand versleuteld zijn. Via internet is gratis versleutelsoftware verkrijgbaar. Deze versleuteling is in potentie zeer sterk, waarbij het moeilijk zo niet onmogelijk is de bestanden te kraken.[73] Ook de versleuteling van de laatste modellen van populaire smartphones met alle geïnstalleerde updates is zeer moeizaam te kraken.[74]

Het bevel tot ongedaan maken van beveiliging
Bij de Wet computercriminaliteit werd al voorzien dat het bij een doorzoeking regelmatig zal voorkomen dat een computer beveiligd is. De doorzoekende autoriteit kan daarom degene van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van beveiliging bevelen toegang te verschaffen tot de desbetreffende computer (artikel 125k lid 1 Sv). Dit kan door zelf de computer te ontsluiten, of – desgevraagd – door de kennis (het wachtwoord) ter beschikking te stellen. Evenzo kan een bevel tot toegankelijk maken van de gegevens gericht worden aan eenieder van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van versleuteling van deze gegevens (artikel 125k lid 2 Sv).[75] De geadresseerde van een bevel ex artikel 125k Sv is daarbij tot geheimhouding verplicht (artikel 125m lid 5 Sv, ingevoerd bij Wet computercriminaliteit III). Een opzettelijke weigering mee te werken is strafbaar met maximaal drie maanden gevangenisstraf (artikel 184 Sr).
Tot 1 september 2006 kon het toegangsbevel worden gegeven *bij* een doorzoeking of een netwerkzoeking. 'Bij' een doorzoeking betekende dat het bevel alleen tijdens de doorzoeking gegeven zou kunnen worden, terwijl in de praktijk veelal computers in beslag genomen worden om later in alle rust en zorgvuldigheid onderzocht te worden. Daarom heeft de Wet computercriminaliteit II de bepaling aangepast: de bevoegdheid is nu mogelijk "indien toepassing is gegeven aan artikel 125i of artikel 125j", dus bij een doorzoeking ter vastlegging van gegevens of een netwerkzoeking. Bij een traditionale doorzoeking ter inbeslagneming – waar evengoed beveiligde computers en gegevensdragers zullen worden aangetroffen, die niet zelden in beslag worden genomen – kan de bevoegdheid nu echter niet meer worden toegepast, als niet tegelijkertijd ook een machtiging tot doorzoeking ter vastlegging van gegevens is afgegeven (wat in de prak-

71 Zie over het belang van cryptografie bijvoorbeeld Kaye 2015 en Arnbak 2016.
72 De gegevens worden omgezet in '*plain text*'.
73 Zie *Kamerstukken II* 2015/16, 34372, 3, p. 7-8. Zie ook Europol 2015a, p. 69.
74 Zie in dat kader bijvoorbeeld Leo Kelion, 'Israel's Cellebrite linked to FBI's iPhone hack attempt', *BBC News*, 23 maart 2016.
75 Dit is een ongelukkige formulering. Veel cryptosystemen werken met een sleutelpaar, waarbij de ene sleutel vérsleutelt en de andere sleutel óntsleutelt. Wie kennis heeft van de wijze van vérsleuteling heeft in principe niet de sleutel tot ontsleuteling (en omgekeerd).

tijk overigens standaard lijkt te gebeuren). Het is de vraag of de wetgever dat bedoeld heeft, maar de wettekst laat moeilijk een andere lezing toe.
De reikwijdte van artikel 125k kent nog meer grenzen: justitie kan ook buiten een doorzoeking in bezit komen van beveiligde computers of beveiligde gegevens, bijvoorbeeld wanneer de rechter-commissaris een laptop in beslag neemt, (artikel 104 Sv) of wanneer iemand de verdachte aanhoudt en een gestolen smartphone in beslag neemt (artikel 95, eerste lid, Sv). Is het niet wenselijk om ook in dergelijke gevallen een ongedaanmakingsbevel te kunnen geven? Zoals het algemeen geredigeerde artikel 125l Sv (over verschoningsgerechtigden) spreekt over "onderzoek in een geautomatiseerd werk", zo lijkt het raadzaam ook artikel 125k uit te breiden tot elk computeronderzoek, zeker nu beveiliging van computers gemeengoed is geworden.[76] Hetzelfde geldt overigens voor artikel 125n, de bepaling over vernietiging en bewaring van gegevens, dat ook niet alle mogelijke gevallen van computeronderzoek beslaat.

Ontsleutelbevel aan verdachte?
Het bevel wordt, vanwege het nemo-tenetur-beginsel, niet aan verdachte gegeven, en de personen bedoeld in artikel 217-219 Sv kunnen zich verschonen (artikel 125k lid 3 jo. 96a lid 3 Sv).[77] Dat levert een forse beperking op, omdat in veel gevallen de verdachte de enige zal zijn die een apparaat kan ontsluiten of bestanden kan ontsleutelen.
In zowel het concept van de Wet computercriminaliteit II als de Wet computercriminaliteit III is het onderwerp van discussie geweest of het ontsleutelbevel ook afgegeven moet kunnen worden aan de verdachte, op straffe van een gevangenisstraf.[78] Beide keren vond de regering de maatregel uiteindelijk niet wenselijk,[79] mede omdat iemand dwingen een sleutel af te geven te zeer op gespannen voet staat met het beginsel niet mee te hoeven werken aan de eigen veroordeling. Wat ons betreft is de discussie over een ontsleutelplicht over verdachten terecht afgesloten; er zijn te veel nadelen aan verbonden om een voldoende gesanctioneerde plicht wettelijk vorm te geven, en er zijn meer aanvaardbare alternatieven voorhanden. Eén daarvan is het onderscheppen van wachtwoorden of onversleutelde gegevens door de nieuwe bevoegdheid tot hacken (paragraaf 3.7). Ook kan onder bijzondere omstandigheden de weigering om bestanden, een harde schijf of een gegevensdrager te ontsleutelen wel eens tot *strafverzwaring* leiden, wanneer op de computer van de verdachte in reeds ontsleutelde delen van de computer bestanden met kinderporno worden gevonden en geen (begin van een) aannemelijke verklaring bestaat voor de aanwezigheid van versleutelde bestanden die de

76 De Tweede Kamer heeft dit punt voorgelegd aan de minister, *Kamerstukken II* 2000/01, 26671, 6, p. 11 en 24, maar daarop is deze in de Memorie van Antwoord, *Kamerstukken II* 2004/05, 26671, 10, niet ingegaan.
77 Hoewel artikel 125k lid 3 alleen zegt dat het bevel "bedoeld in het eerste lid" niet aan de verdachte mag worden gegeven, geldt dit ook voor het bevel in het tweede lid, nu dit het eerste lid – en dus inclusief de daarvoor geldende beperkingen – van overeenkomstige toepassing verklaart.
78 Zie hierover uitgebreid het WODC-onderzoek van Koops naar het ontsleutelbevel en het nemo tenetur-beginsel (Koops 2012b).
79 Zie *Kamerstukken II* 2015/16, 34372, 3, p. 5.

verdachte niet wil ontsluiten.[80] Ook kan wellicht, hoewel deze figuur in Nederland weinig voorkomt, immuniteit worden beloofd voor gebruik van ontsleutelde bestanden ten nadele van de verdachte, waarbij deze bestanden dan wel gebruikt kunnen worden in strafzaken tegen anderen of om bijvoorbeeld slachtoffers van kindermisbruik te identificeren.[81]
Een bijzonder geval, dat in de komende jaren waarschijnlijk relevanter wordt in de praktijk, is beveiliging door middel van *biometrie*. Het standpunt is verdedigbaar dat het wel mogelijk is met behulp van een vingerafdruk of irisscan een verdachte te dwingen om bijvoorbeeld een smartphone te ontgrendelen, omdat dit wilsonafhankelijk materiaal betreft.[82] De dwang moet uiteraard wel proportioneel zijn.

De 'Cryptowars' en cryptobeleid
De discussie over een ontsleutelplicht voor verdachten is onderdeel van een veel bredere beleidsdiscussie, die in de literatuur wordt aangeduid onder de noemer 'Cryptowars'. Al sinds het begin van de jaren negentig spreken opsporingsinstanties de verwachting uit dat de opsporing massaal onderuitgaat ('*going dark*') door crimineel cryptogebruik. Tijdens de eerste *Cryptowars* van halverwege de jaren negentig werden maatregelen voorgesteld als 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.[83] Varianten van deze voorstellen zijn in enkele landen geïmplementeerd, maar uiteindelijk (in elk geval in democratische rechtsstaten) op niets uitgelopen.[84]
Waar rond de eeuwwisseling nog kon worden gezegd dat misdadigers niet op grote schaal cryptografie gebruikten, moet dat beeld anno 2017 worden bijgesteld.[85] Cryptografie is immers zeer gebruiksvriendelijk geworden en standaard geïmplementeerd in veel apparaten en software. Er is geen bijzondere technische kennis noodzakelijk om gebruik te maken van dergelijke beveiligingsmaatregelen en inmiddels wordt het op grote schaal gebruikt. Sinds 2014 pleitten – in het bijzonder Amerikaanse – vertegenwoordigers van opsporingsinstanties voor de wettelijke verplichting handhavingsinstanties toegang te geven tot onversleutelde informatie. Een tweede *Cryptowars* 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 'achterdeur' in systemen moet worden gebouwd om de ver-

80 Zie Rb. Amsterdam 23 juli 2012, ECLI:NL:RBAMS:2012:BX2326, r.o. 8.3 (*Matthijs van der M.*-zaak). Vgl. Koops 2012b, p. 156-160.
81 Koops 2012b, p. 147-150.
82 Zie bijvoorbeeld Van Toor 2017 en Commissie-Koops 2018, p. 104-107. Zie ook Bruce 2017.
83 Zie uitgebreid Koops 1999 en Hoffman 1995.
84 Koops & Kosta 2018.
85 Zie bijvoorbeeld Europol (2015b), p. 50: "More than three-quarters of cybercrime investigations in the EU encountered the use of some form of encryption to protect data and/or frustrate forensic analysis of seized media" en Mevis, Verbaan & Salverda 2016, p. 58, die aangeven dat in hun onderzoek meer dan de helft van de respondenten aangeven dat versleuteling in opslag vaak een uitdaging vormt in opsporingsonderzoeken met betrekking tot alle typen misdrijven.

sleuteling ongedaan te kunnen maken. Dit maakt de ICT-infrastructuur echter inherent onveilig, omdat ook andere actoren misbruik kunnen maken van de achterdeur, zoals de autoriteiten van buitenlandse mogendheden en technisch vaardige misdadigers.[86]
Inmiddels (medio 2018) is de storm wat geluwd en lijkt er impliciet sprake te zijn van een (al dan niet langdurige) wapenstilstand in de *Cryptowars*. Koops en Kosta verklaren dit door twee factoren: beleidsmakers hebben mogelijk lering getrokken uit de eerste *Cryptowars* (die duidelijk maakten dat het inbouwen van achterdeuren een doodlopende beleidsweg is) en landen zijn hard bezig om hackbevoegdheden voor politie in te voeren, waarmee een meer op maat gesneden alternatief voorhanden is om in individuele gevallen encryptiesleutels te achterhalen dan het brute openzetten van een achterdeur bij alle cryptogebruikers.[87]
In dit verband willen wij erop wijzen dat het nog steeds in veel gevallen mogelijk is voldoende ander bewijsmateriaal te verzamelen; een zaak hoeft niet stuk te lopen op encryptie. Ook kan vaak toch een wachtwoord worden bemachtigd, omdat dit ergens is opgeschreven of de verdachte het vrijwillig afgeeft. Ten slotte is ook in sommige gevallen mogelijk een opgeslagen reservekopie van een telefoon of harde schijf bij een bedrijf te vorderen,[88] al stuit dat wel op de beperkingen van internationale rechtshulp.[89]

3.2.5 *Ontoegankelijkmaking*

In het systeem van de wet kunnen gegevens niet in beslag genomen worden, aangezien het geen goederen zijn.[90] Dat betekent dat de autoriteiten gegevens wel kunnen kopiëren ten behoeve van de waarheidsvinding, maar daarbij blijven de gegevens beschikbaar voor de betrokkene. Soms kan het echter ook wenselijk zijn om de gegevens aan diens beschikkingsmacht te onttrekken, bijvoorbeeld bij digitale kinderporno of kraakprogramma's (zoals men goederen ook in beslag kan nemen ter onttrekking aan het verkeer). Volgens artikel 19 lid 3 Cybercrimeverdrag moet daartoe ook een bevoegdheid bestaan. Hierin is voorzien door de Wet computercriminaliteit II.
Dit betreft de bevoegdheid van de officier van justitie of de rechter-commissaris om onrechtmatige gegevens die hij in het systeem aantreft ontoegankelijk te maken en te vernietigen (artikel 125o Sv). Het gaat om bij een onderzoek in een geautomatiseerd werk aangetroffen gegevens die voorwerp uitmaken van een strafbaar feit (bijvoorbeeld discriminatie, bedrijfsgeheimen) of met behulp waarvan een strafbaar feit is gepleegd (bijvoorbeeld een computervirus). Het artikel is van toepassing op situaties waarin bij een doorzoeking onrechtmatige gegevens worden aangetroffen. Indien

86 Zie bijvoorbeeld Bellovin e.a. 2013.
87 Koops en Kosta 2018.
88 Zie ook Paul Rosenzweig, 'iPhones, the FBI, and Going Dark', 4 augustus 2015. Beschikbaar op: https://www.lawfareblog.com/iphones-fbi-and-going-dark (laatst geraadpleegd op 1 juli 2018).
89 Zie *Kamerstukken II* 2015/16, 34372, 3, p. 9.
90 In het Conceptwetsvoorstel Boek 2 (2017) is wel voorgesteld 'beslag' op gegevens te kunnen leggen, maar dat voorstel is sterk bekritiseerd in de consultatie en zal naar verwachting niet terugkeren; zie bijvoorbeeld Vellinga-Schootstra 2017 en Commissie-Koops 2018, p. 80-83.

onrechtmatige gegevens publiekelijk toegankelijk worden aangetroffen op internet, kan de bevoegdheid tot ontoegankelijkmaking dus niet worden toegepast.[91] Daarvoor is de *notice-and-takedown*-bevoegdheid bedoeld (zie paragraaf 3.2.6).

De memorie van toelichting geeft als voorbeeld van een relevante situatie het in een mailbox aantreffen van racistische uitingen. Op zichzelf zijn racistische uitingen in een mailbox nog geen grond tot toepassing van de maatregel. Zulks is wel het geval als er een redelijk vermoeden is dat met die uitingen in de openbaarheid zal worden getreden.

Ontoegankelijk maken is het treffen van maatregelen om te voorkomen dat de beheerder of derden verder van die gegevens kennisnemen of gebruikmaken: de bestanden kunnen worden verwijderd (definitief gewist) met behoud van een kopie voor justitie, maar andere wegen zijn mogelijk (bijvoorbeeld door de gegevens via een encryptieprogramma 'op slot' te zetten). In uitzonderingsgevallen kan de bevoegde autoriteit een systeembeheerder om hulp vragen bij de ontoegankelijkmaking, bijvoorbeeld in netwerkomgevingen, om onnodige schade aan gegevens of systemen te voorkomen. De bevoegde autoriteit kan een derde slechts *verzoeken* om gegevens ontoegankelijk te maken; artikel 125o Sv impliceert dus geen medewerkings*plicht* voor systeembeheerders.[92]

Evenals bij de vastlegging van gegevens bij een doorzoeking bestaat er een notificatieplicht (artikel 125m Sv), en belanghebbenden kunnen zich met een klacht over de ontoegankelijkmaking wenden tot de raadkamer; zij kunnen zich ook beklagen over het opheffen van de ontoegankelijkmaking of het uitblijven van zulk opheffen als de rechter daartoe een last heeft gegeven (artikel 552a Sv). De rechter beslist bij de einduitspraak over de definitieve vernietiging of weer toegankelijkmaking van de gegevens (artikel 354 Sv). Dat veronderstelt dan wel dat er een einduitspraak komt, wat niet altijd het geval zal zijn; in die gevallen krijgt de voorlopige maatregel vanzelf een definitief karakter.

De ontoegankelijkmaking is beperkt tot situaties van onrechtmatige gegevens ("noodzakelijk is ter beëindiging van het strafbare feit of ter voorkoming van nieuwe strafbare feiten"). Wiemans heeft de nuttige suggestie gedaan ook gegevens ontoegankelijk te kunnen maken voor conservatoir beslag, aangezien gegevens in toenemende mate geldswaarde kunnen vertegenwoordigen. Gegevens zouden dan ook als verhaalsobject (vgl. artikel 94a-94b Sv) kunnen dienen voor een mogelijk op te leggen geldboete of ontneming van wederrechtelijk verkregen voordeel.[93] Inmiddels kan echter ook wel worden betoogd dat gegevens die direct een (al dan niet fluctuerende) geldswaarde vertegenwoordigen – denk aan cryptovaluta als bitcoins – in afwijking van de regel wel

91 In de Memorie van Toelichting wordt gesuggereerd dat de bevoegdheid ook mogelijk is wanneer op internet strafbare informatie wordt gevonden die onder Nederlandse rechtsmacht valt (*Kamerstukken II* 1998/99, 26671, 3, p. 51), maar later heeft de wetgever expliciet gezegd: "Het ontoegankelijk maken van gegevens is een maatregel die *onlosmakelijk verbonden* is met het doorzoeken van een geautomatiseerd werk" (*Kamerstukken I* 2005/06, 26671 en 30036, D, p. 8).

92 *Kamerstukken II* 1998/99, 26671, 3, p. 21; *Kamerstukken II* 2004/05, 26671, 10, p. 16.

93 Wiemans 2004a, p. 225.

als 'goed' kunnen worden behandeld, vergelijkbaar met giraal geld, en als zodanig in beslag kunnen worden genomen voor conservatoir beslag.[94]

3.2.6 *Notice-and-takedown*

Artikel 125p Sv

Zoals hiervoor vermeld, is de ontoegankelijkmaking van artikel 125o Sv beperkt tot doorzoekingen. Voor het offline halen van een website of het ontoegankelijk maken van gegevens die via internet worden aangeboden is, na veel vijven en zessen, de zelfstandige bevoegdheid van *notice-and-takedown* (NTD) ingevoerd in artikel 125p Sv. '*notice-and-takedown*' staat voor een procedure waarbij een partij in kennis wordt gesteld (de '*notice*') van onmiskenbaar onrechtmatig of strafbaar materiaal op een online bron met verzoek dit materiaal te verwijderen (de *takedown*).

GESCHIEDENIS

In Nederland bestaat al sinds 2008 een *Notice and Takedown*-gedragscode, waarbij openbare telecommunicatiedienstaanbieders die internetdiensten leveren op verzoek van een ieder onmiskenbaar strafbaar of onrechtmatig materiaal op basis van vrijwilligheid verwijderen.[95] Ook opsporingsambtenaren kunnen een verzoek doen op basis van de gedragscode. De gedragscode is in de praktijk effectief. Het ontbrak de politie en het Openbaar Ministerie echter aan een deugdelijke grondslag voor het *verplicht* verwijderen van strafbaar materiaal.[96]

Artikel 54a Sr (oud) werd in het verleden wel geacht te voorzien in de grondslag voor het afgeven van een bevel van de officier van justitie na een machtiging van een rechter-commissaris om strafbaar materiaal ontoegankelijk te maken. Tegelijkertijd werd in het artikel aangegeven dat de betrokken elektronische communicatiedienstverlener dan vrijgesteld is van vervolging. Deze grondslag is door verschillende rechtbanken en uiteindelijk de regering als ondeugdelijk bevonden.[97] Rechters-commissarissen weigerden toestemming te geven voor een NTD-bevel en in de zaken waarin de officier van justitie een NTD-bevel afgaf zonder een machtiging van de rechter-commissaris werd deze niet-ontvankelijk verklaard.

Bij de Wet computercriminaliteit III is artikel 125p Sv gecreëerd, omdat het voorziet in de *bevoegdheid* strafbare inhoud van internet te kunnen verwijderen. Een officier van justitie kan een ontoegankelijkmakingsbevel geven aan een aanbieder van een communicatiedienst binnen een opsporingsonderzoek naar de misdrijven omschreven in artikel 67, eerste lid Sv, nadat een machtiging van een rechter-commissaris is verkre-

94 Vgl. Royer 2016 over de behandeling van bitcoins naar Belgisch strafprocesrecht.
95 Zie de 'Gedragscode Notice-and-Take-Down', oktober 2008.
96 Zie ook *Kamerstukken II* 2015/16, 34372, 3, p. 57.
97 Zie Rb. Assen, 22 juli 2008, ECLI:NL:RBASS:2008:BD8451 en Hof Leeuwarden, 20 april 2004, ECLI:NL:GHLEE:2009:BI1645.

gen.[98] In het nader verslag wordt als voorbeeld gegeven dat het bevel ook kan worden ingezet om jihadistische propaganda tegen te gaan.[99]
Het bevel wordt pas ingezet als de elektronische communicatiedienstaanbieder geen opvolging geeft aan de vrijwillige NTD-gedragscode of niet bij deze code is aangesloten.[100] Bovendien moet de aanbieder van de rechter-commissaris de gelegenheid krijgen te worden gehoord, desgewenst in bijzijn van een raadspersoon (artikel 125p lid 4 Sv). Indien niet wordt voldaan aan het bevel, kan vervolging worden ingesteld voor het niet voldoen aan een bevoegd gegeven ambtelijk bevel (artikel 184 Sr) of voor het deelnemen aan of medeplegen van het gronddelict.[101] Als de officier van justitie en de betrokkene het niet met elkaar eens zijn, staat de beklagregeling in artikel 552a Sv open.[102]

Trapsgewijze inzet
In het kader van de proportionaliteits- en subsidiariteitstoets ligt het in de rede het *takedown*-bevel trapsgewijs in te zetten, te beginnen bij de *Notice and Takedown*-gedragscode.[103] Eerst moet daarbij de plaatser van het betwiste materiaal worden aangesproken het materiaal te verwijderen. Indien deze daar niet aan voldoet of niet aanspreekbaar is, kunnen de autoriteiten naar de websitehouder stappen. Als de websitehouder tevens weigert mee te werken aan het verwijderen van het (in deze context) strafbare materiaal, kunnen de autoriteiten zich tot de hostingaanbieder wenden. Een hostingaanbieder kan, als dat mogelijk is, de webpagina van een server ontoegankelijk maken. Het volledig offline halen van een volledig domein (bijvoorbeeld www.leidenuniv.nl) of een complete server ligt minder voor de hand, omdat zich daarop honderden of duizenden websites tegelijk kunnen bevinden en de ontoegankelijkmaking daardoor vermoedelijk niet meer proportioneel is. In uitzonderlijke gevallen kan het offline halen van een volledig domein of server wellicht aanvaardbaar zijn, als de r-c acht dat de belangen van de getroffen 'onschuldige' webpagina's niet opwegen tegen het belang van ontoegankelijkmaking van bepaald zeer ernstig materiaal en voor dat laatste geen lichtere alternatieven voorhanden zijn. Als laatste trap in de escalatieladder kan een (IP-)filterverplichting bij een internet-toegangsaanbieder worden opgelegd door de verplichting bepaalde IP-adressen te blokkeren.[104] Als – niet onomstreden – voorbeeld daarvan kan worden gewezen op het bevel van de civiele rechter (in eerste instantie) aan de providers Ziggo en XS4ALL om de domeinnamen en IP-adres-

98 In het conceptwetsvoorstel uit 2010 ontbrak de beperking tot het afgeven van het bevel bij slechts de meer ernstige misdrijven en een machtiging van de rechter-commissaris. Deze twee waarborgen zijn terecht noodzakelijk gebleken, gezien de ernstige inmenging in het recht op vrijheid van meningsuiting (en de toegang tot informatie als onderdeel daarvan) als gevolg van de toepassing van een *takedown*-bevel. Zie ook Oerlemans 2010 en Kus & Ten Voorde 2016.
99 *Kamerstukken II* 2016/17, 34372, 6, p. 8.
100 *Kamerstukken II* 2015/16, 34372, 3, p. 57.
101 Zie ook *Kamerstukken II* 2016/17, 34372, 6, p. 109.
102 *Kamerstukken II* 2015/16, 34372, 3, p. 59. Tegen de beschikking op het beklag staat voor zowel de klager als de officier van justitie beroep en cassatie open.
103 Zie ook Oerlemans 2017b.
104 Zie *Kamerstukken II* 2015/16, 34372, 3, p. 96.

sen van *The Pirate Bay* te blokkeren in 2012.[105] Door een filter is de website niet meer via hun normale internetverbinding bereikbaar voor abonnees van deze providers.[106]
Internetfilters staan op gespannen voet met de vrijheid van meningsuiting, zowel wat betreft de uitingsvrijheid van de afzenders als wat betreft het recht op garing van informatie van de ontvangers.[107] De blokkering van websites is problematisch als via – op zichzelf legale – websites een zeer kleine hoeveelheid illegaal materiaal wordt verspreid en de gehele website offline wordt gehaald, of wanneer het onduidelijk is of de beschikbaarstelling van het materiaal daadwerkelijk strafbaar is.[108] Meer principieel bedreigen internetfilters ook het idee dat via internet in principe alles genetwerkt en toegankelijk moet zijn.
Het is vooralsnog onduidelijk wat de gevolgen van de nieuwe bevoegdheid zijn. Een *de facto* nationale zwarte lijst van strafbare websites en online forums behoort onzes inziens op termijn wel tot de mogelijkheden, maar de effectiviteit van zo'n lijst zal hoe dan ook twijfelachtig zijn, vanwege de mogelijkheden blokkades en filters te omzeilen, en vanwege het hydra-effect[109] dat ontoegankelijk gemaakte pagina's veelal snel, en in veelvoud, elders de kop opsteken.

Toezicht op de takedown-bevoegdheid
Een punt van zorg betreft toezicht op de rechtmatigheid van de inzet van de *takedown*-bevoegdheid. Vooraf vindt een onafhankelijke toets van de rechter-commissaris plaats en bij de uitvoering van het bevel kan de betrokkene worden gehoord. Ook staat beklag open, waarmee de geadresseerde van een bevel onder andere de (vermeende) strafbaarheid van het materiaal kan betwisten (artikel 552a Sv).
De bedoeling is echter wel dat het *takedown*-bevel vooral als *voorlopige maatregel* wordt ingezet en dat de zittingsrechter het laatste woord heeft.[110] Wij vragen ons af of vervolging voor een strafbaar feit altijd wordt doorgezet als het materiaal eenmaal of-

105 Zie Rb. Den Haag 11 januari 2012, ECLI:NL:RBSGR:2012:BV0549. In hoger beroep oordeelde het Hof Den Haag (28 januari 2014, ECLI:NL:GHDHA:2014:88) dat de internetblokkade geen stand mocht houden, omdat deze eenvoudig te omzeilen was en daarmee niet effectief zou zijn. De Hoge Raad stelde prejudiciële vragen over de vermeende auteursrechtinbreuken van The Pirate Bay (HR 13 november 2015, ECLI:NL:HR:2015:3307). Het Hof van Justitie maakte duidelijk dat de The Pirate Bay met haar handelen inbreuk maakt op het auteursrecht van de rechthebbenden (HvJ EU 14 juni 2017, C-610/15, ECLI:EU:C:2017:456 (*Stichting Brein t. Ziggo B.V. & XS4ALL Internet BV*). De Hoge Raad heeft daarop de zaak terugverwezen naar het Hof Den Haag (HR 29 juni 2018, ECLI:NL:HR:2018:1046).

106 Internetgebruikers kunnen echter ook eenvoudig omzeilingsmaatregelen nemen, zoals het gebruik van een '*virtual private network*' (VPN)-verbinding.

107 Zie bijvoorbeeld EHRM 18 december 2012 (*Yildirim t. Turkije*), nr. 3111/10, *NJ* 2014/320, m.nt. E.J. Dommering en EHRM 1 december 2015 (*Cengiz t. Turkije*), nrs. 48226/10 en 14027/11), *NJ* 2016/337, m.nt. E.J. Dommering.

108 Zie ook Schellekens, Koops & Teepe 2007, p. 13-14. Op p. 22 van de memorie van toelichting op het wetsvoorstel Versterking bestrijding computercriminaliteit uit 2010 wordt terecht opgemerkt dat de vraag of materiaal op internet strafbaar is niet altijd eenvoudig te beantwoorden is.

109 Ook wel het 'Streisand-effect' genoemd, naar de grote media-aandacht die ontstond toen Barbra Streisand foto's van haar villa in Malibu wilde verwijderen. Zie https://en.wikipedia.org/wiki/Streisand_effect (laatst geraadpleegd 1 juli 2018).

110 *Kamerstukken II* 2015/16, 34372, 3, p. 59.

fline is gehaald.[111] Als de verdachte al te achterhalen is, is het maar de vraag of deze ook vervolgd kan worden; zeker bij inhoudsaanbieders uit het buitenland zal vervolging vaak achterwege blijven. Daarbij kent de beklagmogelijkheid een feitelijke beperking, doordat er geen notificatieplicht bestaat aan de inhoudsaanbieder van de verwijderde gegevens; degene die het materiaal had geplaatst moet er dus zelf achter zien te komen dat het materiaal is verwijderd, alvorens zich te kunnen beklagen. Tot slot wijzen wij erop dat de Inspectie Justitie en Veiligheid slechts een toezichtstaak heeft met betrekking tot de hackbevoegdheid, en dus niet ziet op het *takedown*-bevel. Aangezien deze bevoegdheid mogelijk wel grote gevolgen heeft, lijkt het ons van groot belang dat een sluitende regeling wordt getroffen die verzekert dat na ontoegankelijkmaking altijd een definitief oordeel wordt geveld over de strafbaarheid van het verwijderde materiaal en de proportionaliteit en subsidiariteit van de maatregel.

3.2.7 *Overzicht*

In onderstaande tabellen geven we een (samenvattend en niet-uitputtend) overzicht van de verschillende typen computeronderzoek, uitgesplitst naar de situaties van een doorzoeking (tabel 3.1) en situaties buiten de doorzoeking (tabel 3.2).

Opsporings-bevoegdheid	**Juridische basis**	**Voorwaarden (specifiek)**	**Voorwaarden (alg.)**	**Voorbeelden toepassing**
Doorzoeking vervoermiddel ter inbeslagneming van gegevensdragers	Art. 96b Sv	Opsporingsambtenaren, bij heterdaad of misdrijven zoals omschreven in art. 67, eerste lid Sv. Niet in woongedeelte voertuig	Geen onderzoek naar geheimhouderinformatie (art. 125l Sv) Notificatie (art. 125m Sv) Vernietiging niet relevante gegevens (art. 125n Sv)	Doorzoeken van auto ter inbeslagneming van fotogeheugenkaarten.
Doorzoeking woning of geheimhouderkantoor ter inbeslagneming van gegevensdragers	Art. 220 Sv	Rechter-Commissaris (ambtshalve of op vordering van officier van justitie), bij elk strafbaar feit. Geheimhouderkantoren alleen onder uitzonderlijke voorwaarden		Doorzoeken caravan ter inbeslagneming laptop; doorzoeking kantoor van verdachte notaris ter inbeslagneming desktop

111 Zie ook Oerlemans 2017c, p. 355.

Opsporings-bevoegdheid	Juridische basis	Voorwaarden (specifiek)	Voorwaarden (alg.)	Voorbeelden toepassing
Spoeddoorzoeking woning of geheim-houderkantoor ter inbeslagneming van gegevensdragers	Art. 97 Sv	Onderzoek door (hulp)officier van justitie, met machtiging rechter-commissa-ris, bij dringende noodzakelijkheid en misdrijven zoals omschreven in art. 67, eerste lid Sv		Indien, indien aannemelijk is dat bij uitstel gegevens verloren zullen gaan
Doorzoeking overige besloten plaatsen ter inbeslagneming van gegevensdragers	Art. 96c Sv	Bevel officier van justitie bij heterdaad of zoals omschreven in art. 67, eerste lid Sv. Spoeddoorzoeking mogelijk door hulpofficier van justitie, met machtiging (vooraf of achteraf) van officier.		Doorzoeken schuur ter inbeslagneming van externe harde schijven
Doorzoeking ter vastleggen van gegevens	Art. 125i jo. 96b e.v. Sv	Zelfde voorwaar-den als voor doorzoeking ter inbeslagneming (zie boven). Bij doorzoeking bij aanbieders van openbare communicatie: voorwaarden ter bescherming van inhoud (art. 125 1a Sv)		Doorzoeking woning om onderzoek te doen in desktop en tablet van verdachte

Opsporings-bevoegdheid	Juridische basis	Voorwaarden (specifiek)	Voorwaarden (alg.)	Voorbeelden toepassing
Netwerkzoeking	Art. 125j Sv	Zelfde voorwaarden als bij art. 125i Sv		Bij een doorzoeking ter vastlegging van gegevens veiligstellen van e-mails op een server die elders staat.
Onderzoek aan tijdens doorzoeking inbeslaggenomen gegevensdragers	Art. 94 Sv jo. art. 96b e.v. Sv	Ligt besloten in de voorwaarden voor de doorzoeking. Bij onderzoek in door opsporingsambtenaar zelfstandig inbeslaggenomen dragers: eventueel bevel of machtiging nodig conform smartphonearrest (par. 3.2.2)		Overnemen en onderzoeken van gegevens uit bij doorzoeking woning inbeslaggenomen harde schijf
Ontsleutelbevel	art. 125k Sv	Bij toepassing van doorzoeking ex art. 125i of 125j Sv. Bevel kan niet worden gegeven aan de verdachte		De (niet-verdachte) systeembeheerder bevelen de zelf aangebrachte versleuteling ongedaan te maken.
Ontoegankelijkmakingsbevel	art. 125o Sv	Door officier van justitie, in het kader van een doorzoeking, bij corpus delicti-gegevens		Ontoegankelijk maken van kinderpornografie aangetroffen in een computer tijdens een doorzoeking.

Tabel 3.1 Overzicht van de juridische basis voor computeronderzoek in het kader van doorzoeking

Opsporingsbevoegdheid	Juridische basis	Voorwaarden	Voorbeelden toepassing
Inbeslagneming van gegevensdragers bij aanhouding of staande-houding	Art. 95 jo. 52-54 Sv	Opsporingsambtenaar bij heterdaad of (op bevel van officier van justitie) bij misdrijven waarvoor voorlopige hechtenis is toegelaten	Inbeslagneming smartphone bij aanhouding
Inbeslagneming van gegevensdragers in overige gevallen	Art. 96 Art. 104 Sv	Opsporingsambtenaar, bij heterdaad of misdrijven zoals omschreven in art. 67, eerste lid Sv. Rechter-commissaris, in alle gevallen	Inbeslagneming USB-stick die wegrennende verdachte over een schutting heeft gegooid
Onderzoek aan (buiten doorzoeking) inbeslag-genomen gegevensdrager	Art. 94 jo. 95 en 96 Sv	Opsporingsambtenaar, conform smartphone-arrest (par. 3.2.2) al dan niet op bevel officier van justitie of met machti-ging van rechter-commissaris. Geen onderzoek naar geheimhouderinformatie (art. 125l Sv).	Bekijken door opsporingsambtenaar van laatste vijf genomen foto's bij heterdaad-aanhou-ding; geautomatiseerd doorzoeken met machtiging rechter-commissaris van gehele smartphone
'*Notice-and-takedown*'-bevel	125p Sv	Bevel officier van justitie, met machtiging rechter-commissaris, misdrijven zoals omschreven in art. 67, eerste lid Sv	Het offline laten halen van webpagina's met racistische inhoud

Tabel 3.2 Overzicht van de juridische basis voor computeronderzoek buiten situaties van doorzoeking

3.3 Het vorderen van gegevens

In deze paragraaf worden de opsporingsbevoegdheden tot het vorderen van gegevens besproken. Hiervoor bestaan twee wettelijke regimes: één voor de vordering aan communicatieaanbieders en één voor andere geadresseerden. We lichten eerst het algemene wettelijke kader voor het vorderen van gegevens toe (paragraaf 3.3.1). Daarna wordt het specifieke wettelijk kader voor het vorderen van vier typen gegevens besproken: gebruikersgegevens (paragraaf 3.3.2), verkeersgegevens (paragraaf 3.3.3), 'andere' gegevens (paragraaf 3.3.4) en communicatie-inhoudelijke gegevens (paragraaf 3.3.5). Tot slot komt de steunmaatregel van bevriezing aan bod (paragraaf 3.3.6).

3.3.1 *Het wettelijk stelsel voor het vorderen van gegevens*

Geschiedenis

Al in 1926 is een bevoegdheid ingevoerd tot het opvragen van inlichtingen over telefoonverkeer bij 'telephonie-instellingen' (artikel 100 lid 3 Sv-1926, artikel 125f Sv-1971). In 1996 heeft de Commissie-Van Traa in haar rapport aanbevolen opsporingsbevoegdheden te creëren in het Wetboek van Strafvordering voor het vorderen van gegevens bij derden door opsporingsdiensten.[112] Hiervoor zijn aparte bevoegdheden nodig naast de traditionele bevoegdheden voor een uitleveringsbevel, omdat gegevens geen 'goed' zijn en dus niet op basis van artikel 96a of 105 Sv (het bevel tot uitlevering van een voorwerp) kunnen worden gevorderd. De aanbevelingen van de Commissie-Mevis uit 2001 (Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij) hebben uiteindelijk geleid tot de Wet vorderen gegevens telecommunicatie in 2004[113] en de Wet vorderen gegevens in 2005.[114] De Wet computercriminaliteit II veranderde op 1 september 2006 'telecommunicatie' in 'communicatiediensten' en verving de definitie van telecommunicatiegebruiker, maar liet overigens de bevoegdheden ongewijzigd.

Vóór 2005 moest de gegevenshouder zelf een afweging maken tussen de belangen van de betrokkene en die van justitie, op basis van artikel 8 onder e jo. artikel 43 Wet bescherming persoonsgegevens.[115] In de praktijk bood de wetgeving weinig mogelijkheden; het werd bovendien onwenselijk geacht dat justitie afhankelijk was van de vrijwillige medewerking van derden. Daarom is een regime voor gegevensvorderingen ingevoerd, dat bedoeld is als een 'sluitend' stelsel: gegevens moeten binnen dit kader worden verkregen.[116] Het is voor de politie dus niet meer toegestaan om vrijwillige afgifte van de gegevens te verzoeken. De Hoge Raad heeft in 2011 in een arrest bevestigd dat de politie gegevens *moet* vorderen.[117] Wel is het mogelijk dat een partij bij aangifte vrijwillig gegevens verstrekt (zoals logbestanden of ander bewijs dat zij zelf heeft verzameld).

Op de wetsvoorstellen voor het vorderen van gegevens is destijds enige kritiek gekomen, met name met betrekking tot het idee dat de voorstellen grotendeels waren ingegeven door de behoeften van de opsporing, waardoor zij een (veel) te ruime reikwijdte zouden hebben gekregen.[118] Ook is kritiek geuit op "het slaafs volgen van de technische

112 *Kamerstukken II* 1995/96, 24072, 11, p. 466.
113 *Stb.* 2004, 105.
114 *Stb*. 2005, 390. De Wet vorderen gegevens bij financiële instellingen werd in 2004 van kracht (*Stb.* 2004, 109), maar deze werd vervolgens in de Wet vorderen gegevens geïncorporeerd.
115 Zie Mac Gillavry 2004, die het oude en nieuwe stelsel kritisch onderzocht en rechtsvergelijking uitvoerde met het stelsel voor het vorderen van gegevens in andere staten.
116 *Kamerstukken II* 2003/04, 29441, 3, p. 3 en 17.
117 HR 21 december 2010, ECLI:NL:HR:2010:BL7688.
118 Zie bijvoorbeeld de bronnen vermeld in *Kamerstukken II* 2001/02, 28366, 1, p. 5 (onder andere Mac Gillavry 2004) en Stevens, Koops & Wiemans 2004 en daarin aangehaalde literatuur van Dommering, Kuitenbrouwer en Prins.

mogelijkheden waar het kabinet blijk van geeft".[119] Onder meer de omstandigheden dat hele bestanden kunnen worden opgevraagd en dat ook het opvragen van individuele gegevens met langdurige heimelijkheid gepaard kan gaan, roepen vragen op. Een evaluatie van de wet in 2011 heeft echter niet tot wijzingen geleid.[120] Bij de bespreking van de bevoegdheden voor het vorderen van gegevens moet in het achterhoofd worden gehouden dat men bij alle vorderingen *altijd* moeten nagaan of de vordering proportioneel is (wordt er niet meer gevraagd dan noodzakelijk?) en subsidiair is (zijn er minder ingrijpende alternatieven om de benodigde informatie te verkrijgen beschikbaar?).

Complexiteit van het wettelijk stelsel

Het stelsel van het vorderen van gegevens door de Nederlandse politie en justitie is complex. De reden is dat er *twee* juridische raamwerken voor het vorderen van gegevens in het Wetboek van Strafvordering gelden. Enerzijds kunnen er gegevens worden gevorderd (1) bij aanbieders van elektronische communicatiediensten en anderzijds (2) bij *een ieder*, zoals een persoon, bedrijf, of instelling.[121] Wij hebben beiden beargumenteerd dat deze tweedeling onnodig en ongewenst is, omdat het onduidelijkheid geeft over de toepasselijke bevoegdheden, terwijl de voorwaarden voor de toepassing van de vorderingen nagenoeg hetzelfde zijn.[122] Veel beter kan voor één regime voor het vorderen van gegevens worden gekozen. In het kader van Modernisering Strafvordering is aangegeven dat men voornemens is slechts één regime aan te houden.[123] Dat blijkt makkelijker gezegd dan gedaan, omdat bepaalde onderdelen specifiek zijn voor de communicatiecontext, zoals de bestandsanalyse (zie paragraaf 3.3.2) en de onverwijlde gedeeltelijke verstrekking van verkeersgegevens.[124] Het tweeledige regime roept afbakeningsvragen op, bijvoorbeeld onder welk regime het vorderen van gegevens bij online dienstaanbieders valt. In de regel zullen online dienstaanbieders bestempeld kunnen worden als elektronische communicatiediensten.[125] Internet-toegangsaanbieders, VPN-diensten, sociale-mediadiensten en online forums verlenen bijvoorbeeld elektronische communicatiediensten. Twijfel kan bestaan over bijvoorbeeld hostingaanbieders en cloud-dienstverleners die primair opslagdiensten aanbieden; ook daarvan wordt aangenomen dat het bijna altijd elektronische communicatiediensten zullen zijn.[126] Dat zal anders liggen als de lijn van het conceptwetsvoorstel Boek 2 (februari

119 Koops 2003b, die een passage uit het kabinetsstandpunt aldus samenvat: "Met andere woorden: omdat de technische mogelijkheden een opsporingsbehoefte kweken, moet de wetgever aan die behoefte voldoen".
120 Zie Spapens, Siesling & De Feijter 2011.
121 Voor het vorderen van gegevens bij geheimhouders of verschoningsgerechtigden gelden bijzondere regels. Deze worden in deze paragraaf niet behandeld.
122 Zie Koops 2003, p. 119-120 en Oerlemans 2017a, p. 205.
123 Zie p. 84 van de brief van 30 september 2015 over het project modernisering strafvordering.
124 Zie Commissie-Koops 2018, p. 123-128.
125 Zie ook Koops e.a. 2012b, p. 42.
126 Deze zienswijze is recentelijk bevestigd in Rb. Overijssel 1 februari 2017, ECLI:NL:RBOVE:2017:417, *Computerrecht* 2017/52, m.nt. J.J. Oerlemans. In het geval een dienstaanbieder toch geen elektronische communicatiedienst blijkt te betreffen, kan altijd een vordering uit het andere regime worden ingezet, zie paragraaf 2.3 van de Aanwijzing bijzondere opsporingsbevoegdheden. Zie ook *Kamerstukken II* 2003/04, 29441, 3, p. 13-14.

2017) wordt aangehouden, aangezien daarin blijkens de toelichting de categorie elektronische communicatieaanbieders beperkt is tot de aanbieders die communicatie als hoofdactiviteit aanbieden,[127] wat naar men mag aannemen als zodanig geen hostingaanbieders omvat.

3.3.2 *Vorderen van identificerende en gebruikersgegevens*

Onder het *algemene regime* kunnen identificerende gegevens bij elk misdrijf door elke opsporingsambtenaar worden gevorderd, mits het gaat om gegevens die niet voor persoonlijk gebruik worden verwerkt (artikel 126nc Sv). Identificerende gegevens zijn NAW-gegevens, geboortedatum en geslacht, en administratieve kenmerken, zoals klantnummers of bankrekeningnummers. Voor rechtspersonen zijn dit naam, adres, postadres, rechtsvorm en vestigingsplaats.[128]
Onder het *communicatieregime* worden onder gebruikersgegevens de volgende typen gegevens verstaan: (1) naam; (2) adres; (3) postcode; (4) woonplaats; (5) nummer; en (6) type dienst van een gebruiker van een communicatiedienst (artikel 126na Sv). Uit de memorie van toelichting wordt duidelijk dat met de categorie 'nummers' ook e-mailadressen en IP-adressen worden bedoeld.[129] Gebruikersgegevens kunnen door opsporingsambtenaren worden gevorderd in opsporingsonderzoeken naar elk misdrijf. De bevoegdheid wordt zeer veel gebruikt, omdat gebruikersgegevens kunnen leiden tot identificatie van een verdachte, en veelal ook nodig zullen zijn om andere bevoegdheden, zoals het vorderen van verkeersgegevens, te kunnen inzetten.[130]
Opsporingsambtenaren kunnen gebruikersgegevens geautomatiseerd raadplegen via het Centraal informatiepunt onderzoek telecommunicatie (het CIOT). Op basis van het Besluit verstrekking gegevens telecommunicatie moeten aanbieders elke 24 uur een actueel overzicht van gebruikersgegevens beschikbaar stellen.[131] Sinds 1 september 2007 zijn ook internetaanbieders wettelijk verplicht gebruikersgegevens via het CIOT beschikbaar te stellen (artikel 11 van het besluit).
Het opvragen van gebruikersgegevens loopt echter stuk wanneer de gebruiker vooruitbetaalde kaarten gebruikt (prepaidkaarten) – de telecomaanbieder weet dan immers niet welke NAW-gegevens bij een telefoonkaart (simkaart) horen. Waar in de tweede helft van de jaren negentig nog een registratieplicht werd overwogen, is uiteindelijk gekozen voor twee alternatieve mogelijkheden. De eerste oplossing is een bestandsanalyse door een telecomaanbieder, waarbij hij door analyse van zijn gegevensbestanden het benodigde aansluitnummer van de mobiele telefoon kan achterhalen (artikel 126na lid 2 Sv). Dit gaat als volgt. Wanneer justitie de af te tappen persoon op minstens twee

127 Concept-memorie van toelichting bij het wetsvoorstel voor Boek 2 (februari 2017), p. 99.
128 De clausule voor rechtspersonen is aangepast door de Reparatiewet II Justitie, *Stb.* 2006, 24, inwerkingtreding 1 februari 2006.
129 *Kamerstukken II* 2001/02, 28059, 3, p. 11.
130 Zie ook Oerlemans 2017a, p. 27-30 over het belang van de opsporingsbevoegdheid voor de identificatie van verdachten in cybercrime-onderzoeken.
131 Besluit van 26 januari 2000, *Stb.* 2000, 71, inwerkingtreding 1 september 2004 (*Stb.* 2004, 411).

verschillende tijdstippen heeft geobserveerd als mobiel bellend, kan zij aan de aanbieder doorgeven op welke tijdstippen op welke locaties door een toestel gebeld is. De aanbieder kan vervolgens in zijn bestand achterhalen welk nummer in al deze gevallen belde – dat zal bijna altijd slechts één nummer zijn. In sommige gevallen (op plaatsen of tijdstippen waar weinig mobiel wordt gebeld, of wanneer justitie weet met wie de persoon belde) kan zelfs worden volstaan met één observatie van tijdstip en locatie. Aldus kan de aanbieder in beginsel in een kwartiertje het gevraagde nummer achterhalen.[132] Deze verplichting van de aanbieder is vastgelegd in artikel 13.4 lid 3 Tw, waarbij ook een bewaarplicht is ingevoerd: de aanbieder van mobiele telecommunicatie moe(s)t gedurende twaalf maanden[133] de gegevens over tijdstip, nummer en basisstation bewaren.[134] De bewaarplicht geldt (of gold) alleen voor zover deze gegevens worden verwerkt door de telecomaanbieder; hij hoeft ze niet te vergaren als hij ze zelf niet verwerkt. De juridische status van artikel 13.4 lid 3 Tw is echter onduidelijk, in het licht van de ongeldigverklaring van de dataretentierichtlijn waarop deze was gebaseerd en de gevoegde HvJ EU-zaken *Tele2* en *Watson*,[135] die de minister aanleiding gaven de aanhangige herstelwet bewaarplicht[136] opnieuw te herzien. Het voornemen is nu de bewaarplicht te beperken tot gebruikersgegevens.[137] Dit betekent dat de verplichting (enkel die) gegevens te bewaren die nodig zijn voor een bestandsanalyse als bedoeld in artikel 126na lid 2 Sv, vermoedelijk gehandhaafd zal blijven.

De tweede mogelijkheid is met de inzet van de zogenoemde 'IMSI-catcher'. In dat geval wordt in de buurt van de geobserveerde verdachte een zender in de lucht gebracht die zich als basisstation voordoet; de gezochte mobiele telefoon van de verdachte meldt zich dan aan bij de IMSI-catcher, denkend dat deze een basisstation is voor toegang tot het netwerk. Bij de aanmelding geeft de telefoon automatisch zijn aansluitnummer (IMSI-nummer) prijs. Omdat deze tweede mogelijkheid ingrijpt in het normale frequentiegebruik, wordt dit gezien als een zwaardere methode dan de eerste.[138] In een arrest over de rechtmatigheid van de inzet van de IMSI-catcher in 2014, achtte de Hoge Raad de inzet van de IMSI-catcher rechtmatig vanwege de kennelijk korte duur van de inzet van het apparaat waarvoor toestemming was gegeven door de officier van justitie.[139]

---

132 Zie de toelichting in het Besluit bijzondere vergaring nummergegevens telecommunicatie, *Stb.* 2002, 31, p. 14-15.

133 Dit was drie maanden, maar de termijn is bij de Wet bewaarplicht verkeersgegevens verlengd tot twaalf maanden, *Stb*. 2009, 333.

134 Artikel 13.4 lid 3 (lid 2-oud) Telecommunicatiewet jo. artikel 7 Besluit bijzondere vergaring nummergegevens telecommunicatie, *Stb.* 2002, 31, van kracht sinds 1 maart 2002.

135 HvJ EU 21 december 2016, C-203/15 en C-698/15, ECLI:EU:C:2016:970 (*Tele2 Sverige AB t. Post- och telestyrelsen* en *Secretary of State for the Home Department t. Tom Watson e.a.*).

136 *Kamerstukken II* 2015/16, 34537, 1-3.

137 *Kamerstukken I* 2017/18, 32317, IU, p. 5, met verwijzingen naar de Europeesrechtelijke ontwikkelingen.

138 Zie over het probleem, de registratieplicht en de technische oplossingen de toelichting in *Kamerstukken II* 1997/98, 25533, 8, p. 10-12. Merk op dat de IMSI-catcher niet dient om verkeersgegevens te vergaren; het gaat om het verkrijgen van de (NAW- en nummer)gegevens die nodig zijn om verkeersgegevens te kunnen opvragen of een tap te kunnen plaatsen. *Kamerstukken I* 1998/99, 25533, 11a, p. 4.

139 HR 1 juli 2014, ECLI:NL:HR:2014:1562, *NJ* 2015/114, m.nt. P.H.P.H.M.C. van Kempen. Zie ook Ashouwer & Geurts 2017.

De mogelijkheid een IMSI-catcher in te zetten is opgenomen in artikel 3.22 (voorheen artikel 3.10 lid 4) Tw en is later aangevuld met een expliciete bevoegdheid in artikel 126nb Sv.[140] De IMSI-catcher en de opsporingsambtenaar die deze inzet uitvoert, moeten voldoen aan de eisen van het Besluit technische hulpmiddelen strafvordering.[141]

3.3.3 *Vorderen van verkeersgegevens*

De tweede categorie onder het communicatieregime betreft verkeersgegevens, dat wil zeggen gegevens over de (1) tijd, (2) duur, (3) gebruikte apparatuur, (4) afgenomen diensten en (5) de locatie van het netwerkaansluitpunt bij een communicatie of van de geografische positie van de randapparatuur van een gebruiker.[142] De gegevens worden onderscheiden van 'inhoudelijke gegevens', zoals de inhoud van een e-mailbericht.[143]
Verkeersgegevens kunnen op grond van artikel 126n Sv worden gevorderd, op bevel van officier van justitie en in opsporingsonderzoeken naar misdrijven zoals omschreven in artikel 67, eerste lid Sv. Met de vordering in artikel 126n Sv kunnen overigens ook gebruikersgegevens worden gevorderd.
In opsporingsonderzoeken worden verkeersgegevens veelvuldig gevorderd om na te gaan met wie de verdachte heeft gebeld (en daarmee zijn sociale omgeving in kaart te brengen) en teneinde de locatie van de verdachte of andere betrokkenen in een opsporingsonderzoek vast te stellen.[144] Deze laatste toepassing is steeds belangrijker geworden, en vergt daarmee aparte aandacht (zie paragraaf 3.6.2 over locatiebepaling). Verkeersgegevens kunnen echter 'vluchtig' zijn; om zeker te stellen dat gevorderde verkeersgegevens daadwerkelijk kunnen worden geleverd, kan een bevriezingsbevel worden gegeven (zie daarover paragraaf 3.3.6). Voor verkeersgegevens gelden daarbij nog aanvullende eisen: de veiliggestelde verkeersgegevens moeten beschikbaar zijn onafhankelijk van het aantal dienstaanbieders die de communicatie hebben vervoerd, en bovendien moeten onverwijld aan justitie voldoende verkeersgegevens doorgegeven kunnen worden opdat die het gevolgde of te volgen pad van de communicatie verder kan traceren (artikel 17 Cybercrimeverdrag). Lid 2 van artikel 126ni Sv bevat daartoe de bepaling dat aanbieders van communicatiediensten verplicht zijn zo spoedig mogelijk de gegevens te verschaffen die nodig zijn om de identiteit te achterhalen van andere aanbieders van wier dienst bij de communicatie gebruik is gemaakt.

---

140 Bij wet van 5 april 2001, *Stb.* 180 (in artikel 126na-oud Sv, vernummerd door de Wet vorderen gegevens telecommunicatie tot 126nb Sv). Zie ook het Aanwijzingsbesluit en de Vrijstellingsregeling afwijkend gebruik frequentieruimte Justitie, *Stcrt.* 2006, 37.

141 *Stb.* 2006, 524. Sinds Besluit van 19 mei 2017, *Stb*. 2017, 265, kunnen ook FIOD-ambtenaren IMSI-catchers inzetten. Zie ook Wet van 15 juni 2018, *Stb.* 2018, 228 (Verzamelwet), waarin een verwijzing naar artikel 3.22 lid 4 Tw is openomen in artikel 126nb Sv.

142 In artikel 2 van het Besluit vorderen telecommunicatiegegevens zijn verkeersgegevens nader gespecifieerd die bij aanbieders van openbare aanbieders van telecommunicatienetwerken- en diensten kunnen worden gevorderd. Zie uitgebreid Koops & Smits 2014 over het onderscheid tussen verkeersgegevens en inhoudelijke gegevens.

143 Zie uitgebreid Koops & Smits 2014 over het soms problematische onderscheid tussen verkeersgegevens en inhoudelijke gegevens.

144 Zie uitgebreid Odinot e.a. 2013.

Bewaarplicht verkeersgegevens

Een tweede mogelijkheid om de vluchtigheid van digitale gegevens tegen te gaan, is een verplichting tot de opslag van verkeersgegevens in combinatie met gebruikersgegevens.[145] De Wet bewaarplicht telecommunicatiegegevens uit 2009 verplichtte in het verleden aanbieders van openbare telecommunicatiediensten en -netwerken om gebruikersgegevens en verkeersgegevens voor een bepaalde duur te bewaren, zodat ze op een later moment gevorderd konden worden door opsporingsdiensten.[146] Het bevriezingsbevel bood geen volwaardig alternatief voor een bewaarplicht, omdat bij een bevriezingsbevel *achteraf* de gegevens worden vastgesteld (ten tijde van het opsporingsonderzoek), in tegenstelling tot de bewaarplicht, waarbij gegevens *vooraf* worden veiliggesteld ten behoeve van de opsporing.[147] Hierbij moet overigens worden opgemerkt dat 'aanbieders van openbare telecommunicatiediensten en -netwerken' *niet hetzelfde* zijn als de 'aanbieders van elektronische communicatiediensten' tot wie vorderingen tot verstrekking van verkeersgegevens kunnen worden gericht; de bewaarplicht geldt voor een beperktere categorie (zie verder paragraaf 3.4.7).

De stevige privacy-inbreuk die de bewaarplicht en het vorderen van verkeersgegevens met zich meebrengt, heeft tot controverse en tot rechtszaken geleid. De Europese richtlijn voor de bewaarplicht is in 2014 ongeldig verklaard en de Nederlandse Wet bewaarplicht verkeersgegevens in 2015.[148] Met een wetsvoorstel aanpassing bewaarplicht telecommunicatiegegevens beoogde de wetgever de situatie te herstellen, met de sterkere waarborg van een machtiging van een rechter-commissaris (naast het bevel van een officier van justitie) voor het vorderen van verkeersgegevens.[149] Op 21 december 2016 heeft het Hof van Justitie echter geoordeeld dat de bewaarplicht als algemene maatregel op zichzelf disproportioneel is en beperkt moet zijn door "objectieve elementen".[150] De minister heeft aangegeven de bewaarplicht te beperken tot "een aangepaste regeling met betrekking tot uitsluitend gebruikersgegevens",[151] wat wij interpreteren als een beperking tot de gegevens die nodig zijn voor aanbieders om een bestandsanalyse te kunnen uitvoeren om een (onbekend prepaid-)nummer te achterhalen (zie paragraaf 3.3.2).

Veel telecommunicatiebedrijven bewaren overigens gegevens voor een periode van bijvoorbeeld zes maanden voor interne facturerings- en beveiligingsdoeleinden. In die zin kan justitie nog steeds gebruikmaken van de aanwezigheid van gegevens die bedrijven uit zichzelf bewaren, zoals dat ook het geval was voor de dataretentiewetgeving. De

145 Zie ook *Kamerstukken II* 2015/16, 34537, 3, p. 5-7.

146 Wet bewaarplicht telecommunicatiegegevens, *Stb.* 2009, nr. 333. De wet is gebaseerd op de Richtlijn van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG, *PubEU* L 105/54, 13.4.2006.

147 Zie ook Odinot e.a. 2013, p. 117.

148 Zie HvJ EU 8 april 2014, C-293/12 (*Digital Rights Ierland t. Ierland*) en C-594/12 (*Seitlinger, Tschohl e.a. t. Kärtner Landsregierung*) en Rb. Den Haag, 11 maart 2015, ECLI:NL:RBDHA:2015:2498.

149 Zie *Kamerstukken II* 2015/16, 34537, 2.

150 Zie HvJ EU 21 december 2016, C-203/15, ECLI:EU:C:2016:970 (*Tele2 Sverige AB t. Post-och telestyrelsen*).

151 *Kamerstukken I* 2017/18, 32317, IU, p. 5.

beschikbaarheid van deze gegevens in opsporingsonderzoeken is voor opsporingsdiensten echter niet verzekerd.

3.3.4 *Vorderen van 'gewone' en 'gevoelige' gegevens*

Het algemene vorderingsregime kent naast identificerende twee andere categorieën gegevens, die we bij gebrek aan wettelijke termen aanduiden als 'gewone' en 'gevoelige' gegevens. Met de vordering in artikel 126nd Sv kunnen 'gewone' gegevens worden gevorderd, nadat een bevel van een officier van justitie is verkregen. Dit geldt alleen voor opsporingsonderzoeken naar delicten zoals omschreven in artikel 67, eerste lid Sv. Bij lichtere strafbare feiten is de vordering ook mogelijk, maar dan heeft de officier voorafgaande machtiging van de rechter-commissaris nodig (artikel 126nd lid 6 Sv). Toekomstige gegevens kunnen worden opgevraagd onder dezelfde voorwaarden, voor een (telkens verlengbare) periode van vier weken. In dringende gevallen kan zelfs, met toestemming van de rechter-commissaris, worden gevorderd dat binnenkomende gegevens "direct na verwerking" (bijna realtime) of binnen een bepaalde periode worden verstrekt (artikel 126ne Sv). Het is onder omstandigheden denkbaar dat op grond van deze vordering het realtime doorgeven van bijvoorbeeld banktransacties van een klant wordt gevorderd.

Gevoelige gegevens
Als op voorhand redelijkerwijs te verwachten is dat de gezochte gegevens 'gevoelige' gegevens betreffen, dan moet een andere vordering worden gebruikt, conform artikel 126nf Sv. Gevoelige gegevens zijn de gegevens die in de wetgeving betreffende persoonsgegevensbescherming als "bijzondere categorieën" worden aangeduid: gegevens over geloofs- of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven en lidmaatschap van een vakbond.[152]
Gevoelige gegevens kunnen op grond van artikel 126nf Sv alleen worden verkregen met machtiging van een rechter-commissaris en wanneer het delict een 'ernstige inbreuk op de rechtsorde' oplevert. Het lijkt ons de vraag of een 'eenvoudige hack' of een kortdurende ddos-aanval op een weinig gebruikte webpagina de rechtsorde ernstig schokt. Wanneer aanvallen veel schade tot gevolg hebben of bijvoorbeeld vitale infrastructuren raken zal daar zeker wel sprake van zijn.
Van gevoelige gegevens kan bijvoorbeeld sprake zijn als op zoek wordt gegaan naar profielinformatie over religie of seksuele voorkeur of foto's van identificeerbare individuen (deze kunnen immers ras- en gezondheidsgegevens betreffen). Het arrest van de Hoge Raad waarin foto's (in casu foto's van OV-chipkaarten) als gevoelige gegevens werden gekwalificeerd (ook als niet beoogd wordt om ras- of medische informatie uit

152 Als bijzondere categorie waarvoor een machtiging van de rechter-commissaris is vereist, wordt mogelijk ook nog bronbescherming toegevoegd, zie *Kamerstukken I*, 2017/18, 34032, A (Wetsvoorstel bronbescherming in strafzaken).

de foto's af te leiden),[153] heeft veel discussie opgeleverd.[154] Het is niet verwonderlijk dat deze lijn in latere rechtspraak is genuanceerd, en dat wordt aangenomen dat foto's die niet als zodanig gekoppeld zijn aan individuen, (met name) camerabeeldgegevens, met de 126nd-vordering kunnen worden verkregen.[155]
Inmiddels is echter voor (bepaalde) camerabeelden ook een speciale regeling getroffen: beelden "gemaakt met camera's voor de beveiliging van goederen, gebouwen of personen" kunnen op basis van artikel 126nda door opsporingsambtenaren, zonder bevel van de officier of r-c-machtiging, worden gevorderd bij verdenking van misdrijven als omschreven in artikel 67, eerste lid Sv. De vordering mag mondeling worden gegeven, met opschriftstelling binnen drie dagen.[156] De beelden mogen echter geen gevoelige gegevens betreffen (artikel 126nda lid 2 Sv). Camerabeelden waaruit een hulpverleningsrelatie met een beroepsmatige verschoningsgerechtigde valt af te leiden, zoals de camerabeelden van de wachtruimte en toegangspaden tot een afdeling spoedeisende hulp, kunnen onder het verschoningsrecht vallen en hoeven dan niet (ook niet op basis van een 126nf-vordering) te worden geleverd.[157]

'Andere' gegevens bij communicatieaanbieders
Hoewel vorderingen aan communicatieaanbieders voornamelijk gebruikersgegevens, verkeersgegevens en communicatie-inhoud zullen betreffen, verwerken deze aanbieders ook andere gegevens. Daarvoor bevat artikel 126ng Sv een schakelbepaling in het communicatieregime, die aangeeft dat de vorderingen van het algemene regime ook kunnen worden gericht aan communicatieaanbieders als het 'andere' gegevens betreft dan gebruikersgegevens, verkeersgegevens of inhoudelijke gegevens. Het gaat bijvoorbeeld om registratiegegevens van gebruikers bij een website, of betalingsgegevens. Ook dergelijke gegevens kunnen essentieel zijn, omdat het een spoor kan opleveren met betrekking tot betalingsgegevens (inclusief transactiegegevens) van een verdachte. '*Follow the money*' is een strategie die ook in digitale opsporingsonderzoeken kan worden ingezet.[158]

3.3.5 *Vorderen van communicatie-inhoudelijke gegevens*

De categorie 'communicatie-inhoudelijke gegevens' betreft de inhoud van bij communicatieaanbieders opgeslagen berichten. De enigszins cryptische omschrijving hiervan in artikel 126ng lid 1 Sv – "gegevens die zijn opgeslagen in het geautomatiseerde werk van de aanbieder en niet voor deze bestemd of van deze afkomstig zijn" – ziet feitelijk op de inhoud van communicatie die onder het grondwettelijke telecommunicatiege-

153 HR 23 maart 2010, ECLI:NL:HR:2010:BK6331.
154 Zie voor een kritische bespreking Zwenne & Mommers 2010.
155 Zie Spapens, Sijsling & de Feijter 2011, p. 38-42 en Rb. Den Haag, 26 september 2011, ECLI:NL:RBSGR:2011:BU3207, Rb. Amsterdam, 7 april 2015, ECLI:NL:RBAMS:2015:1987 en HR 27 juni 2017, ECLI:NL:HR:2017:1166.
156 *Stb*. 2017, 489, inwerkingtreding 1 mei 2018 (*Stb*. 2018, 113).
157 HR 10 april 2018, ECLI:NL:HR:2018:553.
158 Zie hierover bijvoorbeeld Oerlemans e.a. 2016.

heim valt (want in de beschikkingsmacht van de transporteur van de communicatie). Communicatie-inhoud betreft bijvoorbeeld opgeslagen e-mails bij online communicatieaanbieders; deze moeten worden gevorderd op basis van artikel 126ng lid 2 Sv.[159] Dit is slechts mogelijk op bevel van een officier van justitie, met machtiging van een rechter-commissaris, voor zover het belang van het onderzoek dit dringend vordert en bij de verdenking van misdrijven die een ernstige inbreuk op de rechtsorde opleveren. Bovendien mag alleen inhoud van communicatie worden gevorderd van of voor de verdachte of met betrekking tot het strafbare feit. De ratio voor deze strenge voorwaarden voor toepassing van de bevoegdheid ligt met name in het recht op bescherming van vertrouwelijke communicatie.
Hoewel de categorie communicatieaanbieders niet per se hostingaanbieders omvat, ligt het wel voor de hand dat ook opgeslagen documenten bij aanbieders van cloudopslagdiensten, zoals Google Drive, Microsoft SkyDrive en Dropbox, slechts onder de voorwaarden van artikel 126ng lid 2 Sv gevorderd mogen worden. Deze diensten zijn nauw verwant met de transporteurs van communicatie die van oudsher worden geassocieerd met het telecommunicatiegeheim; het past ook bij de benadering in bijvoorbeeld de Verenigde Staten, waar deze inhoudelijke gegevens slechts kunnen worden verkregen met een rechterlijke machtiging (*warrant*).[160] In hoofdstuk 4 wordt verder ingegaan op het onderwerp van het vorderen van gegevens die in het buitenland beschikbaar zijn. In Nederland heeft de Rechtbank Overijssel in februari 2017 in een vonnis duidelijk gemaakt dat opgeslagen documenten bij een cloud-dienstverlener op grond van artikel 126ng lid 2 Sv moeten worden gevorderd.[161]

3.3.6 *Bevriezing van gegevens*

Om te voorkomen dat de opsporing hinder ondervindt van de vluchtigheid van elektronische gegevens, heeft Nederland in navolging van artikel 16 Cybercrimeverdrag bij de Wet computercriminaliteit II een bevriezingsbevoegdheid ingevoerd in artikel 126ni Sv. Als er aanwijzingen zijn dat gegevens bijzonder vatbaar zijn voor verlies of wijziging, kan justitie bevelen dat deze voor een (eenmalig verlengbare) periode van maximaal negentig dagen worden bewaard in de oorspronkelijke vorm. Deze bevoegdheid komt toe aan de officier van justitie bij misdrijven waarvoor voorlopige hechtenis is toegelaten die een ernstige inbreuk op de rechtsorde opleveren. Ook moet het onderzoek dringend de bevriezing vorderen. Dit zijn relatief zware eisen, ingegeven door de doelafwijkende verwerking van de te bevriezen gegevens waar het bevel toe noodzaakt,

159 *Kamerstukken II* 2003/04, 29441, 3, p. 14. Zie ook Commissie-Mevis 2001, p. 89. Zie ook Rb. Rotterdam 26 maart 2010, ECLI:NL:RBROT:2010:BM2520.

160 Zie bijvoorbeeld de uitleg van Google over het vorderen van gegevens: https://www.google.com/transparencyreport/userdatarequests/legalprocess/ (laatst geraadpleegd op 1 juli 2018): een *warrant* is vereist om Google te dwingen tot "openbaarmaking van gegevens met betrekking tot zoekopdrachten van de gebruiker en privé-inhoud opgeslagen op een Google-account, zoals Gmail-berichten, documenten, foto's en YouTube-video's".

161 Zie Rb. Overijssel 1 februari 2017, ECLI:NL:RBOVE:2017:417, *Computerrecht* 2017/52, nr. 2, p. 102-106, m.nt. J.J. Oerlemans.

de lasten voor het bedrijfsleven en de bijzondere inspanning die veelal zal worden gevraagd. De vordering kan overigens niet worden gericht aan de verdachte.
Aansluitend aan de bevriezing kan justitie dan in relatieve rust maatregelen nemen om de gegevens op de gewenste manier te verkrijgen, bijvoorbeeld nadat een officieel rechtshulpverzoek tot 'uitlevering' van de gegevens is binnengekomen. De bedoeling is dat deze maatregelen laagdrempelig kunnen worden getroffen, zonder veel voorwaarden; het gaat immers nog niet om de kennisneming van de gegevens door justitie, maar alleen om het verzekeren van de mogelijkheid dat justitie – op basis van een andere bevoegdheid – er later kennis van kan nemen.

3.3.7 *Overzicht*

In onderstaande tabel zijn de belangrijkste vorderingen voor het vorderen van gegevens weergegeven, met de juridische basis en de voorwaarden.

Categorie van gegevens	**Juridische basis**	**Voorwaarden**	**Voorbeeld van type gegevens**
Gebruikersgegevens	126na Sv	Bevel opsporingsambtenaar, elk misdrijf	Naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van een communicatiedienst
Verkeersgegevens	126n Sv	Bevel officier van justitie, misdrijven zoals omschreven in art. 67, eerste lid Sv	Tijd, duur, gebruikte apparatuur, afgenomen diensten en locatiegegevens
'Gewone' en 'andere' gegevens	126nd Sv, 126ng lid 1 Sv	Bevel officier van justitie, misdrijven zoals omschreven in art. 67, eerste lid Sv	Onder andere betalingsgegevens en profielgegevens, niet zijnde gevoelige gegevens
Beveiligingscamerabeelden	126nda Sv	Bevel opsporingsambtenaar, misdrijven zoals omschreven in art. 67, eerste lid Sv.	Camerabeelden van bedrijfsterrein of bodycam van persoonsbeveiliger, niet zijnde gevoelige gegevens

Categorie van gegevens	Juridische basis	Voorwaarden	Voorbeeld van type gegevens
'Gevoelige' gegevens	126nf Sv	Bevel officier van justitie, machtiging rechter-commissaris, dringend onderzoeksbelang, ernstige inbreuk op de rechtsorde bij misdrijven zoals omschreven in art. 67, eerste lid Sv	Profielgegevens betreffende politieke gezindheid of seksuele leven
Communicatie-inhoudelijke gegevens	126ng lid 2 Sv	Bevel officier van justitie, machtiging rechter-commissaris, dringend onderzoeksbelang, ernstige inbreuk op de rechtsorde bij misdrijven zoals omschreven in art. 67, eerste lid Sv, relatie van bericht met verdachte of misdrijf	Opgeslagen e-mailgegevens. Mogelijk andere inhoudelijke gegevens, zoals opgeslagen documenten.

Tabel 3.3 Overzicht van de juridische basis voor vorderen van gegevens.

3.4 De telecommunicatietap

3.4.1 *Wetsgeschiedenis en definities*

De tapbevoegdheid werd ingevoerd in 1971 in artikel 125g Sv (oud) als mogelijkheid om gesprekken af te luisteren of op te nemen.[162] In 1993 werd dit verruimd tot de bevoegdheid om alle telecommunicatieverkeer, dus ook fax en e-mail, af te tappen of op te nemen.[163] De noodzaak hiertoe was duidelijk geworden door een uitspraak van de Hoge Raad dat het tappen van een fax niet mogelijk was op grond van de tot *gesprekken* beperkte tapbevoegdheid.[164]
Met de Wet BOB is de tapbevoegdheid verplaatst naar de titel over bijzondere opsporingsbevoegdheden, in artikel 126m Sv.[165] In 2004 werd artikel 126m Sv uitgebreid met bepalingen over grensoverschrijdend aftappen.[166] Bij de Wet computercriminaliteit II is de bevoegdheid uitgebreid met het aftappen van besloten telecommunicatie, met een definitie van de nieuwe term 'aanbieder van een communicatiedienst' in artikel 126la Sv en onder verplaatsing van het grensoverschrijdend tappen naar het nieuwe artikel 126ma Sv.

Definitie 'Aanbieder van een communicatiedienst'
Artikel 138g (126la-oud) Sv[167] definieert, in aansluiting op het Cybercrimeverdrag, een 'aanbieder van een communicatiedienst' als "de natuurlijke persoon of rechtspersoon die in de uitoefening van een beroep of bedrijf aan de gebruikers van zijn dienst de mogelijkheid biedt te communiceren met behulp van een geautomatiseerd werk, of gegevens verwerkt of opslaat ten behoeve van een zodanige dienst of de gebruikers van die dienst". Tot 2006 was het alleen mogelijk *openbare* telecommunicatie af te tappen. Vanwege het Cybercrimeverdrag vond de wetgever het nodig om ook besloten telecommunicatie te kunnen aftappen.[168] Men kan daarbij bijvoorbeeld denken aan de interne netwerken van bedrijven, instellingen, ministeries of universiteiten. Het aftappen betreft alle vormen van gegevensverkeer, dus niet alleen vaste of mobiele telefoongesprekken of telefaxen, maar ook e-mail, chatverkeer en webcambeelden.
Door de aansluiting bij het Cybercrimeverdrag is de definitie beperkt tot *computergebaseerde* communicatie, wat de klassieke *analoge* telefonie lijkt uit te sluiten, die van

162 *Stb.* 1971, 180. Zie ook reeds de Richtlijn onderzoek van telefoongesprekken van 2 juli 1984, Sdu-bundel strafrecht (Richtlijnen OM) 3.12 (aanv. 19).
163 *Stb.* 1993, 33.
164 HR 26 mei 1992, *NJ* 1992/753.
165 Wet bijzondere opsporingsbevoegdheden, *Stb.* 1999, 245. Zie ook artikel 19.19 Telecommunicatiewet, *Stb.* 1998, 664.
166 *Stb.* 2004, 107.
167 Bij de Wet computercriminaliteit III is de definitie verplaatst van artikel 126la (dat is vervallen) naar artikel 126g Sv. (In het wetsvoorstel was de definitie opgenomen in artikel 138e, maar omdat de Wet digitale processtukken Strafvordering, *Stb.* 2016, 90, eerder in werking trad, bevat artikel 138e Sv reeds een definitie van elektronische handtekening en is de definitie van aanbieder van een communicatiedienst terechtgekomen in artikel 138g Sv. Zie *Stb.* 2018, 322, artikel IV lid 2 en *Stb.* 2018, 228 (Verzamelwet), artikel XLIIIa.)
168 *Kamerstukken II* 2004/05, 26671, 7, p. 25-26 en 29.

oudsher juist de kern vormde van de tapwetgeving. Wetshistorisch en teleologisch mogen we aannemen dat analoge telefonie toch nog steeds onder de definitie valt. Dit betreft grotendeels een theoretische kwestie, aangezien communicatie-infrastructuur inmiddels vrijwel volledig computergebaseerd is.[169]
Minder theoretisch is de vraag of de definitie ook (pure) hostingaanbieders omvat. De definitie bevat weliswaar de clausule "of gegevens verwerkt of opslaat", maar voegt daar in één adem aan toe: "ten behoeve van een zodanige dienst of de gebruikers van die dienst", wat lijkt te suggereren dat een hostingdienst alleen als een communicatiedienst geldt als de gegevensopslag instrumenteel is voor het faciliteren van communicatie (bijvoorbeeld een discussieplatform of een cloudopslagruimte voor gebruikers van een webmaildienst). In een strikte, grammaticale lezing vallen (pure) hostingaanbieders dan ook buiten de definitie. In de praktijk lijkt echter een ruimere, meer teleologische, lezing te worden gehanteerd, die ook (de meeste) hostingaanbieders zal omvatten.[170]

Definitie 'communicatie'
Het begrip 'communicatie' is niet gedefinieerd in de wet of in de wetsgeschiedenis rond artikel 126m Sv. Analoog aan de definitie van 'vertrouwelijke communicatie' in het kader van artikel 126l Sv (zie onder, noot 677) zou men communicatie kunnen omschrijven als "de uitwisseling van berichten tussen twee of meer personen", waarbij de 'persoon' ook een persoonsvervangend apparaat kan zijn. Met de opkomst van het Internet of Things (IoT) wordt echter onduidelijk in hoeverre berichtenverkeer tussen apparaten nog toe te rekenen valt aan een persoon, en of het onderscheppen van IoT-berichten onder de aftapregeling valt. Het is in dit verband wenselijk dat de wetgever een duidelijke definitie van 'communicatie' opneemt (in wet of toelichting).[171] Ondertussen gaan wij ervan uit, op historische gronden, dat de aftapregeling primair bedoeld is om alles wat over de communicatie-infrastructuur gaat te omvatten, en dus ook IoT-berichtenverkeer omvat dat plaatsvindt met gebruikmaking van een communicatiedienst.

3.4.2 *Voorwaarden inzet tap*

De officier van justitie is degene die beslist over de inzet van een tap, maar hij heeft vanwege de ingrijpendheid van het middel hiervoor machtiging van de rechter-commissaris nodig. In beginsel wordt de machtiging van de rechter-commissaris schriftelijk verleend, maar bij dringende noodzaak kan zulks ook mondeling geschieden, met opschriftstelling binnen drie dagen (artikel 126m lid 5 jo. 126l lid 7 Sv).[172] Een tap is

169 Niettemin zullen sommige thuis- of bedrijfsnetwerken nog gebruik blijven maken van analogie telefonie. Ook stopt KPN pas op 1 september 2019 met de traditionele analoge telefoniedienst PSTN (Public Switched Telephone Network), zie https://www.bellen.com/nieuws/einde-isdn-en-pstn-aangekondigd (laatst geraadpleegd 1 juli 2018). Naar de letter van de wet kunnen deze restanten van het telecomnetwerk niet (althans niet op het analoge deel) worden afgetapt.
170 Zie noot 126.
171 Zie uitgebreid hierover Commissie-Koops 2018, p. 139-142.
172 Zie over deze termijnen Haverkate 2012.

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. Het bevel vermeldt:

a) het misdrijf en indien bekend de naam of anders een zo nauwkeurig mogelijke aanduiding van de verdachte;
b) de feiten of omstandigheden waaruit blijkt dat de voorwaarden voor toepassing zijn vervuld;
c) het nummer of andere aanduiding waarmee de individuele gebruiker van de communicatiedienst wordt geïdentificeerd, of de naam en, voor zover bekend, het adres van de gebruiker;[173]
d) de geldigheidsduur van het bevel;
e) een aanduiding van de aard van de technische hulpmiddelen waarmee de communicatie wordt opgenomen (artikel 126m lid 2 Sv).

Van het opnemen wordt binnen drie dagen proces-verbaal opgemaakt (artikel 126m jo. artikel 126l lid 8 Sv). Aangenomen mag worden dat het proces-verbaal niet de inhoud van de gesprekken hoeft te bevatten, doch ten minste dient in te houden dat er getapt is, door wie er getapt is en op welk nummer er getapt is.[174] Het is overigens gebruikelijk dat de inhoud van de gesprekken in leesbare vorm ter beschikking staat voor de zittingsrechter, zeker wanneer deze voor het bewijs bedoeld is.

3.4.3 *Werking van de taplast*[175]

De kern van het tappen is normaliter een vordering aan een telecomaanbieder, die immers degene is die meestal feitelijk tapt. Het Cybercrimeverdrag eist echter volgens de wetgever dat justitie ook de bevoegdheid moet hebben om zelf te tappen. Daarom is artikel 126m Sv bij de Wet computercriminaliteit II aangepast: de opsporingsambtenaar wordt bevolen dat communicatie wordt afgetapt, waarbij het tappen hetzij door de aanbieder hetzij door de opsporingsambtenaar geschiedt. Lid 3 geeft aan wat de standaardsituatie is bij openbare telecommunicatie: dan tapt de aanbieder, behalve als dat technisch niet mogelijk is of het belang van de strafvordering zich daartegen verzet (bijvoorbeeld als een werknemer van de aanbieder mogelijk betrokken is bij de zaak). Aanbieders van openbare telecommunicatie zijn op basis van artikel 13.2 Telecommunicatiewet verplicht mee te werken aan een tapbevel.

---

173 De laatste clausule, ingevoegd bij Wet van 6 december 2017, *Stb*. 2017, 489, inwerkingtreding 1 mei 2018 (*Stb*. 2018, 113), maakt het zogenoemde 'tappen op naam' mogelijk. Hierdoor is niet langer voor elke afzonderlijke telefoon (of nummer) een machtiging nodig (wat omslachtig is wanneer verdachten tientallen verschillende nummers gebruiken), maar kan één machtiging worden gegeven voor "alle nummers of andere aanduidingen die gedurende de geldigheidsduur van de machtiging bij de gebruiker in gebruik zijn". De rechter-commissaris moet specifiek toestemming geven voor dit tappen op naam. Zie *Kamerstukken II* 2017/18, 34720, 6, p. 3.

174 HR 17 september 1979, *NJ* 1980/22.

175 Zie uitgebreid Smits 2006 over het onderzoek van telecommunicatie in Nederland en de Verenigde Staten van Amerika.

Bij besloten communicatiediensten wordt volgens lid 4 de aanbieder in de gelegenheid gesteld mee te werken aan het tappen. De aanbieder is niet *verplicht* mee te werken, omdat besloten telecommunicatie niet onder de Telecommunicatiewet valt. Niettemin zal het voor een beheerder van een bedrijfsnetwerk soms aantrekkelijker zijn zelf te tappen, bijvoorbeeld als het gaat om het e-mailverkeer van één werknemer, dan de opsporingsautoriteiten toe te laten op het hele netwerk.[176] Wij hebben de indruk dat deze aanbieders doorgaans vrijwillig meewerken aan een tapbevel, maar de politie en het Openbaar Ministerie kunnen, zoals gezegd, ook van eigen apparatuur gebruikmaken.[177] Als opsporingsambtenaren zelf tappen bij een aanbieder, moet de apparatuur volgens artikel 126ee Sv voldoen aan bij AMvB gestelde regels, met betrekking tot onder andere technische eisen, protocollen en controle op de naleving, en de opsporingsambtenaar moet een certificaat van vakbekwaamheid hebben.[178]

In de regel wordt een tap bij deze aanbieders geplaatst op een specifiek telefoonnummer (of ander identificatienummer van een telefoon, zoals een IMEI-nummer). Vervolgens wordt het gehele gesprek opgenomen en tezamen met andere gegevens, zoals locatiegegevens, naar de politie doorgestuurd. Ook het netwerkverkeer dat van en uit een mobiele telefoon gaat, kan worden afgetapt. Het is ook mogelijk een tap op een IP-adres te zetten, waarbij al het netwerkverkeer van bijvoorbeeld een server (waarop een webforum draait) of een router van een woning meekomt. De telefoontap verschilt dus sterk van een internettap.[179] De privacyinmenging die daarbij plaatsvindt is anders, terwijl dezelfde voorwaarden voor de inzet van het middel bestaan. Tegenwoordig registreren opsporingsautoriteiten de inzet van internettaps niet meer apart.

Eenieder (behalve de verdachte) kan worden gevorderd versleutelde taps te ontsleutelen; in de praktijk betekent dit vooral dat communicatieaanbieders verplicht zijn de door hen zelf aangebrachte versleuteling ongedaan te maken om het aftappen te faciliteren (artikel 126m lid 6-9 Sv).[180] De verplichting tot ontsleuteling geldt alleen voor zover de geadresseerde daartoe in staat is. Hij hoeft geen technische voorzieningen aanwezig te hebben om te kunnen ontsleutelen; van hem kan slechts worden verlangd dat hij het signaal in de vorm waarin dit aan hem is aangeboden, ontsleutelt, voorzover hij (nog) over de sleutel beschikt.[181]

176 De kosten die de aanbieder hierbij maakt, lijken echter niet in aanmerking te komen voor vergoeding: artikel 592 Sv vergoedt alleen kosten bij gegevensvordering en ontsleutelbevel, en de Wet tarieven in strafzaken biedt alleen een grondslag voor vergoeding bij verplichte medewerking. Vgl. *Kamerstukken II* 2004/05, 26671, 10, p. 16.

177 Vgl. Huib Modderkolk en Tom Kreling, 'Hoe Nederland een hoofdrol speelde bij het opsporen van een Russische internetcrimineel (en die toch op vrije voeten bleef)', *De Volkskrant*, 27 mei 2017, https://www.volkskrant.nl/kijkverder/2017/hacker/ (laatst geraadpleegd 1 juli 2018).

178 Zie het Besluit technische hulpmiddelen strafvordering, *Stb.* 2006, 524, en de Regeling vakbekwaamheid technische hulpmiddelen strafvordering, *Stcrt.* 27 december 2006, nr. 251, p. 7.

179 Zie ook Koops e.a. 2005, Stratix 2009 en Oerlemans 2012.

180 Deze verplichting bestaat voor aanbieders van openbare communicatie ook reeds op basis van artikel 13.1 TW jo. artikel 2 sub e Besluit aftappen openbare telecommunicatienetwerken en -diensten.

181 *Kamerstukken II* 1998/99, 26671, 3, p. 24-25.

3.4.4 *Tappen van geheimhouders*

Een belangrijk uitgangspunt van het strafrecht is dat bijzondere opsporingsbevoegdheden zoals tappen in principe niet mogen worden uitgeoefend tegenover geheimhouders (advocaten, notarissen, medici, geestelijken) (vergelijk artikel 218 Sv). Zoals de toelichting bij de Wet BOB aangeeft:

CITAAT

> *"Beperkingen ten aanzien van het afluisteren van geheimhouders zijn in dit wetsvoorstel niet opgenomen. Bij het afluisteren van telecommunicatie staan zij thans reeds niet in de wet. Dat geeft – thans – de rechtercommissaris geen vrijbrief om verschoningsgerechtigden af te luisteren, in uitzonderingsgevallen is het echter wel degelijk mogelijk, bijvoorbeeld als de advocaat verdachte is. Daarbij wordt dan een zorgvuldige procedure gevolgd, waarin ook de deken wordt ingeschakeld."*[182]

Wanneer de advocaat geen verdachte is, zal hij dus niet kunnen worden getapt. Dat laat natuurlijk onverlet dat een gesprek met een advocaat wel kan worden getapt door een tap op de verdachte. Voor die situatie geeft artikel 126aa lid 2 Sv aan dat de opnamen van deze gesprekken moeten worden vernietigd (voor zover het gaat om een gesprek met de advocaat als geheimhouder, niet een privé-gesprek).[183] In het eerste decennium van deze eeuw bleek dat in strijd met de wet structureel gesprekken met geheimhouders werden bewaard, omdat het technisch niet mogelijk zou zijn om deze te wissen. Na veel discussies en rechtszaken[184] leidde dit uiteindelijk tot het huidige systeem van nummerherkenning, waarbij geregistreerde nummers van advocaten automatisch worden herkend en worden uitgesloten van de tap.[185] Voor andere beroepsmatige verschoningsgerechtigden bestaat echter niet een dergelijk geautomatiseerd systeem; de

182 *Kamerstukken II* 1996/97, 25403, 3, p. 61. Zie voor een tap op een verdachte advocaat bijvoorbeeld HR 30 september 2003, *Nieuwsbrief Strafrecht* 2003, 386. Zie ook Aanwijzing toepassing opsporingsbevoegdheden en dwangmiddelen tegen advocaten, *Stcrt.* 2011, 4981.

183 Zie ook artikel 4 Besluit bewaren en vernietigen niet-gevoegde stukken, *Stb.* 1999, 548 en de OM-Instructie vernietiging geïntercepteerde gesprekken met geheimhouders. Een verzuim hiervan kan ingrijpende gevolgen hebben voor justitie, zoals niet-ontvankelijkverklaring van het OM, zie bijvoorbeeld Rb. Rotterdam 20 februari 2007, ECLI:NL:RBROT:2007:AZ9179. Vgl. echter ook HR 1 april 2003, *NJ* 2003/303, waarin geen gevolgen aan het verzuim werden verbonden omdat de onrechtmatig uitgewerkte gesprekken met de advocaat geen informatie bevatten waarop het verschoningsrecht zag en ook niet opsporingsrelevant was. In HR 16 juni 2009, ECLI:NL:HR:2009:BH2678, oordeelde de Hoge Raad dat het onrechtmatig operationeel gebruiken van informatie uit een afgetapt geheimhoudergesprek om de verdachte aan te houden, niet zonder meer een dusdanig grove veronachtzaming van de belangen van de verdachte oplevert dat niet-ontvankelijkverklaring op zijn plaats is. Niet-ontvankelijkverklaring is alleen, in uitzonderlijke gevallen, aan de orde indien "doelbewust of met grove veronachtzaming van de belangen van de verdachte aan diens recht op een eerlijke behandeling van zijn zaak is tekortgedaan", waarbij de verwijtbaarheid van het verzuim (opzettelijk of niet) en de Schutznorm een belangrijke rol spelen, zie HR 11 oktober 2011, ECLI:NL:HR:2011:BR0552, r.o. 2.3.1.

184 Zie onder andere *Nieuwsbrief Strafrecht* 2001/10, p. 357-358; EHRM 25 november 2004, nr. 16269/02 (*Aalmoes e.a. t. Nederland*); Rb. 's-Gravenhage 15 maart 2005, ECLI:NL:RBSGR:2005:AT0304, waarin diverse vorderingen van de Nederlandse Vereniging van Strafrechtadvocaten in kort geding werden afgewezen; en College bescherming persoonsgegevens 2007.

185 Zie https://nummerherkenning.advocatenorde.nl/ (laatst geraadpleegd 1 juli 2018).

uitvoerders van taps zullen dus alert moeten blijven op zorgvuldige omgang conform de wettelijke regeling ten aanzien van gesprekken van getapte personen met bijvoorbeeld notarissen of medici die onder het verschoningsrecht vallen. De reikwijdte van het beroepsgeheim van advocaten en andere geheimhouders is overigens al jaren onderwerp van discussie (ook bij andere opsporingsbevoegdheden en dwangmiddelen)[186] en zal dat de komende jaren ook wel blijven. Bij gebrek aan (concept)wetsvoorstellen of regelingen op dit punt – toegespitst op de tap – gaan we verder niet op deze discussie in.

3.4.5 *Grensoverschrijdend tappen*

Op grond van het rechtshulpverdrag tussen EU-lidstaten, dat onder andere grensoverschrijdend aftappen regelt, is de Nederlandse wetgeving in 2004 aangepast.[187] De officier van justitie kan een bevel geven tot aftappen van iemand die zich op het grondgebied van een andere staat bevindt (en die bijvoorbeeld via zijn mobiele telefoon nog in Nederland is af te tappen), mits hij na de afgifte van het bevel tot tappen eerst die andere (verdrags)staat in kennis stelt en om toestemming vraagt (artikel 126ma lid 1 Sv). Het is niet mogelijk in dringende gevallen te tappen en achteraf om toestemming te vragen.[188] Als pas tijdens de tap blijkt dat de verdachte zich in het buitenland bevindt, wordt de buitenlandse (verdrags)staat alsnog in kennis gesteld en om toestemming gevraagd (artikel 126ma lid 2 Sv).[189]
De officier van justitie kan tevens een tapbevel geven om een buitenlandse staat in staat te stellen de benodigde telecommunicatie af te tappen en rechtstreeks door te geleiden voor opname in Nederland (artikel 126ma lid 3 Sv). In tegenstelling tot de binnenlandse tap, kan de buitenlandse tap slechts worden bevolen voor openbare telecommunicatie.
Omgekeerd kan Nederland op verzoek van een andere verdragsstaat telecommunicatie aftappen en rechtstreeks doorgeleiden naar die staat, onder voorwaarden van vernietiging van geheimhoudersgesprekken, doelbinding en notificatie (artikel 5.1.12 (Vijfde Boek) Sv[190]). Ook dient de rechter-commissaris te beslissen op verzoeken van andere staten om iemand binnen Nederlands grondgebied te mogen aftappen (artikel 5.1.13 (552oc-oud) Sv). In deze gevallen kan ook, op basis van artikel 126m Sv, besloten communicatie worden getapt.

186 Zie bijvoorbeeld Rense 2017 en Vellinga-Schootstra 2017. Zie ook paragraaf 3.2.1.
187 Overeenkomst betreffende de wederzijdse rechtshulp in strafzaken tussen de lidstaten van de Europese Unie, 29 mei 2000, *Trb.* 2000, 96: Wet van 18 maart 2004, *Stb.* 2004, 107. De bepalingen zijn overgeheveld bij de Wet computercriminaliteit II naar het nieuwe artikel 126ma Sv.
188 *Kamerstukken II* 2001/02, 28351, 3, p. 3.
189 Dit was aanvankelijk niet mogelijk bij onderzoek naar (beraamde) georganiseerde misdaad, maar is bij *Stb*. 2009, 525 gerepareerd in artikel 126ta Sv.
190 Tot 1 juli 2018 geregeld in artikel 552ob Sv-oud, gewijzigd bij de Wet herziening regeling internationale samenwerking in strafzaken, *Stb*. 2017, 246.

3.4.6 *Bewaren, vernietigen en notificatie*

De officier van justitie behoort de banden of de processen-verbaal die zijn gemaakt naar aanleiding van het onderzoek van telecommunicatie en die niet bij de processtukken zijn gevoegd ter beschikking te houden en twee maanden na het beëindigen van de zaak te vernietigen (artikel 126cc Sv). De gegevens kunnen worden gebruikt voor ander onderzoek (artikel 126dd Sv).[191] Artikel 126bb Sv eist dat betrokkenen worden genotificeerd, voor zover dat redelijkerwijs mogelijk is, dat wil zeggen dat de officier van justitie hen schriftelijk mededeling doet van de uitoefening van de tapbevoegdheid zodra het belang van het onderzoek dat toelaat. Bij uitstel in verband met het onderzoeksbelang moet de officier telkens na drie (of voor zware misdrijven zes) maanden herbeoordelen of alsdan kan worden genotificeerd.[192] Betrokkenen zijn de gebruiker van de getapte communicatiedienst en de persoon ten aanzien van wie de tap is uitgevoerd.[193] In de zaak *Lambert* oordeelde het EHRM dat artikel 8 EVRM is geschonden jegens degene die belde naar (of van) een in verband met een derde afgetapt telefoonnummer en daarover niet kon klagen bij de Franse rechter. Het ging hier dus niet om degene die in eerste instantie werd verdacht, maar om de beller die zich in het opgenomen gesprek zelf belastte.[194] Het arrest roept de vraag op in hoeverre de notificatieplicht van artikel 126bb Sv in dit verband redelijkerwijs mogelijk is. Wij zijn geneigd de notificatieplicht in het licht van artikel 8 jo. artikel 13 EVRM te beschouwen, waarbij niet elke inkomende beller achteraf op de hoogte hoeft te worden gesteld, maar wel frequente in- en uitgaande bellers, zeker als zeer persoonlijke of intieme gesprekken zijn afgeluisterd. Naarmate de inbreuk op de persoonlijke levenssfeer groter is geweest, zal justitie onzes inziens ook meer moeite moeten doen het adres van getapte personen (en frequente gesprekspartners) te achterhalen om deze te notificeren.
In de praktijk bleek overigens dat notificatie maar zeer beperkt plaatsvond, volgens de evaluatie van de Wet BOB uit 2004.[195] De situatie lijkt sindsdien verbeterd; WODC-onderzoek uit 2012 stelde vast dat doorgaans (zonder prioriteit) werd genotificeerd (hoewel ieder parket daar een eigen invulling aan gaf). De notificatie bleef daarbij beperkt tot getapte personen zelf, niet hun communicatiepartners.[196]

191 Zie ook HR 13 mei 2003, *NJ* 2003/471: artikel 126dd Sv staat niet in de weg aan het gebruik van tapgegevens die zijn verkregen in het opsporingsonderzoek in een andere zaak. De officier van justitie kan ook achteraf toestemming geven voor het gebruik van die gegevens in een andere zaak.
192 Als na vijf jaar nog steeds het onderzoeksbelang of veiligheidsrisico's aan notificatie in de weg staan, wordt uitstel definitief afstel. Zie Aanwijzing opsporingsbevoegdheden, *Stcrt.* 2014, nr. 24442, paragraaf 5.4.
193 Artikel 126bb lid 2 Sv verwijst (nog steeds) ten onrechte naar het derde lid van artikel 126m en artikel 126t, bedoeld is het tweede lid.
194 EHRM 24 augustus 1998, *NJCM-Bulletin* 1998, p. 1058-1063.
195 *Kamerstukken II* 2004/05, 29940, 1, p. 5-6; Beijer, Bokhorst, Boone e.a. 2004, p. 145-147.
196 Odinot e.a. 2012, p. 28-29 en p. 138-145.

3.4.7 *Verplichte aftapbaarheid en verminderde waarde van de tap*

Volgens artikel 13.1 Telecommunicatiewet mogen openbare telecommunicatienetwerken en diensten alleen beschikbaar worden gesteld aan gebruikers als ze aftapbaar zijn. De kosten voor het aftapbaar maken van de infrastructuur of dienst komen voor rekening van de aanbieder; de kosten gemoeid met een concrete tap komen voor rekening van justitie (artikel 13.6 Tw).[197]
De aftapbaarheidsverplichting wordt uitgewerkt in het Besluit en de Regeling aftappen openbare telecommunicatienetwerken en -diensten.[198] Artikel 2 van de Regeling somt netwerken op die in elk geval onder de plicht vallen: vaste openbare telefoonnetwerken en diensten, huurlijnen, mobiele netwerken zoals gsm en GPRS, en internet. Het feit dat netwerken en diensten hier expliciet staan vermeld, wil niet zeggen dat andere netwerk- of dienstenaanbieders zich aan de aftapbaarheidsplicht kunnen onttrekken – artikel 13.1 Tw is immers stellig geformuleerd als geldend voor alle aanbieders van *openbare* telecommunicatie.
Eenvoudig gezegd bieden aanbieders van openbare telecommunicatiediensten en -netwerken de internettoegangsdiensten zelf aan, terwijl diverse online communicatiediensten diensten aanbieden over de infrastructuur heen, zoals sociale-mediadiensten. Diensten zoals Facebook, Skype en WhatsApp vallen niet onder de (huidige) Telecommunicatiewet en hoeven dan ook geen aftapinfrastructuur te installeren om taps te installeren. Dit is ook de reden dat een telefoontap of internettap op een telefoon of breedbandinternetverbinding kan worden gezet, maar (tot nog toe) geen tap kan worden gezet bij sociale-mediadiensten om privéberichten te onderscheppen.[199]
Op de aftapbaarheidsplicht is volgens artikel 13.8 Tw ontheffing mogelijk in bijzondere gevallen. Hiervan werd tot 2001 wel gebruikgemaakt door internetaanbieders, totdat ook zij verplicht waren aftapbaar te zijn. Niet voldoen[200] werd nog enige tijd gedoogd, maar sinds ongeveer 2003 geldt de aftapbaarheidsplicht onverkort voor internetaanbieders. In dit kader werd onder andere een Stichting Nationale Beheersorganisatie Internet Providers (NBIP) opgericht om een mobiel tapkastje bij (vooral kleinere) aanbieders te installeren.[201] Ook mobiel internetverkeer is verplicht aftapbaar gemaakt.

In een evaluatie van de aftapbaarheidswetgeving in 2005 werd geconcludeerd dat de telecommunicatie voor het overgrote deel inderdaad aftapbaar was, maar dat de nodige technische en marktontwikkelingen de effectiviteit en efficiëntie van aftapbaarheid

197 Zie ook de Regeling kosten aftappen en gegevensverstrekking, *Stcrt.* 2005, nr. 62, p. 16. De vordering van XS4ALL om de kosten voor het aftapbaar maken door de staat te laten betalen, is door de rechter afgewezen, Rb. 's-Gravenhage 21 februari 2007, ECLI:NL:RBSGR:2007:AZ9109.
198 Besluit van 10 november 1998, *Stb.* 1998, 642, laatst aangepast *Stb*. 2003, 22. Dit besluit is nader uitgewerkt in de Regeling aftappen openbare telecommunicatienetwerken en -diensten, 30 mei 2001, *Stcrt.* 2001, 107. Volgens Smits 2004 valt hieronder ook de verplichting om niet-aftapbare randapparaten, zoals cryptofoons, van het netwerk af te sluiten, een interpretatie die ons te ver gaat.
199 Zie uitgebreid Oerlemans 2012.
200 *Aanhangsel Handelingen II* 2000/01, 1155.
201 Zie https://www.nbip.nl/tapdienst/ (laatst geraadpleegd 1 juli 2018).

in de toekomst zouden kunnen verminderen.[202] De minister heeft in reactie op de evaluatie de handhaving van de wetgeving door het Agentschap Telecom geïntensiveerd en nader onderzoek aangekondigd.[203]

Uit onderzoek is inmiddels gebleken dat de effectiviteit van de tap de laatste jaren sterk is afgenomen. Uit grootschalig WODC-onderzoek uitgevoerd in 2011 en 2012 bleek dat de afname in aftapbaarheid van communicatie – ingegeven door de omslag van communicatie met de telefoon naar communicatie via internet – als een groot obstakel in opsporingsonderzoeken wordt ervaren.[204] Diverse factoren dragen bij aan wat wel het '*going dark*'-probleem wordt genoemd.[205] Wij noemen er hier vier.

1. Versleuteld verkeer kan vaak niet (meer) worden ontsleuteld door opsporingsdiensten. Als gevolg daarvan kan de inhoud van het verkeer niet worden uitgelezen, zoals de inhoud van verstuurde privéberichten over internet. De infrastructuur bij bedrijven kan zijn ingericht op een wijze waarbij de bedrijven niet meer in het bezit zijn van de sleutels om het netwerkverkeer te ontsleutelen. De sleutels liggen bijvoorbeeld veilig opgeslagen bij de eindgebruikers (*end-to-end*-encryptie). Ook kan het netwerkverkeer van populiare online communicatiediensten, zoals sociale-mediadiensten, vaak niet (meer) ontsleuteld worden. Gebruikers kunnen zelf ook het communicatieverkeer versleutelen met diensten die het netwerkverkeer versleutelen, zoals *Virtual Private Network* (VPN)-dienstverleners, of software, zoals *Pretty Good Privacy* (PGP).[206]
2. De tapplicht is alleen afdwingbaar op bedrijven en instellingen op het eigen grondgebied. Alleen zij kunnen verplicht worden een aftapinfrastructuur te bouwen om de tap te faciliteren. Berichten die via internet worden verstuurd met 'over-the-top' (OTT-)diensten, zoals sociale-mediadiensten en berichten via apps op mobiele telefoons, kennen vaak (nog) geen tapinfrastructuur en de hoofdkantoren van deze diensten bevinden zich vaak in het buitenland.[207]
3. Een tap op een mobiele telefoon of router van een woning vangt slechts een deel van iemands internetverkeer op.[208] Mensen maken steeds vaker gebruik van mobiele wifi-spots in restaurants, treinen of op vliegvelden. Dit verkeer komt niet bij de tap mee en het is onduidelijk in hoeverre deze dienstverleners een tapinfrastructuur hebben liggen om de tap te faciliteren.

202 Zie Koops e.a. 2005. Vgl. http://www.netkwesties.nl/editie68/artikel5.php. Vanwege de onduidelijkheid over de reikwijdte van de verplichting en de grote kosten die gemoeid zijn met het aftapbaar maken van infrastructuren en diensten, hetgeen een verkillend effect op innovatie kan hebben, hebben Dries, Gijrath & Knol 2003 de aanbeveling gedaan om bij Ministerieel Besluit expliciet alle netwerken en diensten aan te wijzen waarvan de wetgever vindt dat die aftapbaar moeten zijn (p. 122).

203 *Kamerstukken II* 2005/06, 30517, 1.

204 Zie Odinot e.a. 2012, p. 129.

205 Vgl. de getuigenis van Valerie Caproni, general counsel bij de FBI, op 11 februari 2011: "In the ever-changing world of modern communication technologies, however, the FBI and other government agencies are facing a potentially widening gap between our legal authority to intercept electronic communications pursuant to court order and our practical ability to actually intercept those communications". Zie ook Bellovin e.a. 2013.

206 Zie Bellovin e.a. 2013 en Oerlemans 2017a, p. 45-49.

207 Zie Smits 2006, p. 77 en Oerlemans 2012, p. 22. Zie ook p. 84 van de memorie van toelichting van de Wiv 2017 (*Kamerstukken II* 2016/17, 34588, 3, p. 84).

208 Zie Koops e.a. 2005, p. 63, Oerlemans 2012, p. 30-31 en Bellovin e.a. 2013, p. 63-64.

4. De diversiteit en hoeveelheid aan netwerkverkeer dat wordt afgetapt is in de laatste twintig jaar enorm toegenomen. Het kost veel tijd, capaciteit en schaarse technische expertise het netwerkverkeer te analyseren en in kaart te brengen.[209]

3.5 Direct afluisteren

'Vertrouwelijke communicatie'

Het opnemen van vertrouwelijke communicatie met een technisch hulpmiddel is als wettelijke bevoegdheid geïntroduceerd in artikel 126l Sv.[210] Onder vertrouwelijke communicatie moet worden verstaan de uitwisseling van berichten tussen twee of meer personen die in beslotenheid plaatsvindt.[211] Vertrouwelijke communicatie kan op zeer verschillende wijzen plaatsvinden: bijvoorbeeld door het gesproken of geschreven woord, of door de overdracht van signalen via de ether of de kabel. Onder vertrouwelijke communicatie valt bijvoorbeeld een in beslotenheid gevoerd gesprek, een niet-openbaar e-mailbericht, of niet voor het publiek bestemd radioverkeer.[212] Ook het gebruik van een geldautomaat waarbij een persoon met behulp van zijn bankpas communiceert via de computer van de bank valt volgens de memorie van toelichting onder dit begrip. Het opnemen van communicatie met medeweten van een van de deelnemers aan de communicatie valt ook onder direct afluisteren.[213]

Wel moet het gaan om communicatie met een ander. Het direct afluisteren van hetgeen iemand invoert in zijn computer zonder dat dit wordt verzonden is niet toegestaan; er moet minstens een ander (al dan niet via een andere machine) in het spel zijn. In de praktijk lijkt dit te worden geïnterpreteerd in de zin dat het afvangen van 'zelfcommunicatie', zoals het op een computer intikken van wachtwoorden of een dagboek, niet mogelijk is; het valt niet onder direct afluisteren maar ook niet onder (stelselmatige) observatie, omdat het twijfelachtig is dat onderschepte 'zelfcommunicatie' een vorm van gedrag is.[214] Dit betekent dat de inzet van bijvoorbeeld een keylogger alleen is toegestaan als de redelijke verwachting bestaat dat daarmee communicatie (met anderen)

209 Zie Koops e.a. 2005, p. 60, Diffie & Landau 2007, p. 55 en Odinot e.a. 2012, p. 158.

210 *Stb.* 1999, 245. In de jaren negentig van de vorige eeuw was een wetsvoorstel aanhangig "in verband met de regeling van het opnemen van gesprekken met een technisch hulpmiddel", *Kamerstukken II* 1992/93, 23047, 1-2, maar dit werd in de nasleep van de IRT-affaire ingetrokken en direct afluisteren werd in plaats daarvan opgenomen in de Wet BOB.

211 *Kamerstukken II* 1996/97, 25403, 3, p. 36. Dit roept de vraag op of justitie niet-communicatieve geluiden (zoals in zichzelf praten) met een technisch hulpmiddel kan opnemen. Dit kan niet op basis van de bevoegdheid tot direct afluisteren, maar is onzes inziens wel mogelijk op basis van de bevoegdheid tot stelselmatige observatie, aangezien het een vorm van waarnemen van gedrag betreft (zie paragraaf 3.6).

212 *Kamerstukken II* 1996/97, 25403, 3, p. 36.

213 *Kamerstukken II* 1996/97, 25403, 3, p. 38 en 7, p. 60. Voorheen werd er door velen van uitgegaan dat voor een dergelijk afluisteren geen wettelijke basis vereist was. Dat werd gebaseerd op de tekst van artikel 139a Sr waar heimelijke opname door een gespreksdeelnemer niet strafbaar is gesteld. Daarmee werd echter voorbijgegaan aan het verschil tussen strafbaarstelling en bevoegdheidsverlening; er was altijd al sprake van een ongerechtvaardigde inmenging zijdens de overheid in dergelijke gevallen. Dit is in lijn met Europese rechtspraak, zie EHRM 23 november 1993, nr. 14838/89 (*A. t. Frankrijk*). Zie ook HR 18 februari 1997, *NJ* 1997/500, m.nt. 't H.

214 Zie Commissie-Koops 2018, p. 146.

wordt vastgelegd. Software die niet alleen toetsaanslagen registreert maar ook schermafbeeldingen kan maken, is daarbij niet uitgesloten, mits de schermafbeeldingen alleen worden gemaakt op momenten dat naar redelijke verwachting communicatie in beeld is (het betreft dan immers een alternatieve vorm van het vastleggen van de communicatie). Een en ander is echter moeilijk technisch exact af te kaderen, waardoor vragen rijzen over de controleerbaarheid in concrete zaken of de voorziene vastlegging daadwerkelijk was beperkt tot communicatie (en niet tot voorzienbare 'bijvangst' van zelfcommunicatie).[215]
Zeer twijfelachtig lijkt ons de benadering waarin 'vertrouwelijke communicatie' (achteraf) wordt geïnterpreteerd vanuit de inhoud van opgenomen gesprekken, in de zin dat er geen sprake zou zijn van 'vertrouwelijke' communicatie als iemands persoonlijke levenssfeer niet in het geding is bij het gesprek.[216] Dit zet de deur open om, zonder aan de 126l-voorwaarden te voldoen, gesprekken af te luisteren in de hoop zakelijke (of anderszins niet privé-)gesprekken op te vangen, die dan gewoon voor het bewijs zouden kunnen worden gebruikt. Niet de inhoud van gesprekken is leidend, maar de omstandigheden waarin gesprekken worden gevoerd. Gesprekken op de achterbank van een politie-BMW[217] vinden plaats in beslotenheid en zijn *dus* vertrouwelijke communicatie, ongeacht of de inhoud de persoonlijke levenssfeer betreft.

Voorwaarden inzet bijzondere opsporingsbevoegdheid
De voorwaarden voor het direct afluisteren zijn tamelijk zwaar. In de eerste plaats wordt de verdenking vereist van een misdrijf als omschreven in artikel 67, eerste lid, Sv dat een ernstige inbreuk op de rechtsorde oplevert. Het bevel om af te luisteren kan slechts worden gegeven na schriftelijke machtiging op vordering van de officier van justitie te verlenen door de rechter-commissaris. Opvallend is dat artikel 126l Sv niet vereist dat het gaat om communicatie waaraan de verdachte deelneemt, maar dat artikel 126s Sv (direct afluisteren bij beraamde of gepleegde georganiseerde misdrijven) wel beperkt is tot communicatie van personen die naar redelijk vermoeden betrokken zijn bij het in georganiseerd verband beramen of plegen van misdrijven. Van de toepassing van de bevoegdheid dient binnen drie dagen proces-verbaal te worden opgemaakt, en aangenomen mag worden dat ook in dit verband uitgetikte versies van de afgeluisterde gesprekken zullen worden verstrekt indien zulks mogelijk is. Sinds 2018 is direct afluisteren ook toegestaan voor bijzondere opsporingsdiensten.[218]
De wetgever onderkende dat de bevoegdheid tot het opnemen van communicatie als meer ingrijpend moet worden gezien dan het opnemen van telecommunicatie, maar heeft toch gekozen in beide gevallen dezelfde voorwaarden te stellen. Deze onderken-

215 Vgl. de annotatie van Oerlemans bij Rb. Amsterdam 16 maart 2017, ECLI:NL:RBAMS:2017:1627 (*Aydin C.*), *Computerrecht* 2017/103, nr. 3, p. 179.
216 De Hoge Raad liet deze benadering in stand in de zaak tegen Willem H., waarin het hof had geoordeeld dat de opgenomen gesprekken die Endstra voerde met de CIE niet onder artikel 126l Sv vielen omdat Endstra's persoonlijke levenssfeer niet in het geding was, zie HR 12 oktober 2010, ECLI:NL:HR:2010:BN0526, r.o. 6.4.
217 https://nl.wikipedia.org/wiki/Endstra-tapes (laatst geraadpleegd 1 juli 2018).
218 *Stb*. 2017, 489, inwerkingtreding 1 mei 2018 (*Stb.* 2018, 113).

ning brengt wel met zich mee dat indien in het belang van het onderzoek kan worden volstaan met het opnemen van telecommunicatie het de officier van justitie niet vrij staat een bevel te geven tot direct afluisteren (subsidiariteitsbeginsel).

Binnentreden besloten plaats
Dikwijls zal het opnemen van communicatie pas mogelijk zijn door in de omgeving van de persoon die onderwerp van onderzoek is technische apparatuur te plaatsen. Een samenhangende maar wel afzonderlijk gereguleerde bevoegdheid is dan ook dat de officier van justitie in het belang van het onderzoek kan bepalen dat ter uitvoering van het bevel een besloten plaats, niet zijnde een woning, wordt betreden zonder toestemming van de rechthebbende. Hij kan bovendien bepalen dat ter uitvoering van het bevel een woning zonder toestemming van de rechthebbende wordt betreden indien het onderzoek dit dringend vordert en het een misdrijf betreft waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaar of meer is gesteld (artikel 126l lid 2 Sv; artikel 126s hanteert hier een drempel van zes jaar).
Indien een woning moet worden betreden, dan wordt dat uitdrukkelijk in de machtiging vermeld. De introductie van deze vergaande inbreuk op de privacy is eerst in een later stadium in het traject van de Wet BOB voorgesteld en daardoor relatief – in vergelijking met wat men zou verwachten op grond van buitenlandse ervaringen – tamelijk geruisloos en met weinig debat aanvaard, wat des te opmerkelijker is nu de wetgever stelselmatige observatie binnen de woning wettelijk niet heeft toegestaan. Wij achten het in dat licht belangrijk dat in de rechtspraak vooral in geval van direct afluisteren in woningen de wettelijke eisen zeer streng zullen worden gehanteerd.

Plaatsen van apparatuur
Het opnemen van vertrouwelijke communicatie kan onder meer bestaan uit het opvangen van niet voor het publiek bestemd radioverkeer, het gebruik van richtmicrofoons, het van een microfoontje (bug) voorzien van lampen of andere objecten of het plaatsen van keyloggers in toetsenborden. Gezien het voorgaande mag dit laatste echter alleen gebeuren bij computers die met een netwerk zijn verbonden en die voor communicatie worden gebruikt.
De apparatuur voor direct afluisteren moet aan diverse technische eisen voldoen, met name om de betrouwbaarheid van de resulterende opnames te waarborgen. De eisen zijn vastgelegd in artikel 126ee Sv en het daarop gebaseerde Besluit.[219] Verder mogen

219 Besluit technische hulpmiddelen strafvordering, *Stb.* 2006, 524. In HR 12 juli 2011, ECLI:NL:HR:2011:BP4651, oordeelde de Hoge Raad dat het Besluit "er met het oog op de betrouwbaarheid en herleidbaarheid van de opgenomen gegevens toe [strekt] te waarborgen dat de mogelijkheid wordt uitgesloten dat een gesprek of een deel van een gesprek wordt afgeluisterd of onderschept zonder dat het wordt opgenomen, zodat alleen technische hulpmiddelen die aan die waarborgen (kunnen) voldoen mogen worden ingezet" voor direct afluisteren. Dat betekent echter niet dat hulpmiddelen per definitie uitgesloten zijn als deze (ook) kunnen worden gebruikt voor afluisteren zonder registreren van gesprekken; het gaat erom dat hulpmiddelen een registratiefunctie hebben en dat deze apparatuur moet worden goedgekeurd; als een goedgekeurd middel vervolgens (deels) wordt gebruikt voor afluisteren zonder registratie, kan niet worden geklaagd dat het hulpmiddel zelf niet aan de eisen voldoet, maar alleen over het afwijkend gebruik dat van het hulpmiddel in concreto is gemaakt.

alleen politiefunctionarissen die voldoen aan bepaalde bekwaamheidseisen uitvoering geven aan een bevel tot het opnemen van vertrouwelijke communicatie. In een regeling worden de eisen weergegeven waaraan deze politiefunctionarissen moeten voldoen.[220] De minister heeft sterk benadrukt dat anderen dan de aangewezen ambtenaren niet tot plaatsing bevoegd zullen zijn.[221]

3.6 Stelselmatige observatie en locatiebepaling

Stelselmatige observatie en locatiebepaling zijn bevoegdheden die primair een fysieke component hebben en dus niet als zodanig direct van toepassing zijn op internet. Wel hebben ze een ICT-component die steeds belangrijker wordt naarmate observatie- en tracking-technologie geavanceerder wordt. Dit maakt het relevant om de opsporingsbevoegdheden in dit hoofdstuk te bespreken. We combineren observatie en locatiebepaling hier, omdat deze traditioneel sterk met elkaar te maken hebben: het volgen van iemand in de publieke ruimte is immers een vorm van observatie waarbij de (vaak letterlijke) wandelgangen van iemand worden gevolgd.[222] Er is echter een scala aan methoden beschikbaar voor beide toepassingen, wat betekent dat de bevoegdheden behorend bij observatie en locatiebepaling niet altijd samenvallen.

3.6.1 *Stelselmatige observatie*

Volgens artikel 126g Sv kan de officier van justitie een opsporingsambtenaar bevelen stelselmatig een persoon te volgen of stelselmatig diens aanwezigheid of gedrag waar te nemen. Dat kan bij verdenking van elk misdrijf. Er is sprake van stelselmatigheid indien een "min of meer volledig beeld van bepaalde aspecten van iemands leven wordt verkregen".[223] Bij de vraag of sprake is van stelselmatigheid spelen factoren als gebruik van een technisch hulpmiddel (dat verder gaat dan simpele versterking van de zintuigen), plaats, frequentie, intensiteit en duur een belangrijke rol.[224] Niet-stelselmatige observatie kan worden gebaseerd op het algemene taakstellende artikel 3 Politiewet 2012. Jurisprudentie laat zien dat zeer verschillend wordt gedacht over de vraag of een bepaalde observatie stelselmatig is.[225] Het zestig maal waarnemen van het gedrag van

220 Regeling opnemen vertrouwelijke communicatie politie van 10 januari 2000, *Stcrt.* 11 januari 2000, nr. 7, p. 10; Regeling vakbekwaamheid technische hulpmiddelen strafvordering, *Stcrt.* 27 december 2006, nr. 251, p. 7.

221 *Kamerstukken II* 1996/97, 25403, 3, p. 79 en *Kamerstukken I* 1998/99, 25403 en 23251, 119b, p. 4.

222 Vgl. artikel 40 Wiv 2017, waarin deze vormen bij elkaar in één regeling zijn geplaatst.

223 *Kamerstukken II* 1996/97, 25403, 3, p. 26. Zie Buruma 2000 en Haverkate 2000 voor een discussie over het stelselmatigheidsbegrip. Zie ook Commissie-Koops 2018 voor een voorstel tot uitbreiding en uitwerking van dit criterium in het digitale tijdperk.

224 Zie onder andere *Kamerstukken II* 1996/97, 25403, 3, p. 26-27 en *Kamerstukken II* 1998/99, 26671, 7, p. 46. Zie ook HR 12 februari 2002, *NJ* 2002/301, ECLI:NL:HR:2002:AD7804, paragraaf 3.4. Zie Koops 2016, p. 28-29 voor een samenvattend overzicht.

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

een verdachte binnen 27 maanden wil immers nog niet zeggen dat toepassing van de bijzondere opsporingsbevoegdheid is vereist.[226]

In artikel 126g lid 3 Sv is geëxpliciteerd dat de officier van justitie kan bepalen dat ter uitvoering van het bevel een technisch hulpmiddel wordt gebruikt voor zover daarmee geen vertrouwelijke communicatie wordt opgenomen. Een technisch hulpmiddel in deze zin heeft de wetgever wel aangeduid als "een apparaat, dat iets geavanceerder is dan een huis-, tuin- en keukenverrekijker".[227] Een technisch hulpmiddel mag overigens niet op een persoon worden bevestigd, tenzij met diens toestemming (artikel 126g lid 3 Sv). Een peilzender mag wel worden gebruikt op bijvoorbeeld een koffer of personenauto die aan een specifieke persoon gekoppeld is; ook hierbij is dan sprake van stelselmatige observatie, in tegenstelling tot bijvoorbeeld een peilzender die aan een containerschip verbonden is en waarmee geen personen worden geobserveerd.[228]

Een uitgangspunt bij de Wet BOB was dat het belang van het huisrecht zwaarder weegt dan het belang van de opsporing om binnen te kunnen treden om heimelijk te kunnen vastleggen wat zich binnen de woning afspeelt. Er kan daarom niet in de woning worden binnengetreden om heimelijk camera's te plaatsen.[229] Wel is observatie van buitenaf in de woning mogelijk "voor zover het gaat om waarnemingen die zonder technische manoeuvres kunnen plaatsvinden: hetgeen normaal gesproken van buiten af zichtbaar is, mag worden waargenomen".[230] De wetgever heeft enigszins in het midden gelaten in welke mate met een technisch hulpmiddel van buitenaf in de woning mag worden geobserveerd. Het is niet toegestaan met een camera 'permanent' waar te nemen wat zich in een woning afspeelt;[231] dat sluit echter niet uit dat een "rechercheur met een camera in de bosjes plaatsneemt, en alle voor strafvorderlijke beslissingen relevante gedragingen daarop vastlegt", zolang maar niet "een 'onbemande' camera alle gedragingen die zich in het desbetreffende huis afspelen van a tot z vastlegt".[232] De wetsgeschiedenis laat hiermee een behoorlijke bandbreedte open voor bemande camera's in bosjes, evenals overigens voor onbemande (bijvoorbeeld 'slimme') camera's die incidentele (dus niet permanente of alle gedragingen betreffende) opnamen maken. Iets strikter is de Aanwijzing opsporingsbevoegdheden, die het "plaatsen van een camera (met zicht) in een woning" uitsluit, maar daarmee wel de mogelijkheid openlaat van met camera's uitgeruste rechercheurs die van buitenaf naar binnen kijken.[233]

---

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

227 *Kamerstukken II* 1996/97, 25403, 3, p. 70. Elders duidt de wetgever aan: "Betreft het een zintuigversterkend hulpmiddel, zoals een verrekijker, of een camera die als oog fungeert (dus zonder te registreren) dan gelden hiervoor geen bijzondere voorwaarden. Betreft het observatie van een persoon met behulp van een technisch hulpmiddel dat over een kortere of langere periode signalen registreert, dan moet dit in beginsel worden beschouwd als stelselmatige observatie. Hieronder valt niet het incidenteel maken van een of enkele foto's". *Kamerstukken II* 1996/97, 25403, 3, p. 27.

228 *Kamerstukken II* 1996/97, 25403, 3, p. 28.

229 *Kamerstukken II* 1996/97, 25403, 3, p. 43. Zie ook Koops, Van Schooten & Prinsen 2004, p. 66-71 en 105-108.

230 *Kamerstukken II* 1996/97, 25403, 3, p. 70-71.

231 *Kamerstukken II* 1996/97, 25403, 3, p. 71.

232 *Kamerstukken II* 1997/98, 25403, 7, p. 66.

233 Aanwijzing opsporingsbevoegdheden, *Stcrt.* 2014, nr. 24442, paragraaf 2.2.

De wetgever heeft het belang van deze bevoegdheid in de digitale sfeer niet genoemd. Toch kan de bevoegdheid van belang zijn, vooral in verband met het zoeken en vastleggen van gegevens op internet. De wetgever heeft bij de Wet BOB aangegeven dat opsporingsambtenaren in principe vrijelijk kunnen rondstruinen op internet en noteren en binnenhalen wat zij daar tegenkomen.[234] Daarbij stond de wetgever vermoedelijk een politieagent voor ogen die handmatig googelt en surft op het internet zoals dat er destijds uitzag. Wanneer het zoeken echter een stelselmatig karakter krijgt (wat anno nu veel sneller het geval zal zijn dan in 1999), doordat een "min of meer volledig beeld van bepaalde aspecten van iemands leven" wordt verkregen, zal hiervoor een bevel van de officier van justitie nodig zijn (zie uitgebreid paragraaf 3.8 en specifiek in relatie tot stelselmatige observatie paragraaf 3.8.3).

3.6.2 *Locatiebepaling*

Zoals opgemerkt kan stelselmatige observatie worden ingezet om een persoon fysiek te volgen in de publieke ruimte, door een observant of met bijvoorbeeld een peilbaken op de auto. Van belang is wel dat, ingevolge artikel 126g lid 3 Sv, peilbakens niet op een persoon (zonder diens toestemming) mogen worden bevestigd. Onder dit verbod valt "plaatsbepalingsapparatuur die wordt aangebracht in een aansteker of pen die in of op de kleding wordt gedragen".[235] Wel kan plaatsbepalingsapparatuur worden geplaatst op een koffer (en vergelijkbare losse zaken die iemand veelal meeneemt maar niet in of op de kleding draagt).[236] In deze zin is het door een observant of met peilbakens in kaart brengen van iemands bewegingen een belangrijke toepassing van stelselmatige observatie.

Er zijn echter diverse andere methoden die kunnen worden gebruikt om iemands locatie te bepalen.[237] Dit kan twee verschillende toepassingen hebben: het volgen van iemands bewegingen over een bepaalde periode, bijvoorbeeld om in kaart te brengen met wie een verdachte allemaal contact heeft of patronen te vinden in diens gedrag; of het vaststellen van iemands locatie op een bepaald moment, bijvoorbeeld om hem te kunnen aanhouden of andere opsporingsmethoden te kunnen inzetten zodra bekend is waar de verdachte zich bevindt.

Naast fysiek volgen en het plaatsen van peilbakens op auto's kunnen iemands bewegingen ook worden gevolgd door de locatie van de mobiele telefoon over een periode te volgen. Bij locatiebepaling via de mobiele-telefoonsignalen wordt de inhoud van telefoongesprekken niet afgeluisterd en fungeert de mobiele telefoon feitelijk als een soort peilzender. Locatiegegevens kunnen echter niet worden gevorderd op basis van de ob-

234 *Kamerstukken II* 1998/99, 26671, 3, p. 38.

235 *Kamerstukken II* 1996/97, 25403, 3, p. 71. Zie ook *Kamerstukken II* 2015/16, 34372, 3, p. 27. Bij de Wet computercriminaliteit III is artikel 126g lid 3 Sv aangepast om een uitzondering te maken op het verbod wanneer artikel 126nba Sv wordt toegepast, oftewel wanneer van afstand wordt binnengedrongen in apparaten die iemand in of op de kleding draagt, zoals een smartphone, ter ondersteuning van stelselmatige observatie.

236 *Kamerstukken II* 1996/97, 25403, 3, p. 71.

237 Zie Koops, Newell & Škorvánek 2019 voor een overzicht.

servatiebevoegdheid: artikel 126g Sv legitimeert niet tot het vorderen van gegevens bij een telecomaanbieder.[238] Daarvoor moet dus de bevoegdheid tot het vorderen van (verkeers)gegevens worden gebruikt (zie paragraaf 3.3.3). Overigens mag artikel 126n Sv volgens de toelichting worden gebruikt om frequent verkeersgebonden locatiegegevens op te vragen, ook als daarmee een persoon stelselmatig kan worden gevolgd en het opvragen van de gegevens het karakter krijgt van observatie.[239]
Locatiegegevens van mobiele telefoons worden echter alleen geregistreerd door aanbieders als een toestel feitelijk aan het communiceren is, niet als het toestel alleen stand-by staat. Afhankelijk van verdachtes communicatiepatroon zal dus meer of minder zicht op diens locaties ontstaan door verkeersgegevens te vorderen. Om actief verkeers- en dus ook locatiegegevens te genereren, is de methode van de 'stille sms' (stealth-sms) ontwikkeld, waarbij heimelijk (dus niet zichtbaar) een sms naar het gezochte toestel wordt gestuurd. 'Stille sms' om de verdachte te localiseren mag alleen worden ingezet voor zover het niet op stelselmatige wijze plaatsvindt en een "min of meer volledig beeld van bepaalde aspecten van het privéleven wordt verkregen".[240] De politie en het Openbaar Ministerie hebben een intern beleid vastgesteld, waarbij een officier van justite een bevel afgeeft voor de inzet van stille smsjes als opsporingsmiddel en het gebruik van het opsporingsmiddel wordt geverbaliseerd (artikel 152 Sv).[241]
In het conceptwetsvoorstel voor Boek 2 in het gemoderniseerde wetboek wordt voorgesteld een wettelijke grondslag te scheppen voor stelselmatige locatiebepaling (artikel 2.8.2.10.1). Het gaat om het "met een technisch hulpmiddel op stelselmatige wijze bepalen van de locatie van een persoon", vormgegeven als steunbevoegdheid die dient voor de uitoefening van andere bevoegdheden.[242] Naast de stille sms wordt hiermee ook het gebruik van de IMSI-catcher (zie paragraaf 3.3.2) gereguleerd als die wordt gebruikt in het kader van locatiebepaling. Door de techniekonafhankelijke formulering komen echter ook tal van andere methoden in beginsel in aanmerking voor uitvoering van locatiebepaling. Totdat het nieuwe wetboek in werking is, moet de praktijk het echter doen met de huidige catalogus aan bevoegdheden, waarbij locatiebepaling afhankelijk van de methode en inzet kan worden gebaseerd op stelselmatige observatie, vorderen van verkeersgegevens of – indien beperkt tot een geringe privacyinbreuk – artikel 3 Polw 2012.

3.7 Hacken als opsporingsbevoegdheid

Hacken als opsporingsbevoegdheid is een paraplubegrip, waarbij het kenmerkend is dat opsporingsambtenaren zich heimelijk en op afstand toegang verschaffen tot een

238 *Kamerstukken II* 2001/02, 28059, 3, p. 9.
239 *Kamerstukken II* 2001/02, 28059, 3, p. 8-9.
240 Zie HR 1 juli 2014 ECLI:NL:HR:2014:1563, *NJ* 2015/114, m.nt. P.H.P.H.M.C. van Kempen.
241 Zie antwoord op Kamervragen van 9 mei 2014 van de leden Gesthuizen, Kooiman, Berndsen-Jansen en Schouw over het gebruik van stealth-sms'jes door opsporingsinstanties voor opsporingsdoeleinden.
242 Zie Commissie-Koops 2018, p. 169-175 voor een analyse, met aanbeveling om de steunbevoegdheid ook mogelijk te maken ter aanhouding van de verdachte.

geautomatiseerd werk.[243] Veelal zal dit gebeuren door het op afstand (doen) installeren van een technisch hulpmiddel (zoals een Trojaans paard of andere monitoringssoftware), waarmee vervolgens tal van handelingen mogelijk zijn, zoals het bekijken en kopiëren van gegevens, het heimelijk aanzetten van microfoon of camera, en het ontoegankelijk maken van gegevens.

Wij gebruiken in dit hoofdstuk hiervoor de term 'hacken', als compacte en duidelijkste aanduiding van waar de bevoegdheid op neerkomt. Opsporingsinstanties zijn het oneens met het gebruik van de term in dit verband, omdat 'hacken' duidt op *onrechtmatig* binnendringen van computers, terwijl de politie – althans waar gebaseerd op de wettelijke bevoegdheid – niet onrechtmatig handelt. Wij vinden dat geen doorslaggevend argument tegen de term – bevoegdheden worden wel vaker aangeduid met een term die ook een strafbare handeling aanduidt, zoals 'aftappen', terwijl artikel 139c Sr het *wederrechtelijk* aftappen of opnemen van communicatie strafbaar stelt.[244]

Hoewel in het verleden wel is betoogd dat de politie bevoegd was te hacken op basis van bestaande bevoegdheden,[245] bestond daarvoor tot 2019 geen juridische basis, met uitzondering van het hacken ter plaatsing van afluistersoftware in het kader van artikel 126l Sv.[246] Een voorbeeld daarvan is te vinden in de recente *Aydin C.*-zaak.[247] De politie installeerde na een fysieke inbraak software op C.'s computer, waarbij door middel van 'vinkjes' in het softwareprogramma werd aangegeven dat toetsaanslagen en schermafbeeldingen moesten worden vastgelegd. Het vastleggen van toetsaanslagen, nog voordat ze zijn gecommuniceerd of door versleuteling onbegrijpelijk zijn geworden, is mogelijk op basis van artikel 126l Sv.[248] De vraag is wel of het maken van schermafbeeldingen is toegestaan in het kader van direct afluisteren; zoals in paragraaf 3.5 gesteld, lijkt ons dat op zich mogelijk, mits het alleen gebeurt op momenten dat er naar redelijke verwachting communicatie zichtbaar is op het scherm. Of dat in casu het geval was (en of dat überhaupt technisch mogelijk is), kunnen we op basis van de rechtszaak niet beoordelen.

De voorbereidingen voor het invoeren van een 'hackbevoegdheid' zijn terug te voeren tot 2009. In een Kamerbrief uit 2009 gaf de toenmalige minister van Justitie aan dat het opsporen van cybercrime door anonimiseringstechnieken en encryptie 'extreem gecompliceerd' is geworden.[249] Om met deze problematiek om te gaan is in de Wet computercriminaliteit III een nieuwe opsporingsbevoegdheid voorgesteld om hacken mo-

243 Zie Oerlemans 2011 en Koning 2012.

244 Wanneer men expliciet wil benadrukken dat de politie bevoegd is om op afstand binnen te dringen, kan hiervoor eventueel de term *legal hacking* worden gebruikt, zoals interceptie door politie ook wel met *legal interception* wordt aangeduid.

245 Boek 2000.

246 Koops & Buruma 2007, p. 118-119.

247 Rb. Amsterdam 16 maart 2017, ECLI:NL:RBAMS:2017:1627, *Computerrecht* 2017/103, nr. 3, p. 169-180, m.nt. J.J. Oerlemans (*Aydin C.*).

248 *Kamerstukken II* 1996/97, 25403, 3, p. 35-36.

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

gelijk te maken.[250] De 'hackbevoegdheid' – officieel het "toegang verschaffen op afstand tot een geautomatiseerd werk" genoemd – is nu geregeld in artikel 126nba Sv.
De benaming van de nieuwe achtste afdeling waarin artikel 126nba Sv is ondergebracht, "Onderzoek in een geautomatiseerd werk", is ongelukkig. Er zijn immers ook vele andere bevoegdheden (zoals die uit de afdeling "Doorzoeking ter vastlegging van gegevens") die eveneens onderzoek in computers regelen. Verder dekt het de lading niet, omdat het niet alleen gaat om onderzoek *in* een computer, maar ook om het onderzoeken van wat er gebeurt in de omgeving van de computer: het binnendringen in de computer voor direct afluisteren (via de microfoon) of observatie (via de camera); dit zijn andere opsporingshandelingen en kan men moeilijk als '*onderzoek in* een computer' aanduiden.[251]

In deze paragraaf wordt eerst de achtergrond besproken voor invoering van de nieuwe opsporingsbevoegdheid (paragraaf 3.7.1). Vervolgens worden de voorwaarden voor de inzet van de nieuwe bevoegdheid besproken (paragraaf 3.7.2). Daarna worden de afzonderlijke toepassingen van de bijzondere opsporingsbevoegdheid behandeld, namelijk de online doorzoeking (paragraaf 3.7.3), de inzet van politiesoftware voor uiteenlopende doelen (paragraaf 3.7.4) en het op afstand ontoegankelijk maken van gegevens (paragraaf 3.7.5).

3.7.1 *Achtergrond: anonimiteit, versleuteling en deterritorialisering*

In cybercrime-onderzoeken kan de identificatie en lokalisering van verdachten bijzonder lastig zijn, omdat verdachten veelal gebruikmaken van verschillende wifi-netwerken en anonimiseringstechnieken, zoals proxy-diensten, VPN-diensten en het Tor-netwerk.[252] Als gevolg daarvan wijzigt het IP-adres van bijvoorbeeld het thuisnetwerk waarvan de verdachte normaal gesproken gebruikmaakt. De gebruikersgegevens die horen bij het IP-adres dat door een bepaalde online dienstaanbieder wordt uitgegeven, zijn in dat geval niet beschikbaar of niet meer direct herleidbaar tot de verdachte.
Illustratief is een zaak waarin een leerling van het Maerlant College in Den Haag het bericht *"Tomorrow I'll go and kill some peeps from my old school, the Maerlant college in The Hague"* plaatste op *4Chan.org*. Op dit forum kunnen gebruikers het pseudoniem '*Anonymous*' gebruiken,[253] maar het ligt wel voor de hand dat een IP-adres wordt gelogd. De Nederlandse politie kwam via het (rechtstreeks of via rechtshulpverzoek verkregen) IP-adres en de daarbij behorende gebruikersgegevens die bij de Nederlandse internetaanbieder waren gevorderd, uit bij het adres van de buren van de verdachte. De

250 In de praktijk is het wetsvoorstel enige malen ingezet op basis van artikel 125i Sv jo. artikel 94 Sv (zie voor een overzicht: Oerlemans 2017a, p. 258-261). Zie ook het Antwoord op Kamervragen van 17 oktober 2014 over het hacken van servers door de politie terwijl de zogenoemde hackwet nog niet door de Kamer is behandeld.
251 Koops, Conings & Verbruggen 2016, p. 39-40.
252 Zie ook Bernaards, Monsma & Zinn 2012, p. 61.
253 De naam 'Anonymous' is overgenomen door de 'hacktivisten'-groep Anonymous. Deze losgeorganiseerde groep pleegt computerdelicten met het doel aandacht te vestigen op een politiek of ideologisch doel.

getuigenis van de onschuldige buren dat ze de inloggegevens hadden gedeeld met een jongeman even verderop leidde uiteindelijk tot de verdachte. Zijn bekentenis en een tijdelijk bestand op zijn computer met de bedreiging als inhoud gaven voldoende bewijs.[254] Merk op dat de verdachte wellicht niet getraceerd had kunnen worden als hij ongemerkt het wifi-netwerk had gehackt van mensen waarmee hij geen enkele relatie had.[255] Het hangt dus vaak af van de technieken en beveiligingsmaatregelen die een verdachte gebruikt of hij anoniem kan blijven.

Wanneer gebruik wordt gemaakt van een VPN-dienstverlener die, anders dan de meeste reguliere VPN-aanbieders, als onderdeel van zijn verdien- of gebruikersmodel zo anoniem mogelijk internet verschaft, kan het onder omstandigheden onmogelijk zijn een internetgebruiker te identificeren.[256] Cruciale gegevens voor de identificering van een internetgebruiker zijn in dat geval door de architectuur van het systeem of door een bewuste keuze niet meer beschikbaar.

Tor, een afkorting voor 'The Onion Router', is een voorbeeld van een systeem om internetverkeer zo veel mogelijk te anonimiseren. Het systeem versleutelt internetverkeer en routeert netwerkverkeer door verschillende 'relays' (of 'nodes') in het netwerk, van degenen die het Tor-programma hebben gedownload en gebruiken. Elke relay kent de voorgaande en volgende relay, maar geen enkele kent de gehele route. Zo voorkomt Tor dat er een link wordt gelegd tussen het begin- en eindpunt van het netwerkverkeer.[257] Tor kan worden gebruikt door onschuldige mensen die simpelweg anoniemer willen internetten vanwege privacy- of veiligheidsoverwegingen. Het is in de loop der jaren echter ook helder geworden dat het systeem vaak wordt gebruikt door misdadigers die anoniemer in drugs willen handelen, illegale diensten willen aanbieden of kinderpornografie willen verspreiden en downloaden.[258] Het Tor-systeem maakt het ook mogelijk websites en online diensten te benaderen die exclusief via het Tor-programma toegankelijk zijn; deze diensten worden ook wel 'hidden services' genoemd en zijn samen onderdeel van het '*dark web*': dat gedeelte van internet waarbij de IP-adressen van de computers verborgen zijn.[259]

Door toepassing van hacken als opsporingsmethode is het mogelijk *rechtstreeks* toegang te verschaffen tot de computer waarvan een verdachte gebruikmaakt. Ook is het

254 Zie Rb. Den Haag 2 april 2010, ECLI:NL:RBSGR:2010:BM1481, Hof Den Haag 9 maart 2011, ECLI:NL:GHSGR:2011:BP7080 en HR 26 maart 2013 ECLI:NL:HR:2013:BY9718.

255 Een modus operandi waarbij hackers rondrijden in busjes op zoek naar een slecht beveiligd wifi-netwerk om te hacken, wordt ook wel '*war driving*' genoemd (zie bijvoorbeeld Bryant e.a. 2008, p. 113).

256 Zie uitgebreid Oerlemans 2017a. Zie ook Bernaards, Monsma & Zinn 2012, p. 61.

257 Zie https://www.eff.org/torchallenge/what-is-tor.html en https://www.torproject.org/about/overview.html.en (laatst geraadpleegd 1 juli 2018).

258 Zie Bernaards, Monsma & Zinn 2012, p. 62, Europol 2015b, p. 19 en Moore & Rid 2016, p. 21. In Nederland werd veel media-aandacht besteed aan het gebruik van Tor door de kinderpornogebruiker Robert M., die veroordeeld is voor het misbruik van 84 kinderen en het bezit, verspreiden en vervaardigen van kinderpornografie (Rb. Amsterdam 23 juli 2012, ECLI:NL:RBAMS:2012:BX2325). Zie ook het persbericht van het Openbaar Ministerie van 31 augustus 2011, 'Kinderporno op anonieme, diep verborgen websites'.

259 Andy Greenberg, 'Hacker Lexicon: What Is the Dark Web?', *Wired*, 19 november 2014. Het *dark web* moet worden onderscheiden van het *deep web*, het deel van internet dat wel open IP-adressen kent maar dat niet via zoekmachines zoals Google doorzoekbaar is.

mogelijk met behulp van een programma (ook wel 'policeware'[260] genoemd, zijnde de goedaardige variant van malware), het echte IP-adres van de gebruiker en andere identificerende gegevens naar opsporingsdiensten toe te sturen.[261] De anonimiseringsmaatregelen of technieken die de verdachte heeft genomen, zijn in die gevallen nutteloos. Toch moet men zich realiseren dat het niet altijd mogelijk zal zijn de computer waar een verdachte gebruik van maakt te hacken. Het is onder andere afhankelijk van het type apparaat en de beveiligingsmaatregelen die een verdachte heeft genomen of het haalbaar en kosteneffectief is de computer van de verdachte op afstand binnen te dringen.

Naast anonimisering is ook het toenemend gebruik van (end-to-end) encryptie een belangrijke reden voor de invoering van hacken als opsporingsbevoegdheid (zie nader paragraaf 3.2.5 en 3.4.7). Hacken draagt als opsporingsmethode bij aan de oplossing van dit probleem, omdat, nadat op afstand toegang is verkregen tot een geautomatiseerd werk, de politie op afstand "op de bron" kan aftappen door gesprekken via een microfoon of camerabeelden op te nemen en door te sturen naar een politieserver,[262] of door elektronische berichten in klare tekst te onderscheppen voordat deze versleuteld, of nadat deze ontsleuteld, zijn. Met de zogenoemde 'keylog'-functionaliteit van politiesoftware kunnen bovendien inlognamen en wachtwoorden van computergebruikers worden vastgelegd, zodat deze later kunnen worden gebruikt voor toegang tot beveiligde gegevens.[263]

Ten slotte is de hackbevoegdheid nadrukkelijk ook geïntroduceerd om met het probleem van cloud computing in opsporingsonderzoeken om te gaan.[264] Bij gebruik van cloud computing is het vaak niet meer redelijkerwijs vast te stellen waar gegevens zich op enig moment bevinden. Deze bevinden zich vaak (verspreid) op servers in datacentrums in het buitenland. Met de inzet van de hackbevoegdheid kunnen opsporingsambtenaren – voor zover aan alle voorwaarden van de voorgestelde bevoegdheid wordt voldaan – webmail-accounts of accounts die worden gebruikt voor online opslagdiensten hacken om een 'online doorzoeking' van het account uit te voeren.[265]

3.7.2 *Algemene schets van de regeling en voorwaarden*

De 'hackbevoegdheid' in artikel 126nba Sv is gelaagd opgebouwd. In het eerste deel wordt de bevoegdheid omschreven waarmee opsporingsambtenaren zich op afstand

260 Zie Jacobs 2012.
261 *Kamerstukken II* 2015/16, 34372, 3, p. 20.
262 *Kamerstukken II* 2015/16, 34372, 3, p. 10.
263 Zie Oerlemans 2011 en, in enigszins andere bewoordingen, *Kamerstukken II* 2015/16, 34372, 3, p. 21.
264 Zie ook *Kamerstukken II* 2015/16, 34372, 3, p. 11-12.
265 Daarbij moet wel worden opgemerkt dat zich hierbij mogelijk problemen met betrekking tot de territoriale soevereiniteit van andere staten kunnen voordoen. In dit boek wordt daarop niet uitgebreid ingegaan. Zie bijvoorbeeld Koops 2012a, Koops & Goodwin 2014 en Oerlemans 2017a, p. 293-356 voor meer informatie over het onderwerp.

toegang verschaffen tot een geautomatiseerd werk. Daarbij mogen opsporingsambtenaren de volgende vijf opsporingshandelingen inzetten:

1. het vaststellen van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker, zoals de identiteit of locatie, en de vastlegging daarvan;
2. het opnemen van communicatie, zoals bedoeld in artikel 126l Sv of 126m Sv;
3. het stelselmatig observeren van gedrag van een persoon met een technisch hulpmiddel, zoals bedoeld in artikel 126g Sv;
4. het vastleggen van gegevens die in een computer zijn, of tijdens de uitvoering worden, opgeslagen; en
5. de ontoegankelijkheidsmaking van gegevens, als bedoeld in (het nieuwe) artikel 126cc lid 5 Sv.[266]

De officier van justitie en rechter-commissaris (lid 4) evenals de Centrale Toetsingscommissie[267] zullen elk een afweging maken of inzet van de bevoegdheid proportioneel en subsidiair is, mede in het licht van de omstandigheden van het geval. De bijzondere opsporingsbevoegdheid mag verder slechts worden ingezet in opsporingsonderzoeken naar misdrijven zoals omschreven in artikel 67 Sv die de rechtsorde ernstig schaden en voor zover dat strikt noodzakelijk is (lid 1). De inzet ten behoeve van de online doorzoeking en het ontoegankelijk maken van gegevens is verder beperkt tot misdrijven met een gevangenisstraf van maximaal acht jaar of meer, dan wel misdrijven die bij Algemene Maatregel van Bestuur worden aangewezen. In deze AMvB worden typische cybercrimes opgenomen, zoals (het bezit, verspreiding en vervaardiging) van kinderporno, het gebruik van botnets (als gekwalificeerde variant van computervredebreuk) en grooming.[268] In de AMvB worden echter veel meer misdrijven aangewezen, zoals mensensmokkel, witwassen, bommeldingen en het gebruik van een valse betaalpas,[269] met het argument dat het gaat om ernstige commune delicten die zich verplaatsen naar internet ('gedigitaliseerde misdaad') en dat er vaak geen andere opsporingsmethoden voorhanden zijn dan hacken.[270]

Na afloop van het onderzoek moet de *policeware* worden verwijderd, tenzij dit niet (geheel) mogelijk is; als het laten staan van de software risico's oplevert voor het functioneren van het geautomatiseerd werk (wat veelal het geval zal zijn, er is immers een achterdeur aangebracht waardoor ook anderen dan de politie naar binnen kunnen) dan moet de beheerder worden genotificeerd met informatie ten behoeve van volledige verwijdering (lid 6).

Belangrijke voorwaarden zijn voorts dat alleen speciaal geautoriseerde en opgeleide politieambtenaren het binnendringen (oftewel het vervaardigen en doen installeren van de *policeware*) mogen uitvoeren (lid 8 onder a), waarbij functiescheiding plaats-

266 Zie ook uitgebreid *Kamerstukken II* 2015/16, 34372, 3, p. 21-31.
267 *Kamerstukken II* 2015/16, 34372, 3, p. 37-38.
268 Artikel 2 Besluit onderzoek in een geautomatiseerd werk, *Stb.* 2018, 340. Zie ook *Kamerstukken II* 2016/17, 34372, 6, p. 59.
269 *Ibid.*
270 *Kamerstukken II* 2017/18, 34372, 27, p. 4-6.

vindt tussen het technisch team en het tactisch team;[271] dit voorkomt misbruik van de (functionaliteiten van de) software. Ook moet de uitvoering van het hacken worden gelogd (lid 8 onder b), zodat het gebruik van de hacksoftware traceerbaar en betwistbaar is voor de verdediging en controleerbaar voor de rechter.[272] De logplicht beslaat alle aspecten: het gaat om inzetlogging, bewijslogging, systeemlogging en autorisatie- en authenticatielogging.[273] Een interessante vraag hierbij is in hoeverre de verdediging een deskundige kennis mag laten nemen van de logging,[274] waar nodig afgeschermd onder toezicht van de rechter-commissaris of zittingsrechter. Wat ons betreft zou dit tot de mogelijkheden moeten behoren.
De Inspectie Justitie en Veiligheid houdt toezicht op de inzet van *policeware* door de politie en het Openbaar Ministerie. Tijdens de parlementaire behandeling is in verschillende stadia gediscussieerd over het stelsel van toezicht.[275] Staatssecretaris Dijkhoff legde daarbij uit dat de Inspectie [toen nog] Veiligheid en Justitie achteraf toezicht houdt op de inzet van de hackbevoegdheid,[276] wat vervolgens bij nota van wijziging is geëxpliciteerd in een nieuw lid 7.[277] Het toezicht ziet echter in de eerste plaats op het nakomen van de voorgeschreven procedures en niet op de rechtmatigheid van de toepassing van de bevoegdheid. In de Eerste Kamer werd aangedrongen op een meer onafhankelijke vorm van (systeem)toezicht, maar een motie van die strekking van Strik e.a.[278] haalde het niet, vermoedelijk mede omdat de minister toezegde de in de wet opgenomen evaluatietermijn van vijf jaar te verkorten tot twee jaar.[279]

De kritiek op de hackbevoegdheid en het parlementaire debat over het wetsvoorstel betroffen vooral de reikwijdte van de hackbevoegdheid en het gebruik van kwetsbaarheden om bij computers van verdachten binnen te komen. De hackbevoegdheid beperkt zich namelijk niet tot laptops, pc's en smartphones van verdachten, maar kan worden ingezet voor het binnendringen in álle geautomatiseerde werken. Daaronder vallen ook apparaten binnen het Internet of Things, zoals slimme meters, lampen, en slimme auto's, alsmede kritische apparaten als pacemakers. In de wetsgeschiedenis is aangegeven dat het hacken van een pacemaker of auto al snel disproportioneel is van-

271 *Kamerstukken II* 2015/16, 34372, 3, p. 54. Zie voor een uitleg van de werking hiervan de nota van toelichting bij het Besluit onderzoek in een geautomatiseerd werk, *Stb.* 2018, 340, p. 14-15.
272 *Kamerstukken II* 2015/16, 34372, 6, p. 59.
273 *Kamerstukken II* 2017/18, 34372, 27, p. 8. Zie ook de nota van toelichting bij het Besluit onderzoek in een geautomatiseerd werk, *Stb.* 2018, 340, p. 17-18.
274 Zie in dit kader ook Rb. Amsterdam 16 maart 2017, ECLI:NL:RBAMS:2017:1627, *Computerrecht* 2017/103, nr. 3, p. 169-180, m.nt. J.J. Oerlemans (*Aydin C.*).
275 Zie ook de bijdrage van de heer Baardman, senior raadsheer van het Gerechtshof Den Haag en coördinator van het Kenniscentrum Cybercrime, aan een debat over het wetsvoorstel op 10 februari 2016 in de Tweede Kamer en verschillende bijdragen aan de deskundigenbijeenkomst in de Eerste Kamer, *Kamerstukken I* 2016/17, 34372, E herdruk.
276 *Kamerstukken II* 2016/17, 34372, 6, p. 82-83.
277 *Kamerstukken II* 2016/17, 34372, 7.
278 *Kamerstukken I* 2017/18, 34372, J.
279 *Handelingen I* 19 juni 2018, EK 34-5-16.

wege de grote risico's met betrekking tot de veiligheid van personen die het hacken van deze apparaten met zich meebrengt.[280]
Het tweede punt van kritiek richt zich op het gebruik van kwetsbaarheid 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 meebrengt. De redenering hierbij 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.[281] Uiteindelijk heeft deze discussie geleid tot het aangenomen amendement Recourt/Tellegen, waarbij een verplichting is geïntroduceerd onbekende kwetsbaarheden te melden die bij de politie bekend zijn geworden bij toepassing van de hackbevoegdheid.[282] Slechts bij een zwaarwegend opsporingsbelang kan, na accordering van het centraal aanspreekpunt bij het Landelijk Parket, worden besloten een rechter-commissaris toestemming te vragen om de melding van de onbekende kwetsbaarheid uit te stellen (artikel 126ffa Sv).[283]

3.7.3 *De verschillende functionaliteiten en toepassingen*

Politiesoftware kan veel functionaliteiten bevatten. Volgens de memorie van toelichting moet worden gedacht aan:
1. het opnemen van geluid (via de microfoon);
2. het vastleggen en doorsturen van toetsaanslagen;
3. het maken van screenshots;
4. het aanzetten van de camera; en
5. het creëren van een achterdeurtje voor toegang op afstand.[284]

280 Zie *Kamerstukken II* 2016/17, 34372, 6, p. 32 en *Kamerstukken I* 2016/17, 34372, D, p. 30.
281 Overigens wijzen sommige cybersecuritydeskundigen erop dat in veel gevallen geen gebruik hoeft te worden gemaakt van onbekende kwetsbaarheden voor het hacken van apparaten, omdat bekende kwetsbaarheden vaak volstaan. Daarnaast zijn onbekende kwetsbaarheden zeer kostbaar en slechts kort bruikbaar, zeker als de politie verplicht is tot het gelijk melden van de kwetsbaarheid. Zie bijvoorbeeld de bijdrage van de heer Prins aan de deskundigenbijeenkomst in de Eerste Kamer over het wetsvoorstel computercriminaliteit III, *Kamerstukken I* 2016/17, 34372, E herdruk, p. 41 en 45.
282 *Kamerstukken II* 2016/17, 30372, 14.
283 Zie ook *Kamerstukken I* 2016/17, 34372, D, p. 20-21. De staatssecretaris geeft aan dat de politie geen onbekende kwetsbaarheden zal inkopen, maar sluit niet dat van onbekende kwetsbaarheden gebruikt wordt gemaakt door de software die de politie aanschaft om de hackbevoegdheid uit te voeren. In een tamelijk unieke brief van 23 november 2016 (*Kamerstukken II* 2016/17, 26643, 428) zetten de staatssecretaris van Veiligheid en Justitie en de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Defensie hun gezamenlijke standpunt uiteen over het omgaan met kwetsbaarheden en het beleid met een expliciete afweging omtrent het melden van onbekende kwetsbaarheden.
284 *Kamerstukken II* 2015/16, 34372, 3, p. 21-24.

Gezien de werking van commercieel verkrijgbare *policeware* van FinFisher en Hacking Team, wordt de politiesoftware vaak op pc's of mobiele telefoons geïnstalleerd.[285] Gelet op de hoeveelheid gegevens die op computers en smartphones staan in combinatie met de lijst van mogelijke functionaliteiten, is duidelijk dat het gebruik van *policeware* veelal andere gegevens oplevert dan een telefoon- of internettap en bovendien een andere, verdergaande privacy-inmenging voor de betrokkene oplevert. De opsporingsautoriteiten zullen dan ook telkens moeten nagaan welke opsporingshandelingen en -functionaliteiten van de *policeware* precies noodzakelijk zijn om het omschreven doel in het schriftelijke bevel van de officier van justitie te bereiken. De ingezette functionaliteiten moeten expliciet in het bevel tot de inzet van de hackbevoegdheid worden genoemd.[286]

De in de toelichting genoemde diverse functionaliteiten van *policeware* zijn, samen met andere functionaliteiten en in een wat andere indeling, terechtgekomen in artikel 126nba lid 1 Sv: het vaststellen van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker (ook wel een 'virtuele inkijkoperatie' genoemd), een steunbevoegdheid voor het vastleggen van communicatie of stelselmatige observatie, het vastleggen van (huidige of toekomstige) gegevens op een computer, en het ontoegankelijk maken van gegevens. Het op één hoop gooien van deze vele functionaliteiten in één algemene hackbevoegdheid is wel bekritiseerd als een 'Zwitsers zakmes' dat te veel werktuigen wil combineren, "waardoor het onoverzichtelijk en daarmee moeilijker te hanteren" wordt.[287] Niettemin is dit het gereedschap waarmee de wetgever de praktijk heeft toegerust, dus die zal zich moeten richten op de vijf genoemde functionaliteiten. In deze paragraaf bespreken we kort de verschillende toepassingen van hacken als opsporingsbevoegdheid, de indeling in artikel 126nba lid 1 Sv volgend.[288]

a) Identificerende kenmerken ('virtuele inkijkoperatie')
De bedoeling bij de doelhandeling onder a in lid 1 is dat wordt binnengedrongen in de computer voor een beperkter doel dan het onderzoek van de hele computer, namelijk om bepaalde kenmerken van de computer vast te stellen van de computer of van de verdachte, bijvoorbeeld welk besturingssysteem, software of beveiliging die gebruikt. Met deze kennis in het achterhoofd kan de politie vervolgens andere bevoegdheden

285 Zie Morgan Marquis-Boire, 'From Bahrain With Love: FinFisher's Spy Kit Exposed?', *Citizen Lab*, 25 juli 2012 en Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire en John Scott-Railton, 'Mapping Hacking Team's "Untraceable" Spyware', *Citizen Lab*, 17 februari 2014.
286 *Kamerstukken II* 2015/16, 34372, 3, p. 32 en 102.
287 Koops, Conings & Verbruggen 2016, p. 61.
288 Vgl. voor een andere systematische indeling Koops, Conings & Verbruggen 2016, p. 54-58, die een onderscheid maken tussen a) eenmalig onderzoek van de harde schijf, b) periodiek onderzoek van computergebruik en c) inzet als steunbevoegdheid. De bespreking hier is wel gedeeltelijk gebaseerd op het preadvies van Koops, Conings & Verbruggen.

inzetten. Het gaat hier dus om een beperkte en voorbereidende bevoegdheid, vergelijkbaar met de inkijkoperatie van artikel 126k Sv.[289]
Voorbeelden van de vast te stellen kenmerken in wettekst en toelichting zijn de identiteit en de locatie van de gebruiker of de verdachte.[290] De FBI heeft in het verleden regelmatig van software gebruikgemaakt die gericht was op het vastleggen van het IP-adres en andere identificerende gegevens van computergebruikers.[291] In 2014 heeft de FBI naar verluidt in het kader van '*operation Torpedo*' kinderpornogebruikers via Tor geïdentificeerd.[292] Via een populaire website onder kinderpornogebruikers infecteerde de FBI kennelijk de computers van de bezoekers. De software registreerde vervolgens het IP-adres van de computer en andere identificerende gegevens over computergebruikers. De hackbevoegdheid lijkt een dergelijke toepassing ook mogelijk te maken, alhoewel opsporingsdiensten daarbij goed zullen moeten motiveren waarom de inzet proportioneel en subsidiair is.

b) en c) Steunbevoegdheid voor aftappen of observeren
Lid 1 onder b) en c) regelt de inzet van hacken als middel om de bevoegdheid tot vastleggen van communicatie, respectievelijk stelselmatig observeren, uit te voeren. Vastleggen van communicatie kan bestaan uit een tap (artikel 126m Sv), bijvoorbeeld door toetsaanslagen vast te leggen terwijl de gebruiker aan het e-mailen of WhatsAppen is, of uit direct afluisteren (artikel 126l Sv). Dit laatste zal vooral plaatsvinden door de microfoon heimelijk aan te zetten en mee te luisteren met gesprekken die met (of in de omgeving van) het apparaat worden gevoerd.
Koops e.a. achten het twijfelachtig of communicatie wel voldoende kan worden onderscheiden van non-communicatie. Zij stellen dat het bij gebruik van een keylogger tot op zekere hoogte mogelijk is om te onderscheiden tussen computergebruik 'voor zichzelf' en communicatie met anderen, omdat hiervoor vaak verschillende applicaties worden gebruikt; gezien de grote en steeds groeiende hoeveelheid applicaties in omloop zal het echter moeilijk zijn een lijst bij te houden van non-communicatie- en communicatie-applicaties.[293] Bij direct afluisteren zal het vastleggen in beginsel beperkt kunnen worden tot gesprekken, als de software herkent wanneer iemand belt of met een bepaalde app spraakcommunicatie uitvoert. Dit wordt mogelijk technisch

289 *Kamerstukken II* 2015/16, 34372, 3, 19. Koops, Conings & Verbruggen 2016, p. 43-44, stellen hierbij de vraag of de functionaliteit van lid 1 onder a wel feitelijk veel beperkter is dan het doorzoeken van de computer. De 'bepaalde' kenmerken lijken niet alleen technisch-identificerende kenmerken te zijn, maar mogelijk ook inhoudelijke kenmerken die kunnen leiden tot identiteits- of locatiebepaling. Ook is het volgens hen de vraag in welke mate de 'inkijkoperatie' voldoende duidelijk afgebakend kan worden van de zwaardere functionaliteit onder d (het doorzoeken van potentieel de hele computer).
290 *Kamerstukken II* 2015/16, 34372, 3, 20.
291 Zie Kevin Poulsen, 'FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats', *Wired*, 18 juli 2007 en Kevin Poulson, 'Documents: FBI Spyware Has Been Snaring Extortionists, Hackers for Years', *Wired*, 16 april 2009, http://archive.wired.com/politics/law/news/2007/07/fbi_spyware (laatst geraadpleegd op 1 juli 2018).
292 Zie Kevin Poulson, 'The FBI Used the Web's Favorite Hacking Tool to Unmask Tor Users', Wired, 16 december 2014 over operatie 'Torpedo', waarbij het IP-adres van Tor-gebruikers zeer waarschijnlijk met behulp van soortgelijke software op grotere schaal is ontmaskerd. Zie https://www.wired.com/2014/12/fbi-metasploit-tor (laatst geraadpleegd op 1 juli 2018).
293 Koops, Conings & Verbruggen 2016, p. 56-57.

moeilijker naarmate spraak-aansturing van computers en smartphones gemeengoed wordt; in dat geval kunnen al snel de communicatie met anderen en spraakcommando's aan het apparaat (die geen communicatie betreffen, want niet tussen twee of meer personen) door elkaar gaan lopen en gelijkelijk opgevangen worden. Dat lijkt ons niet de bedoeling van de steunbevoegdheid van lid 1 onder b. Sowieso zal slechts in hoge uitzonderingsgevallen voor deze functionaliteit de microfoon doorlopend of veelvuldig kunnen worden geactiveerd om gesprekken in de omgeving vast te leggen; het risico van non-communicatieve bijvangst, maar ook van bijvangst van gesprekken van onverdachte derden in de buurt van verdachtes apparaat, lijkt ons daarvoor snel te groot. Iets soortgelijks geldt voor de inzet ter stelselmatige observatie.[294] Het aanzetten van de camera in verdachtes apparaat is zeer geschikt om het gedrag van de verdachte waar te nemen, maar zal ook veel bijvangst opleveren van wat op de achtergrond te zien is. Bovendien mag stelselmatige observatie niet (mede) gericht zijn op het vastleggen van communicatie; de technische uitvoering zou dus moeten verzekeren dat de camera wordt gedeactiveerd zodra communicatie-apps worden geactiveerd waarmee de gebruiker zichtbaar in beeld communiceert, zoals bij Skype- of FaceTime-gesprekken (tenzij tegelijkertijd een andere bevoegdheid – zoals direct afluisteren – wordt ingezet). Weliswaar registreert de camera alleen beeld en geen geluid, maar het van dichtbij registreren van het pratende gezicht zal met gebruik van software voor geautomatiseerd liplezen (zo niet nu dan in de nabije toekomst) redelijk gemakkelijk het achterhalen van het gesprokene faciliteren.

Een andere beperking is dat observatie binnen de woning niet is toegestaan.[295] De webcam van een vaste computer in een woning mag dus niet worden aangezet, en wanneer de camera van een mobiel apparaat van afstand wordt of is aangezet, moet het opnemen stoppen zodra het mobiele apparaat een woning binnenkomt. Een en ander zal niet altijd duidelijk zijn, omdat de locatie van een apparaat vaak niet exact bepaalbaar is, evenmin als de locatie van mobiele woningen (zoals caravans). De waarborg van functiescheiding zal zich hier moeten bewijzen doordat de technisch rechercheurs beelden waarvan zij naar redelijk vermoeden (zouden moeten) vaststellen dat die binnen een woning zijn gemaakt, niet doorsturen naar de tactisch rechercheurs. (De beelden zouden wel technisch adequaat afgeschermd bewaard moeten blijven opdat ze op verzoek van de verdediging eventueel kunnen worden gecontroleerd.)

294 Koops, Conings & Verbruggen 2016, p. 41, werpen de vraag op of de inzet van de hackbevoegdheid als ondersteuning van stelselmatige observatie ook het monitoren van computergebruik kan omvatten. Zij suggereren dat dit mogelijk is, zolang geen communicatie wordt opgenomen, met als voorbeelden het monitoren van surfgedrag en het monitoren van het op de computer maken van geschriften. Volgens ons valt dergelijk monitoren echter niet onder stelselmatige observatie maar onder de functionaliteit onder d (vastlegging van gegevens die zijn of worden opgeslagen); zie *Kamerstukken II* 2015/16, 34372, 3, p. 20 ("Met speciale software kan het internetgebruik van de verdachte worden gevolgd").

295 *Kamerstukken II* 2015/16, 34372, 3, p. 26-27; *Kamerstukken II* 2016/17, 34372, 6, p. 50; *Kamerstukken I* 2016/17, 34372, D, p. 3. Zie ook paragraaf 3.6.1 over het verbod van stelselmatige observatie binnen de woning.

d) De online doorzoeking

De doorzoeking op afstand wordt geregeld in artikel 126nba lid 1 onder d Sv. Hierbij kunnen zowel de op het moment van binnendringen opgeslagen gegevens worden vastgelegd, als gegevens die daarna binnenkomen gedurende de periode waarbinnen de hackbevoegdheid wordt uitgeoefend.[296] Het eerste is een heimelijke variant van de doorzoeking ter vastlegging van gegevens; het tweede kent geen offline analogie en is daarmee een zeer vergaande bevoegdheid. Het is mogelijk om gedurende (telkens) vier weken iemands volledige computergebruik te monitoren, teneinde voor het onderzoek relevante gegevens vast te leggen. Dat gaat aanzienlijk verder dan het (telkens) vier weken lang buitenshuis observeren van iemands gedrag en het (eventueel ook binnenshuis) direct afluisteren van zijn communicatie. Niet voor niets is deze bevoegdheid dan ook beperkt tot achtjaarsmisdrijven of bij AMvB aangewezen misdrijven. De mogelijkheid om de bevoegdheid ook toe te laten voor bij AMvB aangewezen misdrijven is voorstelbaar, aangezien sommige computerdelicten moeilijk anderszins op te sporen zijn, maar de vraag is wel of de AMvB zich voldoende beperkt tot de echt ernstige computerdelicten waarvoor een zo ingrijpende bevoegdheid nodig zou kunnen zijn. De meeste genoemde misdrijven[297] zijn weliswaar in beginsel ernstig, maar omvatten ook delicten die onder omstandigheden tamelijk triviaal kunnen zijn (zoals een 22-jarige die een 17-jarige met een concertkaartje verleidt tot ontuchtige handelingen voor de webcam, artikel 248a Sr). Te hopen valt dat rechter-commissaris en de Centrale Toetsingscommissie (CTC) dan ook strikt zullen toezien op de proportionaliteit van hacken in de gevallen die in concreto minder ernstig zijn dan de maximumstraf of aanwijzing bij AMvB in abstracto suggereert, in het geval de bevoegdheid wordt ingezet om de volledige harde schijf te doorzoeken of wekenlang computergebruik te monitoren.

Een minder vergaande toepassing, die mogelijk ook vaker zal worden toegepast dan het complexe infecteren met software, is als een online doorzoeking wordt toegepast om het internetaccount van een verdachte (voor zover dit binnen de Nederlandse jurisdictie valt[298]) op bewijsmateriaal te doorzoeken. De vereiste inloggegevens kunnen

296 Lid 1 onder d bevat een enigszins bevreemdende temporele aanduiding: "gegevens die in het geautomatiseerde werk zijn opgeslagen, of die eerst na het tijdstip van afgifte van het bevel worden opgeslagen". Het lijkt hier om elkaar uitsluitende mogelijkheden te gaan. Normaliter zit er echter enige tijd tussen de afgifte van het bevel en het begin van uitvoering (het zal vaak even duren voordat malware kan (doen) worden geïnstalleerd). Dit roept vragen op onder welke categorie de gegevens vallen die na de afgifte van het bevel, maar vóór het begin van uitvoering, op de computer worden opgeslagen. Nu maakt het in dit geval voor de praktijk niet uit, omdat de formulering zowel historische als toekomstige gegevens omvat, maar de formulering roept wel wetssystematische vragen op over het temporele bereik van andere bevoegdheden. Zou bij een doorzoeking ter vastlegging van gegevens (die immers ook ziet op reeds opgeslagen gegevens) het niet toegestaan zijn om gegevens vast te leggen die *na* afgifte van het bevel maar *voor* de uitvoering ervan zijn opgeslagen?

297 Zie artikel 2 Besluit onderzoek in een geautomatiseerd werk, *Stb.* 2018, 340.

298 Merk op dat vanwege de Schutznorm het inloggen op buitenlandse servers veelal niet zal leiden tot bewijsuitsluiting; zie nader hoofdstuk 4. Relevant hier is verder dat de Schutznorm ook wordt toegepast op het eigendom van het account. Volgens Hof Den Haag 27 april 2011, ECLI:NL:GHSGR:2011:BR6836, maakte het door de politie rechtstreeks inloggen op een hotmailaccount (zonder de vordering aan Microsoft af te wachten) geen inbreuk op de rechten van de verdachte, omdat (naar verdachte zelf verklaarde) dit Hotmail-account niet bij hem zelf in gebruik was.

mogelijk worden verkregen door inbeslagname van een apparaat van de verdachte, via bekenden van de verdachte of 'social engineering', waarbij de verdachte met listige kunstgrepen wordt bewogen de informatie prijs te geven, bijvoorbeeld met een phishing-e-mail.
Alleen gegevens die redelijkerwijs nodig zijn om de waarheid aan de dag te brengen, kunnen worden vastgelegd. Het is dus niet mogelijk gegevens die geldswaarde vertegenwoordigen (zoals bitcoins) vast te leggen voor conservatoir beslag (tenzij ze ook nodig zijn voor waarheidsvinding).
Na het binnendringen worden de relevante gegevens vastgelegd. Op welke wijze dit technisch precies plaatsvindt, wordt in de toelichting op de Wet computercriminaliteit III niet duidelijk gemaakt. In de memorie van toelichting en het nader verslag wordt alleen aangegeven dat het hele proces wordt vastgelegd door middel van 'logging'. Een technisch rechercheur doet de uitvoering, terwijl een tactisch rechercheur de operatie heeft bedacht en aangeeft waar de politie naar op zoek is.[299]

e) Ontoegankelijkmaking van gegevens
Het 'op afstand ontoegankelijk maken van gegevens' wordt als een verstrekkende toepassing van de hackbevoegdheid gezien. De toepassing is namelijk eveneens beperkt tot misdrijven met een gevangenisstraf van acht jaar of meer en tot een beperkte lijst van bij AMvB aangewezen (computer)delicten. In de memorie van toelichting en het nader verslag wordt opgemerkt dat het hier in het bijzonder gaat om het op afstand ontoegankelijk maken van kinderporno en onklaar maken van botnets.[300] De hackbevoegdheid kan hierbij ook worden ingezet voor 'verstoringsdoeleinden'.[301]
In het verleden heeft de politie al eens een operatie uitgevoerd waarbij 220.000 kinderpornoafbeeldingen en video's op het *dark web* werden vervangen door een Nederlands politielogo.[302] In Europees verband zijn Nederlandse opsporingsinstanties in het EC3-centrum van Europol ook actief in het coördineren van internationale acties om botnets uit te schakelen.[303] Met de hackbevoegdheid bestaat er voortaan ook een expliciete grondslag in het Wetboek van Strafvordering voor dergelijke operaties.
Een punt van zorg betreft echter het gebrek aan controle *achteraf* bij toepassing van de bevoegdheid, vergelijkbaar met het hierboven genoemde zorgpunt bij het ontoegankelijkmakingsbevel (paragraaf 3.2.6).[304] Vooraf gelden strenge waarborgen, zoals de machtiging van een rechter-commissaris, het inwinnen van advies bij de Centrale Toetsingscommissie en de beperking tot ernstige misdrijven. De kans is echter tamelijk groot dat een rechtsmatigheidstoets van de inzet achteraf achterwege blijft, en dus niet

299 Zie *Kamerstukken II* 2015/16, 34372, 6, p. 40-41, 52 en 59.
300 Zie *Kamerstukken II* 2015/16, 34372, 3, p. 21-22.
301 *Kamerstukken II* 2015/16, 34372, 3, p. 59.
302 Zie Landelijk Parket, 'Kinderporno op anonieme, diep verborgen websites', 31 augustus 2011. Zie ook Wil Thijssen, 'De digitale onderwereld', *De Volkskrant* 10 maart 2012.
303 Zie bijvoorbeeld de volgende berichten, beschikbaar op www.europol.europa.eu: 'Notorious botnets infecting 2 million computers disrupted', 5 december 2013, 'Global action targeting Skylock malware', 10 juli 2014, en 'Botnet taken down through international law enforcement cooperation', 25 februari 2015.
304 Zie ook uitgebreid Oerlemans 2017c.

wordt gecontroleerd of de *uitoefening* (bijvoorbeeld de feitelijk ontoegankelijk gemaakte gegevens) ook daadwerkelijk proportioneel was. Voor veel cybercrime wordt namelijk niet vervolgd, omdat het (digitale) spoor in het buitenland doodloopt of de verdachte in een staat woont die geen eigen onderdanen uitlevert, waardoor de vervolging van de verdachte in een Nederlandse rechtbank niet mogelijk is.[305] Het is zeer de vraag of de rechtmatigheid van een dergelijke verstoringsactie tijdens een zitting door een Nederlandse rechter wordt getoetst. Wij achten de kans gering dat de betrokkenen (bijvoorbeeld degenen van wie onterecht informatie op een server ontoegankelijk is gemaakt bij een bulk-ontoegankelijkmakingsactie) gebruikmaken van de beschikbare klachtprocedure, mede omdat inhoudsaanbieders of beheerders van de ontoegankelijk gemaakte informatie veelal niet zullen worden genotificeerd bij gebrek aan bekende adresinformatie.

3.8 Vergaren van publiekelijk toegankelijke online gegevens

De term 'publiekelijk toegankelijke online gegevens' is afkomstig uit artikel 32 sub a van het Cybercrimeverdrag. Het betreft gegevens die voor eenieder via internet toegankelijk zijn. Het gaat daarbij ook om gegevens die na registratie beschikbaar zijn, zolang er maar geen restrictie geldt voor de groep personen die zich kan registreren, en om gegevens die pas na betaling beschikbaar zijn.[306] Daarbij kan worden gedacht aan het bekijken en vergaren van gegevens van online discussieforums en sociale-mediadiensten, ook als daarvoor registratie is vereist. Met de groeiende populariteit van sociale-mediadiensten komt steeds meer informatie over mensen beschikbaar. Opsporingsautoriteiten maken daar handig gebruik van.
De term 'publiekelijk toegankelijke gegevens' is volgens sommigen beter geschikt dan de term 'open bron',[307] maar anderen gebruiken deze termen veelal als synoniemen. Dat is ook het geval in de Wet op de inlichtingen- en veiligheidsdiensten 2017 (zie artikel 38 Wiv 2017), waaruit blijkt dat het hier om gegevens gaat die zonder meer kunnen worden geraadpleegd en waarvoor geen drempels bestaan.[308] In een online context gaat het daarbij in het bijzonder om gegevens die simpelweg via zoekmachines toegankelijk zijn. In het verleden heeft het invullen van een nickname in een zoekmachine in een cybercrimezaak al eens tot identificatie van de verdachte geleid.[309] Het verzamelen van gegevens uit open bronnen, inclusief gegevens op internet, is in de meeste opspo-

305 Zie ook Oerlemans 2017b.
306 Zie voor een gelijksoortige definitie Eijkman & Weggemans 2012, p. 287. Deze auteurs sluiten op hun beurt aan bij de definitie van National Open Source Enterprise, Intelligence Community Directive 301 (juli 2006). Zie voor een gelijksoortige definitie ook: artikel 25 lid 4 van het Besluit van de Raad van 6 april 2009 tot oprichting van de Europese politiedienst (Europol) (2009/271/JHA), L 121/51.
307 Zie ook Commissie-Koops 2018, p. 151-153.
308 *Kamerstukken II* 2016/17, 34588, 3, p. 38. Zie ook de juridische bijlage bij CTIVD-rapport nr. 55 (2018) en J.J. Oerlemans, *T&C Openbare Orde & Veiligheid*, artikel 38 Wiv 2017.
309 Gary Cutlack, 'Police Caught an Anonymous Hacker by Googling his IRC Name', *Gizmodo*, 12 december 2012, http://gizmodo.com/5968402/police-caught-an-anonymous-hacker-by-googling-his-irc-name (laatst geraadpleegd op 25 november 2016).

ringsonderzoeken standaard geworden.[310] Dat is ook niet verwonderlijk, gezien de hoeveelheid en diversiteit aan persoonlijke informatie die over delicten en verdachten of personen in de nabijheid van de verdachte te vinden is. Hoewel mensen er soms voor kiezen vrijwillig persoonlijke informatie met iedereen op internet te delen, betekent dat niet dat de informatie 'vogelvrij' is; de informatie wordt immers in een bepaalde context gedeeld, waarbij mensen niet (altijd) zullen beseffen dat ook personen buiten de context, waaronder de politie, de informatie kunnen zien en gebruiken. Belangrijk is ook dat veel informatie op internet niet door personen zelf maar door anderen is geplaatst.
Het verzamelen van persoonsgegevens uit publiek toegankelijke bronnen vormt daarom een inmenging in de privacy en behoeft dus een wettelijke basis. Maar welke wettelijke basis? De relevante wetsgeschiedenis wordt kort besproken in paragraaf 3.8.1, waaruit blijkt dat beperkte vormen van openbrononderzoek op grond van het algemene taakstellende artikel kunnen plaatsvinden. De relevante huidige en toekomstige bijzondere opsporingsbevoegdheden worden vervolgens in paragraaf 3.8.2 en 3.8.3 behandeld.

3.8.1 *Artikel 3 Politiewet 2012*

In de Wet BOB werd duidelijk gemaakt dat opsporingsambtenaren (1) "op internet kunnen rondkijken", (2) de gevonden informatie kunnen downloaden van verschillende bronnen op internet en (3) deze informatie kunnen opslaan in hun politiesysteem op basis van artikel 3 Politiewet 2012 (Polw).[311] De opsporingsactiviteit is in dat geval onderdeel van de taakstelling van de politie om bewijs te verzamelen in opsporingsonderzoeken.[312] De toepassing van de opsporingsmethode vergt dan geen bevel van een officier van justitie en de opsporingsmethode kan worden toegepast in opsporingsonderzoeken naar elk type strafbaar feit.
Artikel 3 Polw biedt slechts een voldoende juridische basis voor zover de opsporingsactiviteit een geringe inmenging in de rechten en vrijheden van de betrokken individuen met zich meebrengt en de integriteit van het opsporingsonderzoek niet in gevaar wordt gebracht. In 2011 maakte de Rechtbank Den Haag duidelijk dat opsporingsambtenaren tot op zekere hoogte gebruik mogen maken van Google Earth op grond van artikel 3 Polw voor hun bewijsgaringsdoeleinden.[313] In casu ging het om een persoon die verdacht werd van fraude. De rechercheurs konden met behulp van Google Earth vaststellen dat de betrokkene de designerstoelen van het type 'Bubble Club' had aangeschaft, omdat Google Earth het mogelijk maakt tot in tuinen van mensen in te zoomen. Het verweer van de advocaat dat deze opsporingsmethode een meer dan geringe pri-

310 Zie ook Harry Lensink & Gerard Janssen, 'Plaats delict: social media', Vrij Nederland, 18 april 2014, http://www.vn.nl/Archief/Justitie/Artikel-Justitie/Plaats-delict-social-media.htm (laatst geraadpleegd op 25 november 2016).
311 Zie *Kamerstukken II* 1998/99, 26671, 3, p. 35-36.
312 Zie *Kamerstukken II* 1998/99, 26671, 3, p. 35.
313 Rb. Den Haag 23 december 2011, ECLI:NL:RBSGR:2011:BU9409.

vacy-inmenging met zich meebrengt, slaagde niet; het ging immers slechts om een enkele foto.
De rechter benadrukte wel, in navolging van de wetsgeschiedenis, dat het niet de bedoeling is dat "stelselmatig gegevens van internet worden gedownload en in politiesystemen worden opgeslagen" op basis van de algemene taakstelling in artikel 3 Polw.[314] In dat geval vindt mogelijk een meer dan geringe inmenging in het recht op privacy plaats en moet een expliciete wettelijke opsporingsbevoegdheid worden toegepast. De wetgever gaf destijds al aan dat bijzondere opsporingsbevoegdheden ook "in de digitale wereld" kunnen worden ingezet.[315] Het is echter lang onduidelijk gebleven welke bijzondere opsporingsbevoegdheid bij een meer dan geringe privacy-inbreuk van toepassing is.

3.8.2 *Stelselmatige informatie-inwinning en stelselmatige observatie*

Stelselmatige informatie-inwinning
In de huidige catalogus bijzondere opsporingsbevoegdheden is er geen bevoegdheid die eenvoudig of naadloos kan worden toegepast op openbrononderzoek. Men zou in eerste instantie kunnen denken aan 'stelselmatige informatie-inwinning'.[316] Het kenmerk van deze undercover-bevoegdheid is echter dat daarbij de interactie met verdachte en betrokkenen uit diens omgeving plaatsvindt. Dat is hier niet het geval, tenzij de opsporingsambtenaar zich daadwerkelijk actief opstelt en bijvoorbeeld met de verdachte of personen uit diens omgeving gaat communiceren en daarbij een dekmantel gebruikt. Niettemin wordt deze bevoegdheid in de praktijk wel gebruikt voor openbrononderzoek, vermoedelijk bij gebrek aan een beter hierop toegesneden bevoegdheid. Dit kan worden verdedigd door een creatieve interpretatie te geven aan het begrip 'interactie': het zoeken naar en vastleggen van gegevens op internet kan men interpreteren als het inwinnen van informatie door interactie met servers in de omgeving van de verdachte, waarbij de servers dan als plaatsvervangend kunnen worden gezien voor personen in de omgeving van de verdachte. Vergelijkbaar met een praatje aanknopen met de barman in de stamkroeg van verdachte, kan de politie aldus een 'praatje' aanknopen met (de server van) een hostingaanbieder met wie de verdachte, of diens vrienden, informatie hebben 'gedeeld'. Deze interpretatie achten wij grammaticaal en misschien ook wel teleologisch verdedigbaar, maar in de wetsgeschiedenis valt hiervoor geen aanknopingspunt te vinden. Een belangrijk normatief argument tegen deze interpretatie van de bevoegdheid is dat het geheugen van mensen en computers fundamenteel verschilt: de barman en andere personen uit verdachtes omgeving kunnen vertellen wat hun bekend is over de verdachte, maar alleen wat zij bewust hebben onthouden, terwijl de servers alles 'onthouden' wat hen ooit is verteld (en niet actief is verwijderd). Bovendien is de reproductie van servers volledig, exact en betrouwbaar,

314 *Kamerstukken II* 1998/99, 26671, 3, p. 36.
315 Zie *Kamerstukken II* 1996/97, 25403, 3, 29 en p. 55 en *Kamerstukken II* 1998/99, 26671, 3, p. 36.
316 Aldus Stol, Leukfeldt & Klap 2012.

terwijl het menselijk geheugen onvolledig, feilbaar en daardoor minder betrouwbaar is. Interactie met hosting-servers kan daarom bezwaarlijk op één lijn worden gesteld met interactie met personen. Om die redenen achten wij deze bevoegdheid een weliswaar voorstelbare, maar gebrekkige, grondslag voor openbrononderzoek.

Stelselmatige observatie

De bijzondere opsporingsbevoegdheid van stelselmatige observatie wordt ook wel geassocieerd met openbrononderzoek.[317] Deze bijzondere opsporingsbevoegdheid is behandeld in paragraaf 3.6.1. Het kijken op internet en het overnemen van aangetroffen relevante online gegevens lijkt immers wel op het volgen van personen, het rondkijken in de fysieke openbare ruimte en het maken van foto's van aangetroffen relevante gedragingen.

Stelselmatige observatie onderscheidt zich echter van vastlegging van gegevens van internet in de zin dat het eerste ziet op het stelselmatig volgen van een persoon of stelselmatig waarnemen van diens aanwezigheid of gedrag gedurende een periode vanaf het moment van het bevel; het is dus 'realtime' en 'toekomstig' van aard. Het verzamelen van gegevens in open bronnen ziet daarentegen vooral ook op 'historische gegevens'.[318] Een ander verschil is dat observatie gericht is op waarneming van gedrag, terwijl internetonderzoek vaak vooral is gericht op waarneming van uitingen, en het is twijfelachtig of de inhoud van uitingen als 'gedrag' kan worden gekwalificeerd.[319]

Niettemin kunnen sommige vormen van openbrononderzoek wel als (stelselmatige) observatie worden gezien. Hierbij kan worden gedacht aan het stelselmatig (passief) volgen of waarnemen van gedrag van mensen op sociale media, eventueel na registratie op het medium.[320] Een persoon kan op internet bijvoorbeeld actief zijn op sociale media, discussieforums of chatkanalen. Het online gedrag van een persoon uit zich in die gevallen in het plaatsen van statusupdates of het delen van berichten op sociale media, het deelnemen aan of starten van discussies op forums, of het communiceren met anderen in chatkanalen. In elk geval geldt het *type* activiteit daarbij als een vorm van gedrag: de opsporingsambtenaar neemt waar *dat* en met wie een verdachte berichten deelt, discussies voert en chat. De inhoud van de communicatie valt onzes inziens niet direct onder gedrag. Men zou echter wellicht kunnen redeneren dat, nu direct afluisteren niet van toepassing is omdat de communicatie niet in beslotenheid plaatsvindt, het kennisnemen van de inhoud van op internet publiek uitgewisselde berichten niet als afluisteren maar als observatie kan worden gekwalificeerd. Bij stelselmatige

317 Zie ook Oerlemans & Koops 2012.

318 Zie ook Memorie van toelichting bij het Conceptwetsvoorstel Boek 2 (2017), p. 60 en J.J. Oerlemans, *T&C Openbare Orde & Veiligheid*, artikel 40 Wiv 2017, aant. 1. Zie voor een soortgelijke redenering het CTIVD rapport over sociale media (2014, p. 9 en p. 42) en CTIVD-rapport nr. 55 (2018, p. 10) in de context van 'open source intelligence' (OSINT). In de memorie van toelichting bij de Wiv 2017 wordt deze interpretatie eveneens aangehouden (*Kamerstukken II* 2016/17, 34588, 3, p. 62-63).

319 Zie Commissie-Koops 2018, p. 146.

320 Zie ook Rb. Den Haag, 10 december 2015, ECLI:NL:RBDHA:2015:14365, *Computerrecht* 2016/46, nr. 2, p. 113-124, m.nt. J.J. Oerlemans.

observatie kan per slot van rekening ook een foto worden gemaakt van een briefje dat de verdachte op het prikbord van de buurtsupermarkt ophangt.

Stelselmatigheid

Net als observatie in de fysieke wereld, moet de bijzondere opsporingsbevoegdheid van stelselmatige observatie worden ingezet wanneer het openbrononderzoek stelselmatig van aard wordt.[321] Stelselmatigheid betekent dat een min of meer volledig beeld van bepaalde aspecten van iemands privéleven wordt verkregen, waarbij de volgende factoren relevant zijn: duur, plaats, intensiteit, frequentie en het gebruik van een technisch hulpmiddel.[322]

Tot op zekere hoogte kunnen de factoren naar een online context worden vertaald.[323] De duur van de observatie van online waarnemingen spreekt vanzelf, voor zover het gaat om het waarnemen van gedrag vanaf het moment van het bevel. Voor historische gegevens is duur geen goed criterium, omdat binnen een paar seconden gegevens over vele afgelopen jaren kunnen worden vergaard. In dat licht valt te overwegen het openbrononderzoek te beperken tot gegevens die een afgelopen periode, bijvoorbeeld de laatste drie maanden, online zijn gezet; het valt echter te betwijfelen of zulks technisch voldoende haalbaar en tactisch voldoende verdedigbaar is. Met betrekking tot de frequentie kan gedacht worden aan het verschil tussen het vijf keer per dag waarnemen van de gedragingen of één keer per week. De intensiteit als factor laat zich moeilijker vertalen. Mogelijk kan worden gedacht aan het waarnemen van gedrag uit verschillende online bronnen, de hoeveelheid vergaarde informatie en de gevoelige context van een bron.[324] Zo kan het waarnemen van gedrag in een chatkanaal voor politieke gesprekken gevoeliger worden geacht dan gesprekken in een chatkanaal over het maken van opnames met drones.[325] Het is onduidelijk hoe het gebruik van een technisch hulpmiddel als factor voor online observatie kan worden vertaald. Het gebruik van computers en internet lijkt in ieder geval niet hieronder te vallen;[326] wel kan het gebruik van geavanceerde analyse- of visualisatiesoftware als een relevante factor worden gezien, omdat deze het observatievermogen van de opsporingsambtenaar substantieel vergroten.

De lijst met factoren kan nog verder met internetspecifieke factoren worden aangevuld en nader worden gegroepeerd tot vier clusters factoren: de omvang en het type van de gegevens, de aard van de bron, de wijze van zoeken en het gebruik van de gegevens en de mogelijke impact daarvan op de persoon.[327] Helaas maakt de bovenstaande opsomming van factoren nog steeds weinig concreet wanneer observatie in een online con-

321 Zie *Kamerstukken II* 1998/99, 26671, 3, p. 36 en *Kamerstukken II* 1996/97, 25403, 3, p. 26-27. Zie ook Oerlemans 2013.
322 Zie noot 224.
323 Zie uitgebreid Oerlemans & Koops 2012, Koops 2012a, p. 42 en Koops 2013, p. 663-664, alsook Commissie-Koops 2018, p. 162-165.
324 Zie ook Oerlemans & Koops 2012, p. 45.
325 Vergelijk *Kamerstukken II* 1997/98, 25403, 7, p. 47.
326 Zie ook Koops 2012a, p. 42 en Koops 2013, p. 663-664.
327 Commissie-Koops 2018, p. 163-164.

text nu precies de toepassing van de bijzondere opsporingsbevoegdheid van stelselmatige observatie vereist. Nadere uitwerking in praktijkrichtlijnen en in jurisprudentie is wenselijk.

Verbaliseringsplicht
Aangezien openbrononderzoek regelmatig een meer dan geringe privacy-inbreuk zal opleveren, maar niet altijd duidelijk is welke bijzondere opsporingsbevoegdheid het meest geschikt is om in te zetten, is in elk geval van belang dat de toepassing van de opsporingsbevoegdheid wordt geverbaliseerd en duidelijkheid wordt verschaft over de gebruikte juridische grondslag tijdens het proces. Het maken van een proces-verbaal, met daarbij vermelding van de juridische basis voor toepassing van de opsporingsmethoden die de officier van justitie heeft goedgekeurd, is belangrijk voor de beoordeling van de legitimiteit van het opsporingsmiddel. Oosterhoff signaleert dat in de praktijk vaak wordt volstaan met zinnen als: "Uit onderzoek op social media is gebleken dat …".[328] Dat is niet voldoende. Onzes inziens zouden op zijn minst de bezochte online bronnen moeten worden gemeld, een indicatie (met concrete voorbeelden van zoektermen) van de manier waarop is gezocht, alsmede de duur en frequentie van het onderzoek in de publiek toegankelijke bronnen. De verbaliseringsplicht (artikel 152 Sv) stelt de officier van justitie in de gelegenheid controle uit te oefenen over het opsporingsonderzoek en een verantwoorde vervolgingsbeslissing te nemen. Daarnaast stelt het ook de rechter en de verdediging op de terechtzitting in staat om de rechtmatigheid van het onderzoek te beoordelen.[329]

3.8.3 *Stelselmatige vastlegging van gegevens uit open bronnen*

Uit het voorgaande blijkt genoegzaam dat er rechtsonzekerheid bestaat op welke wettelijke basis openbrononderzoek kan plaatsvinden. Het conceptwetsvoorstel tot wijziging van Boek 2 schept gelukkig duidelijkheid door de nieuwe bijzondere opsporingsbevoegdheid van "stelselmatige vastlegging van informatie uit open bronnen" (artikel 2.8.2.4.1 Sv) voor te stellen. De regering is ook van mening dat de stelselmatige vastlegging van persoonsgegevens, ook al zijn de gegevens mogelijk vrijwillig beschikbaar gesteld, een meer dan geringe inmenging in de rechten en vrijheden van de betrokkene vormt en dat toepassing van een expliciete bevoegdheid noodzakelijk is.[330] Dit komt vooral ook door de grote toename van publiekelijk beschikbare gegevens van mensen, alsmede de diversiteit van deze gegevens en de snelheid waarmee deze gegevens beschikbaar komen. Daarbij worden ook gegevens die betrekking hebben op gedrag, ge-

328 Oosterhoff 2016.
329 In HR 19 december 1995, *NJ* 1996/249, geeft de Hoge Raad aan dat een redelijke uitleg van artikel 152 Sv met zich meebrengt dat het opsporingsambtenaren slechts vrij staat het opmaken van een proces-verbaal achterwege te laten als het niet van belang kan zijn voor een door de rechter in het eindonderzoek te nemen beslissing.
330 Conceptwetsvoorstel Boek 2 (2017), p. 59.

voelens, meningen en sociale contacten van mensen, al dan niet automatisch, vastgelegd.[331]
De voorgestelde bijzondere opsporingsbevoegdheid in artikel 2.8.2.4.1 Sv (concept) hoeft pas te worden ingezet als het verzamelen van de gegevens 'stelstelmatig' wordt. Voor de inzet van de bevoegdheid is een voorafgaand bevel van de officier van justitie vereist, waarbij de bevoegdheid voor ten hoogste drie maanden kan worden toegepast, met de mogelijkheid tot verlenging. Het vastleggen van gegevens wordt volgens de toelichting stelselmatig indien een "min of meer volledig beeld van bepaalde aspecten van het persoonlijke leven ontstaat".[332] In de toelichting worden echter weinig aanknopingspunten gegeven om te bepalen wanneer van stelselmatigheid sprake is. In plaats daarvan wordt opgemerkt dat bij twijfel de bijzondere opsporingsbevoegdheid moet worden toegepast. Het moet nog blijken waar in de praktijk de grens wordt getrokken.

Veel vragen blijven vooralsnog onbeantwoord. Moet de bijzondere bevoegdheid bijvoorbeeld worden toegepast voor stelselmatige vastlegging van gegevens van *hidden services* op het *dark web* of stelselmatige vastlegging van gegevens op online fora waarvoor registratie noodzakelijk is? Voor beantwoording van de vraag of deze bronnen als 'open bronnen' zijn te kwalificeren, heeft de Commissie-Koops voorgesteld aan te knopen bij de strafbaarstelling van computervredebreuk: publiek toegankelijke bronnen zijn die bronnen waarbij toegang (kan) worden verkregen zonder een beveiliging te doorbreken of op misleidende wijze (bijvoorbeeld door een technische ingreep, valse signalen of een valse identiteit) binnen te komen. Volgens dat criterium is het *deep web* een publiek toegankelijke bron (je hoeft alleen maar een URL in te tikken), evenals het *dark web* (waarvoor wel een technisch *hulpmiddel*, zoals een bepaalde browser, nodig is, maar geen technische *ingreep*).[333] Zo valt ook het registreren op een forum onder openbrononderzoek, maar niet het toegang verkrijgen tot sociale media door te proberen met een nep-account vrienden te worden met verdachte personen – dat valt onder het gebruik van een valse hoedanigheid.[334]
Een andere vraag is in hoeverre opsporingsinstanties gebruik mogen van maken van software, zoals *spiders*, *crawlers*, en *scrapers*, die automatisch gegevens binnenhalen ten behoeve van de publieke handhavings- en opsporingstaak.[335] De memorie van toelichting van het conceptwetsvoorstel voor Boek 2 hint erop dat in dit geval, waarbij gebruik wordt gemaakt van een 'technisch hulpmiddel' voor de vastlegging van gegevens, al snel een "min of meer volledig beeld van bepaalde aspecten van het persoonlijke leven

331 Zie p. 59 van de memorie van toelichting bij Conceptwetsvoorstel Boek 2 (2017). Zie hierover ook Oerlemans & Koops 2012.
332 Memorie van toelichting bij het Conceptwetsvoorstel Boek 2 (2017), p. 60.
333 Zie ook ter vergelijking CTIVD-rapport nr. 55 (2018), p. 10.
334 Commissie-Koops 2018, p. 154-155.
335 *Spiders* en *crawlers* gaan automatisch op zoek naar relevante informatie op basis van bepaalde parameters, waarbij de zoekresultaten nog door opsporingsambtenaren moeten worden overgenomen in politiesystemen. *Scrapers* downloaden de informatie ook rechtstreeks in politiesystemen. Zie voor een analyse van het gebruik van *intelligent agents* voor de opsporing in het algemeen Schermer 2003, en over *crawlers* specifiek Schermer 2003, p. 78. Zie ook Oerlemans & Koops 2012, Lodder & Schuilenberg 2016 en Gritter 2018.

van de betrokkene" wordt verkregen.[336] In dat geval moet de bijzondere opsporingsbevoegdheid worden toegepast. Het technisch hulpmiddel moet voldoen aan in een algemene maatregel van bestuur neergelegde eisen.[337] Uiteraard wordt ook voorzien in logging van gegevens met betrekking tot de handelingen die met het programma worden verricht.[338] Enkele auteurs pleiten ook voor aanvullende gedetailleerde wetgeving, mogelijk buiten het Wetboek van Strafvordering, voor het gebruik van deze geautomatiseerde gegevensverzamelsystemen voor open bronnen op internet.[339]
Het zal nog de nodige jaren duren voordat het gemoderniseerde wetboek in werking kan treden. Gelet op de huidige rechtsonzekerheid, is voorgesteld om niet te wachten op het nieuwe wetboek, maar de bevoegdheid tot vastleggen van gegevens uit publiek toegankelijke bronnen eerder te regelen.[340] Hopelijk komt er in dat licht snel een specifiek wetsvoorstel voor deze belangrijke opsporingsmethode.

3.9 Online undercover opsporingsmethoden

Bij de Wet BOB zijn drie bijzondere opsporingsbevoegdheden met betrekking tot undercover opsporingsmethoden in het Wetboek van Strafvordering 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 is opgemerkt dat opsporingsbevoegdheden, zoals observatie en infiltratie, onder gelijke voorwaarden in de digitale wereld kunnen worden toegepast.[341] Undercover opsporingsmethoden worden gekenmerkt door de *interactie* tussen individuen *onder dekmantel* met het doel bewijs te verzamelen in een opsporingsonderzoek.[342] De betrokken individuen die onderwerp zijn van het onderzoek, zijn niet op de hoogte van het doel van de interactie noch van de identiteit van de undercoveragenten.[343] In cybercrimezaken zijn de opsporingsmethoden

336 Zie p. 59-60 van de memorie van toelichting bij Conceptwetsvoorstel Boek 2 (2017).
337 Verwarring is mogelijk over wat in dit verband als 'technisch hulpmiddel' moet worden verstaan. Duidelijk zal zijn dat, indien de politie algemene zoekmachines als Google gebruikt, deze niet goedgekeurd kunnen worden op basis van het Besluit technische hulpmiddelen strafvordering. Zie hierover Commissie-Koops 2018, p. 165. Vgl. ook Rb. Amsterdam 19 april 2018, ECLI:NL:RBAMS:2018:2504 ('Tandem II'), r.o. 7.3, waarin de rechtbank oordeelt dat de door het NFI ontwikkelde en gebruikte zoekmachine Hansken (waarmee grote hoeveelheden gekopieerde gegevens kunnen worden doorzocht) wel een technisch hulpmiddel is, maar niet een technisch hulpmiddel in de zin van artikel 126ee Sv en dus niet onder het Besluit valt.
338 Memorie van toelichting bij Conceptwetsvoorstel Boek 2 (2017), p. 60.
339 Zie Lodder & Schuilenburg 2016, p. 152 en Oerlemans 2017a, p. 161-163. In deze wetgeving kunnen elementen worden opgenomen over (1) het doel van de vastlegging van de gegevens en de veronderstelde noodzaak, (2) voor welke delicten het middel kan worden ingezet, (3) welke gegevens kunnen worden opgeslagen, (4) wie toegang hebben tot het systeem en (5) welke bewaartermijn van de gegevens wordt aangehouden.
340 Commissie-Koops 2018, p. 151.
341 Zie *Kamerstukken II* 1998/99, 26671, 3, p. 36. Zie ook Siemerink 2000b.
342 Vgl. Fijnaut & Marx 1995 en Kruisbergen & De Jong 2010, p. 239.
343 Zie ook Joh 2009, p. 161.

bijzonder relevant, omdat een nickname, vaak een gebruikt pseudoniem in een chatkanaal of online discussieforum of handelsplatform, of ander *online handle*, zoals een e-mailadres, veelal de enige beschikbare digitale sporen zijn.[344] Opsporingsambtenaren en burgers onder instructie van de politie en OM kunnen – praktisch gezien – net zo anoniem en grensoverschrijdend[345] te werk gaan als de betrokken verdachten in een opsporingsonderzoek. Daarbij kan worden gedacht aan de online interactie onder dekmantel met verdachten door het versturen van privéberichten via e-mail, sociale media en online fora.

In deze paragraaf wordt de toepassing van de volgende opsporingsbevoegdheden in een online context besproken: de pseudokoop en pseudodienstverlening (paragraaf 3.9.1), stelselmatige informatie-inwinning (paragraaf 3.9.2) en infiltratie (paragraaf 3.9.3). De bijzondere opsporingsbevoegdheid van stelstelmatige observatie in een online context is uitgebreid besproken in paragrafen 3.6.1 en 3.8.2.

3.9.1 *Pseudokoop en pseudodienstverlening*

Het uitvoeren van een pseudokoop op internet kan het best worden omschreven als de situatie waarbij een undercoveragent zich voordoet als potentiële koper van een illegaal via internet aangeboden goed of dienst. Daarbij kan worden gedacht aan het kopen van drugs of wapens op een online drugsforum op het *dark web*.[346] Bij een pseudo-dienstverlening moet worden gedacht aan het verlenen van een dienst aan een verdachte, zoals het regelen van een loods voor de opslag van drugs of een auto voor het transport daarvan. Deze bevoegdheid is geregeld in artikel 126i Sv.
De pseudo*koop* is niet geschikt om gegevens te kopen of verkopen, omdat gegevens geen goed zijn en dus niet onder de koopbepaling vallen.[347] Daarom is bij de Wet computercriminaliteit II in artikel 126i lid 1 onder b Sv expliciet opgenomen dat naast pseudokoop en dienstverlening ook het bevel kan worden gegeven dat een opsporingsambtenaar "gegevens (...) door tussenkomst van een openbaar telecommunicatienetwerk afneemt van de verdachte". Merk op dat hij dus alleen via een openbaar netwerk (bijvoorbeeld internet) gegevens kan afnemen, niet via besloten netwerken. Deze vorm kan van belang zijn bijvoorbeeld voor de aankoop van malware, creditcardgegevens of andere via hacken verkregen persoonsgegevens die op internet worden aangeboden. Bepaalde goederen, zoals menselijke organen, zijn echter om ethische redenen problematisch om aan te schaffen via pseudokoop;[348] volgens deze redenering moet ook handel in kinderporno door opsporingsinstanties problematisch worden geacht.[349]

344 Zie uitgebreid Oerlemans 2017a, p. 30-36.
345 In hoofdstuk 4 wordt ingegaan de jurisdictievraagstukken die hierbij opkomen.
346 Zie bijvoorbeeld ook Arrondissementsparket Amsterdam, 'Pseudokoop wapen met bitcoins door politie en OM', 17 januari 2014, https://www.om.nl/vaste-onderdelen/zoeken/@32570/pseudokoop-wapen/ (laatst geraadpleegd op 6 december 2016).
347 *Kamerstukken II* 1998/99, 26671, 3, p. 36-37.
348 Aanwijzing opsporingsbevoegdheden, *Stcrt.* 2014, nr. 24442, paragraaf 2.8.
349 Nationaal Rapporteur Mensenhandel 2011, p. 164-165.

Voor de toepassing van de pseudokoop of pseudo-dienstverlening is een bevel van een officier van justitie vereist; het mag alleen worden toegepast in opsporingsonderzoeken met betrekking tot misdrijven zoals omschreven in artikel 67, eerste lid Sv (artikel 126i lid 1 Sv). De opsporingsbevoegdheid kan ook door een burger worden toegepast, indien uitvoering door een opsporingsambtenaar niet mogelijk is (artikel 126ij Sv).
Hoewel een algemeen verbod tot uitlokking al van toepassing is, wordt in artikel 126i lid 2 Sv (en artikel 126ij lid 3 Sv) nogmaals expliciet erop gewezen dat de opsporingsambtenaar (of burger) "een verdachte niet [mag] brengen tot andere strafbare feiten dan waarop diens opzet reeds tevoren was gericht". Dit criterium is afgeleid van het *Tallon*-arrest.[350] Als een opsporingsambtenaar een (op het eerste gezicht) illegaal goed op internet te koop zet, op een forum dat vaker gebruikt wordt voor illegale goederen, en vervolgens een persoon het goed koopt, dan zal van uitlokking bij aankoop geen sprake zijn. Maar als bijvoorbeeld een opsporingsambtenaar, op een forum waarin illegale spullen niet gemeengoed zijn, drugs aanbiedt en het nodige online contact heeft met iemand om hem te wijzen op het aantrekkelijke aanbod, dan kan wel sprake zijn van uitlokking; de koper wordt dan immers (mogelijk) op een idee gebracht dat hij nog niet had.[351] Het bevel voor toepassing van de opsporingsbevoegdheid moet al verkregen zijn voordat de daadwerkelijke aankoop begint, dus op het moment dat de interactie met de verdachte plaatsvindt om het goed of de gegevens aan te schaffen.[352] De handelingen in undercoveroperaties moeten zorgvuldig worden geverbaliseerd, zodat ter zitting kan worden nagegaan dat geen sprake is van uitlokking en het recht op een eerlijk proces in artikel 6 EVRM niet is geschonden.

De online pseudokoop wordt in de praktijk vaak toegepast.[353] Daarbij kan bijvoorbeeld worden gedacht aan de aankoop van drugs op online handelsplaatsen, de aankoop van illegaal vuurwerk bij webwinkels en de aankoop van gestolen goederen van marktplaats.nl, in het kader van opsporingsonderzoeken.[354] De online pseudokoop kan be-

350 Zie HR 4 december 1979, ECLI:NL:HR:1979:AB7429, *NJ* 1980/356, m.nt. Th.W. van Veen (*Tallon*-arrest) en EHRM november 2010, *Bannikova t. Rusland*, nr. 18757/06, *EHRC* 2011/9, m.nt. Ölçer. Zie ook *Kamerstukken II* 1996/97, 25403, 3, p. 31.

351 Dat van ongeoorloofde uitlokking al snel sprake kan zijn, blijkt uit een andere context: het OM heeft enkele tientallen zaken onderzocht afkomstig uit het Sweetie-project van Terre des Hommes, waarin een virtuele creatie werd gebruikt voor de (burger)opsporing van webcamsekstoeristen. "In geen van de zaken is vervolging ingesteld ter zake van grooming of verleiding van een minderjarige, omdat telkens sprake was van ongeoorloofde uitlokking", aldus *Kamerstukken I* 2016/17, 34372, D, p. 28.

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

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

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

wijs opleveren in een strafzaak, omdat de verdachte bijvoorbeeld contactgegevens bij de verkoop achterlaat. Het is ook mogelijk dat de vingerafdrukken op een afgeleverd pakket resultaat opleveren of dat de verdachte bewogen kan worden het pakket in persoon af te leveren, wat tot observatie of aanhouding van die persoon kan leiden.
Over de pseudodienstverlening in een online context is beduidend minder jurisprudentie aanwezig. In één zaak hebben rechercheurs een geprepareerd busje via speurders.nl aangeboden aan een verdachte. Na de aankoop konden de opsporingsambtenaren de verdachte via het busje volgen en de gesprekken in het busje aftappen met behulp van de toepassing van de bijzondere bevoegdheid van direct afluisteren. De raadsman beargumenteerde dat met betrekking tot de levering van een busje sprake was pseudo-dienstverlening. Het Hof Amsterdam ging hier echter niet in mee, omdat slechts sprake was van een beperkte inbreuk op de privacy van de verdachte, vanwege de beperkte duur (twee dagen) en intensiteit (een aantal telefonische contacten die dienden om tot een afspraak te komen).[355] De pseudo-verkoop kon in dit geval klaarblijkelijk op grond van artikel 3 Polw worden toegepast.

3.9.2 *Stelselmatige informatie-inwinning*

De bevoegdheid
Via internet kunnen opsporingsambtenaren onder dekmantel *interacteren* met een verdachte en personen in diens omgeving. Deze interacties kunnen bijvoorbeeld plaatsvinden door te chatten op een chatkanaal, berichten te plaatsen op een online discussie- of handelsforum en door 'vrienden' te worden met de verdachte of diens vrienden op sociale media om vervolgens met hen te communiceren. De actieve interventie in het leven van de verdachte door de opsporingsambtenaar is kenmerkend voor de toepassing van stelselmatige informatie-inwinning als bijzondere opsporingsbevoegdheid. Dit gaat verder dan louter het observeren van gedrag van personen of zaken.[356] Slechts met de juiste kennis van internetsubculturen, kunnen opsporingsambtenaren op een geloofwaardige manier op internet communiceren en relaties aangaan met mensen in het kader van een opsporingsonderzoek.[357]
De juridische basis voor het online interacteren onder dekmantel met verdachten of derden is artikel 3 Polw (voor zover het niet stelselmatig is) of artikel 126j Sv, de stelselmatige informatie-inwinning. De wetgever heeft bij de Wet BOB expliciet aangegeven dat deze bijzondere opsporingsbevoegdheid ook op internet mag worden toegepast.[358] De vraag is wanneer het inwinnen van informatie als *stelselmatig* is te kwalificeren. Daarvan is sprake als een "min of meer volledig beeld van bepaalde as-

355 Hof Amsterdam 31 mei 2013, ECLI:NL:GHAMS:2013:2090. Overigens werd niet aannemelijk gemaakt dat de verdachte door de politie is gebracht tot andere handelingen dan die waarop zijn opzet reeds was gericht. De omstandigheid dat de politie mogelijk de auto te koop heeft aangeboden voor een prijs die lager ligt dan de marktprijs, maakt dit niet anders, volgens het hof.
356 Zie *Kamerstukken II* 1996/97, 25403, 3, p. 35.
357 Zie ook onder andere Siemerink 2000a, p. 145.
358 Zie *Kamerstukken II* 1996/97, 25403, 3, p. 34. Zie ook *Kamerstukken II* 1998/99, 26671, 3, p. 37.

pecten van iemands privéleven" wordt verkregen. De factoren die dat bepalen (zie paragraaf 3.6.1) zijn echter geformuleerd in het kader van stelselmatige observatie[359] en niet expliciet voor stelselmatige informatie-inwinning. Toch nemen wij aan dat deze factoren ook van belang zijn voor stelselmatige informatie-inwinning. Jurisprudentie geeft ook geen duidelijk antwoord op de vraag wanneer sprake is van stelselmatigheid bij het informatie inwinnen onder dekmantel.
Voor het toepassen van deze BOB-bevoegdheid door een opsporingsambtenaar[360] is een bevel van een officier van justitie vereist. Artikel 126j Sv kan worden ingezet bij de opsporing van elk misdrijf en voor een (telkens verlengbare) periode van drie maanden. Op bevel van de officier van justitie kan ook een burger worden belast met het stelselmatig inwinnen van informatie (artikel 126v).

De toepassing van deze bijzondere opsporingsbevoegdheid 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' door de undercoveragent. Het is ook van belang dat de betrokken undercoveragent niet verder gaat dan is afgesproken met zijn leidinggevenden in de undercoveroperatie en dat dit voldoende wordt gecontroleerd. Hier wordt onder andere in EHRM-jurisprudentie met betrekking tot het recht op een eerlijk proces in artikel 6 EVRM op gewezen. Daarbij zij opgemerkt dat in Nederland geen machtiging van een rechter-commissaris is vereist, terwijl het EHRM deze wel voor het toezicht in undercoveroperaties prefereert.[361]

'Vrienden' worden op sociale media
Jurisprudentie over de BOB-bevoegdheid van stelselmatige informatie-inwinning in een online context is zeer schaars. Slechts één zaak geeft antwoord op de bovengenoemde vraag wanneer sprake is van stelselmatigheid bij online interacties met de verdachten in een opsporingsonderzoek. In de zogenoemde 'Context-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 de leden zich bezighielden met jihadistische activiteiten. Kort gezegd waren de rechters van mening dat al voor het aanmaken van een profiel de bevoegdheid tot stelselmatige informatie-inwinning moest worden inge-

359 Zie *Kamerstukken II* 1996/97, 25403, 3, p. 26-27 en *Kamerstukken II* 1998/99, 26671, 7, p. 46. Zie ook HR 12 februari 2002, *NJ* 2002/301, ECLI:NL:HR:2002:AD7804, paragraaf 3.4.

360 Volgens artikel 126j lid 4 onder b vallen hieronder ook opsporingsambtenaren als bedoeld in artikel 141, onderdelen c (KMar) en d (BOD'en) Sv, mits deze voldoen aan bepaalde opleidings- en samenwerkingseisen. Bij Wet van 6 december 2017, *Stb*. 2017, 489 (wetsvoorstel 34720) worden alle opsporingsambtenaren (artikel 141, onderdelen b, c en d Sv) in lid 1 genoemd, waarbij lid 4 wordt veralgemeniseerd tot AMvB-eisen aan de bekwaamheid van de opsporingsambtenaren; dit onderdeel is (stand juni 2018) nog niet in werking getreden.

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

zet. De opsporingsambtenaren hebben het bevel van de officier van justitie pas later verkregen en er was sprake van een gebrekkige verbalisering van de opsporingshandelingen. De vormverzuimen leidden echter niet tot een sanctie, omdat ze werden 'gerelativeerd' door de rechter.[362] Het standpunt van de rechtbank is begrijpelijk, in de zin dat bij het maken van een nepprofiel om vrienden te worden met de verdachte al een redelijke kans bestaat dat een "min of meer volledig beeld van bepaalde aspecten van zijn privéleven" wordt verkregen. Op Facebookprofielen zetten mensen immers in de regel veel privégegevens online, zoals foto's, interesses, activiteiten en relaties. Daarnaast is het gehele online sociale netwerk van de betrokkene met betrekking tot die dienst zichtbaar.
Zoals de 'Context-zaak' ook aangeeft, is de bijzondere opsporingsbevoegdheid van stelselmatige informatie-inwinning van toepassing op het aanmaken van een nepprofiel en het 'vrienden' worden met de verdachte op een sociale-mediaforum. Twijfel bestaat er onzes inziens wel over grensgevallen, waarbij bijvoorbeeld gechat wordt met de verdachte tijdens een groepschat op een bepaald chatkanaal of kortstondig een privéchat plaatsvindt waarbij bijvoorbeeld een e-mailadres of telefoonnummer wordt bemachtigd om verder te communiceren. De opsporingsambtenaar moet in ieder geval nagaan of de opsporingshandeling kan plaatsvinden op basis van artikel 3 Polw of dat de drempel van stelselmatigheid kan worden overschreden, in welk geval een bevel tot stelselmatige informatie-inwinning nodig is. Wellicht moet daarover met een officier van justitie overleg worden gepleegd. Het maken van een proces-verbaal van de opsporingshandelingen is ook noodzakelijk, zodat de opsporingshandelingen tijdens de zitting kunnen worden getoetst.

De 'lokpuber'
Ten slotte speelt nog de vraag in hoeverre een opsporingsambtenaar zich mag voordoen als minderjarige – ook wel 'lokpuber' genoemd – om bijvoorbeeld groomers op te sporen.[363] De wetgever benadert dit vooral als materieelrechtelijk vraagstuk; in de Wet computercriminaliteit III is artikel 248e Sr aangepast om ook het 'groomen' van (volwassen) lokpubers strafbaar te stellen (zie paragraaf 2.11.2). Ook burgers kunnen zich daarbij voordoen als 'lokpuber' om groomers te pakken.[364]
De vraag is echter op welke basis opsporingsambtenaren contact kunnen zoeken met (verdachte) groomers of andere verdachten van zedendelicten. Volgens de toelichting kan de lokpuber worden ingezet op basis van artikel 3 Polw: "Bij de huidige stand van de jurisprudentie zie ik geen aanleiding voor een nadere regeling over de inzet van de lokpuber. Die inzet vindt een toereikende grondslag in de algemene taakstellende be-

362 Zie Rb. Den Haag 10 december 2015, ECLI:NL:RBDHA:2015:14365, *Computerrecht* 2016/46, nr. 2, p. 113-124, m.nt. J.J. Oerlemans, r.o. 5.26-5.27, bevestigd in Hof Den Haag 25 mei 2018, ECLI:NL:GHDHA:2018:1248.
363 Zie ook Smeets 2013, p. 336 en Ölçer 2014, p. 18. Zie paragraaf 2.11.2 over grooming.
364 Zie uitgebreid Lindenberg 2016. Zie echter ook *Kamerstukken I* 2016/17, 34372, D, p. 27: burgeropsporing is mogelijk maar wordt afgeraden, omdat de opsporing van zedenmisdrijven maatwerk en specifieke deskundigheid vergt.

palingen van opsporingsambtenaren, zoals die in de rechtspraak is genormeerd".[365] Hierbij sluit de wetgever kennelijk aan bij de lokfiets, die volgens jurisprudentie kan worden neergezet op basis van artikel 3 Polw.[366]

Er bestaat echter wel een verschil tussen lokfietsen en lokpubers waar het gaat om de verwachte privacy-inbreuk. Bij een lokfiets ontstaat normaal gesproken weinig zicht op het privéleven van de verdachte of derden; bij de lokpuber ligt dat anders. Er wordt immers heen en weer gechat, gedurende vaak langere tijd – grooming is immers een langzaam proces waarbij geleidelijk het vertrouwen van de minderjarige wordt verworven[367] – en in die chats zal niet alleen over fietsen, bloemetjes of bijtjes worden gesproken, maar ook over de activiteiten en interesses van de verdachte. Bij lokpubers zal daarom al snel een min of meer volledig beeld van bepaalde aspecten van verdachtes privéleven ontstaan,[368] zodat inzet op basis van het algemene taakstellende artikel niet mogelijk is. Daarbij komt dat het online profiel van de lokpuber niet alleen groomers zal kunnen aantrekken, maar ook derden die gewoon willen chatten met de (vermeende) puber; de opsporingsambtenaar zal ook enige tijd met deze derden chatten voordat duidelijk kan worden dat het niet om groomers gaat en het contact dus verbroken kan worden. Er is gerede kans dat in deze aftastende periode ook een min of meer volledig beeld ontstaat van bepaalde aspecten van het privéleven van de onschuldige chatters. Daarom kan volgens ons de inzet van een lokpuber voor de opsporing van grooming niet worden gebaseerd op artikel 3 Polw. Het ligt in deze situatie voor de hand dat de bijzondere opsporingsbevoegdheid van stelselmatige informatie-inwinning wordt toegepast.

Bij de inzet van lokpubers voor de opsporing van webcamseks ligt dat mogelijk anders, als het contact beperkt blijft tot een eenmalig contact waarin vrijwel direct wordt vastgesteld of een contactzoeker wel of geen (webcam)seksuele intenties heeft; in dat geval zal de inzet wel op de algemene taakstellende artikelen kunnen worden gebaseerd. Zodra echter langer of vaker wordt gechat, zal onzes inziens al snel de drempel van stelselmatigheid kunnen worden bereikt.

---

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

366 Zie HR 28 oktober 2008, ECLI:NL:HR:2008:BE9817 (*lokfiets*); zie ook HR 23 januari 2018, ECLI:NL:HR:2018:62.

367 In die zin is er een belangrijk verschil in de opsporing van grooming (artikel 248e Sr) en de opsporing van webcamseks (artikel 248a Sr). Bij het laatste is er veel sneller en directer sprake van seksuele gerichtheid van het contact (vgl. *Kamerstukken I* 2016/17, 34372, D, p. 27: "In de praktijk leidt het uitlokkings-verbod ertoe dat een opsporingsambtenaar in beginsel zelf de communicatie niet start, maar afwacht totdat iemand *contact met hem legt voor seksuele doeleinden*" (cursivering toegevoegd)). Bij grooming is er juist geen sprake van het (als zodanig herkenbaar) leggen van contact 'voor seksuele doeleinden', maar probeert de groomer eerst het vertrouwen te winnen van de minderjarige alvorens geleidelijk over seksuele zaken te beginnen.

368 In rechtspraak wordt wel de lijn gehanteerd dat het privéleven niet aan de orde is wanneer iemand (mogelijk) strafbare feiten aan het plegen is, omdat er dan sprake is van een publieke zaak. Volgens ons miskent deze argumentatielijn dat ook misdadigers en verdachten recht op privacy hebben; het feit dat er, bij redelijke of zware verdenking van een strafbaar feit, goede redenen zijn om zicht te krijgen op het privéleven, wil niet zeggen dat het niet om privéleven gaat.

3.9.3 *Infiltratie*

Infiltratieoperaties onderscheiden zich door het kenmerk dat undercoveragenten (tot op zekere hoogte) strafbare feiten mogen plegen om hun dekmantel te behouden en het vertrouwen te winnen van leden van een criminele organisatie.[369] Met andere woorden, in een infiltratieoperatie *participeren* opsporingsambtenaren in een criminele organisatie teneinde bewijsmateriaal over strafbare feiten te verzamelen en toegang te krijgen tot de hogere regionen van een criminele organisatie.[370] Het is daarbij mogelijk dat (geautoriseerde) strafbare feiten worden gepleegd.
Voor de inzet van infiltratie als bijzondere opsporingsbevoegdheid door een opsporingsambtenaar (artikel 126h Sv)[371] of burger (artikel 126w) geldt geen drempel zoals 'stelselmatig infiltreren'. Zodra wordt deelgenomen aan een groep die zich bezighoudt met georganiseerde misdaad of diensten worden geleverd aan een dergelijke groep, is de bijzondere opsporingsbevoegdheid van toepassing. Een infiltratieoperatie mag alleen worden gestart nadat een bevel is verkregen van een officier van justitie in opsporingsonderzoeken naar misdrijven zoals omschreven in artikel 67, eerste lid Sv, met een ernstige inbreuk op de rechtsorde. Als intern controlemechanisme moet ook de Centrale Toetsingscommissie van het Openbaar Ministerie advies geven over de inzet van infiltratieoperaties. Deze zware voorwaarden zijn aangewezen, gelet op de indringendheid van deze opsporingsbevoegdheid en vooral het risico omtrent de integriteit van een opsporingsonderzoek.

Infiltratieoperaties kunnen ook in een online context worden ingezet, zoals op online fora of handelswebsites, als het vermoeden bestaat dat aldaar strafbare feiten in georganiseerd verband worden gepleegd. Tijdens een infiltratieoperatie op een drugsforum is het bijvoorbeeld mogelijk ook een pseudokoop te plegen, alhoewel daarvoor ook de desbetreffende bijzondere opsporingsbevoegdheid apart kan worden ingezet. Nederlandse opsporingsinstanties lijken echter niet kinderporno te willen gebruiken om te infiltreren in een criminele organisatie die zich bezighoudt met (de distributie of zelfs vervaardiging van) kinderporno. Het achterliggende idee is dat anders de 'markt' voor de handel in kinderporno in stand wordt gehouden en het slachtofferschap van de betrokken minderjarigen voortduurt. Deze toepassing van infiltratie wordt wel expliciet

369 Zie voor dit onderscheid ook Joh 2009, p. 166.
370 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".
371 Volgens artikel 126h lid 4 onder b vallen hieronder ook opsporingsambtenaren als bedoeld in artikel 141, onderdelen c (KMar) en d (BOD'en) Sv, mits deze voldoen aan bepaalde opleidings- en samenwerkingseisen. Bij Wet van 6 december 2017, *Stb.* 2017, 489 (wetsvoorstel 34720) worden alle opsporingsambtenaren (artikel 141, onderdelen b, c en d Sv) in lid 1 genoemd, waarbij lid 4 wordt veralgemeniseerd tot AMvB-eisen aan de bekwaamheid van de opsporingsambtenaren; dit onderdeel is (stand juni 2018) nog niet in werking getreden.

in de memorie van toelichting op de Wet BOB en de Wet computercriminaliteit genoemd.[372]

Jurisprudentie over de online toepassing van de opsporingsbevoegdheid tot infiltratie is schaars. In één gepubliceerde zaak bij de Rechtbank Middelburg is sprake van een infiltratieoperatie op een online drugsforum.[373] Het is de opsporingsambtenaren niet gelukt zelf moderator te worden op het forum, maar zij wisten wel het vertrouwen te winnen van een van de moderators op het forum. Door middel van een pseudokoop werden drugs aangekocht (de moderator verkocht zelf ook drugs) en voor de aflevering werd een afspraak in de fysieke wereld gemaakt. Na de aankoop van de drugs is de verdachte gevolgd tot zijn woonhuis door een observatieteam, waarvoor de bijzondere bevoegdheid van stelselmatige observatie werd ingezet. De verdediging protesteerde tegen het feit dat de operatie zowel in de fysieke wereld als 'virtueel' werd ingezet; de rechter keurde deze hybride toepassing van infiltratie echter goed.[374]

Daarnaast maakte de politie in mei 2017 bovendien bekend dat het Nederlandse Team High Tech Crime 27 dagen lang een online drugsmarktplaats, 'Hansa', in de lucht had gehouden, nadat het deze had overgenomen. Via een kopie van de server in Estland, verkregen door een rechtshulpverzoek, kon de website verder blijven draaien in Nederland. Met de volledige toegang konden de opsporingsambtenaren bovendien het communicatieverkeer van de kopers en verkopers ontsleutelen en actieve forumgebruikers in kaart brengen. Nadat de website offline was gehaald, werd aan enige digitale dealers duidelijk gemaakt dat ze in beeld waren bij het Team High Tech Crime en werden enkele arrestaties verricht.[375]

3.9.4 *Overzicht*

De onderstaande tabel verschaft een overzicht van de juridische basis van undercover opsporingsbevoegdheden en geeft voorbeelden van de online toepassing daarvan.

372 *Kamerstukken II* 1996/97, 25403, 3, p. 29 en *Kamerstukken II* 1998/99, 26671, 3, p. 36-37. In de memorie van toelichting van de Wet computercriminaliteit II wordt tevens expliciet opgemerkt dat de bijzondere opsporingsbevoegdheid van infiltratie "op internet" kan worden toegepast (*Kamerstukken II* 1998/99, 26671, 3, p. 37).

373 Rb. Midden-Nederland 9 oktober 2014, ECLI:NL:RBMNE:2014:4790 en ECLI:NL:RBMNE:2014:4792. De rechtbank beschrijft in omslachtige termen hoe de verdachten gebruikmaakten van een "beveiligd netwerk" waarmee "anoniem" drugs gekocht en verkocht werden op een online handelsplaats. Door de timing van de uitspraak is duidelijk dat het hierbij waarschijnlijk ging om de online marktplaatsen 'Black Market Reloaded' en 'Utopia' die alleen via Tor toegankelijk zijn. Zie ook *ANP*, 'OM wil tot zeven jaar cel voor internetdealers', 23 september 2014.

374 *Ibid*. Siemerink 2000a, p. 144, gaf in 2000 al aan dat deze hybride toepassing veel zal voorkomen. Net als in het normale leven beginnen infiltratie-interacties soms op internet en kunnen deze leiden tot ontmoetingen in de fysieke wereld.

375 Zie Europol, 'Massive blow to criminal Dark Web activities after globally coordinated operation', 20 juli 2017.

Opsporingsbevoegdheid	Juridische basis	Voorwaarden	Voorbeelden toepassing
Pseudokoop en dienstverlening	Art. 126i Sv	Bevel officier van justitie, misdrijven zoals omschreven in art. 67, eerste lid, Sv	De aankoop van drugs, wapens en andere illegale goederen op internet
Stelselmatig inwinnen van informatie	Art. 126j Sv	Bevel officier van justitie, elk misdrijf	Chatten, en online interacties op sociale media met verdachte of diens omgeving onder dekmantel
Infiltratie	Art. 126h Sv	Bevel officier van justitie, misdrijven zoals omschreven in art. 67, eerste lid, Sv die de rechtsorde ernstig schaden; toestemming Centrale Toetsingscommissie	Deelnemen aan een online forum, waarbinnen in georganiseerd verband drugs of wapens worden verhandeld

Tabel 3.4: Overzicht van de juridische basis voor undercover opsporingsbevoegdheden.

3.10 Digitaal bewijs

Na het overzicht van opsporingsbevoegdheden volgen hier nog enkele opmerkingen over bewijsaspecten. De rechter mag de bewezenverklaring alleen funderen op wettige bewijsmiddelen (artikel 338-339 Sv). Eén daarvan is de 'eigen waarneming' van de rechter, en langs die weg kunnen ook video-, geluids- en (andere) elektronische gegevens de rechter rechtstreeks bereiken. Het is volgens het wettelijk systeem niet vereist dat een deskundige of een getuige vertelt wat hij in een computer heeft aangetroffen. Rapporten van deskundigen kunnen in de vorm van schriftelijke bescheiden als bewijsmiddel gelden (artikel 339 jo. 344 lid 1 onder 4 Sv), waarbij zo nodig de deskundige ter zitting de bevindingen kan toelichten en door de verdediging kan worden ondervraagd. Het Nederlands Register Gerechtelijk Deskundigen[376] heeft inmiddels zes registers opengesteld binnen Digital Forensics.[377]
Er spelen verschillende problemen bij het bepalen van de bewijswaarde van in een computer opgeslagen gegevens. Daarbij lijken de grootste problemen betrekking te

376 Zie artikel 51k Sv, ingevoerd bij de Wet deskundige in strafzaken, *Stb.* 2009, 33.
377 Zie https://www.nrgd.nl/zoek-een-deskundige/zoeken-in-het-register.aspx (laatst geraadpleegd 1 juli 2018). Zie ook Henseler & van Loenhout 2016.

hebben op de vaststelling van de identiteit van degene die de computer bediende op het moment dat met die computer een strafbaar feit werd gepleegd,[378] alsook op de integriteit van aangetroffen en overgenomen gegevens. Wat dit betreft lijken de handvatten die in het civiel- en bestuursrechtelijk denken ter waarborging van de kwaliteit van bewijs zijn ontwikkeld,[379] iets minder goed rechtstreeks toepasbaar in het strafprocesrecht. In die rechtsgebieden gaat het namelijk om de invoer van gegevens waarbij veelal twee partijen belang hebben bij de juistheid (*business confidence* en betrouwbare gegevensverwerking binnen de overheid), terwijl in het strafrecht hoogstpersoonlijke aantekeningen (die niet geschreven zijn om ooit door een derde te worden gelezen, zoals agenda-aantekeningen) van doorslaggevend belang kunnen zijn.
Er bestaan al lange tijd technieken[380] om te garanderen dat bewijsmateriaal dat (bij een doorzoeking) in een computer wordt aangetroffen op verantwoorde wijze wordt veiliggesteld.[381] Meestal wordt een integrale, een-op-een kopie (image) van de gegevensdrager gemaakt op het moment van de doorzoeking in aanwezigheid van de officier van justitie of de rechter-commissaris, of aansluitend aan inbeslagneming. Door deze image op een niet-overschrijfbare gegevensdrager te plaatsen, of een hashwaarde van de kopie elektronisch te ondertekenen, kan de integriteit van de gegevens worden gewaarborgd. Dat garandeert weliswaar dat de opsporingsautoriteiten niet hebben geknoeid met het materiaal, maar het geeft nog geen zekerheid over de vraag wie de gegevens heeft ingevoerd – zelfs niet als een elektronisch stuk is 'ondertekend' door de eigenaar van de computer. Dat is wellicht anders met een (gekwalificeerde) elektronische handtekening (vergelijk artikel 3:15a BW), maar die zal – met uitzondering van sommige fraudezaken – slechts in een beperkt aantal zaken voorkomen: de boekhouder van een criminele organisatie sluit zijn aantekeningen niet af met zo'n elektronische handtekening.
Interessant is de ontwikkeling in jurisprudentie waarbij 'sensoren' die in de fysieke ruimte worden gebruikt, digitaal bewijs opleveren. Daarbij kan gedacht worden aan

378 Hiervoor kunnen bijvoorbeeld locatiegegevens van de verdachte (en van eventuele medegebruikers van een computer) relevant zijn, maar ook sporen die duiden op het gebruik van de computer door de verdachte, die bijvoorbeeld blijk geven van activiteiten kort voor of kort na het relevante moment (zoals cookies, cachegegevens en internetsessies waarbij is ingelogd met accountgegevens van de verdachte).

379 Zie bijvoorbeeld Franken 1997, p. 249-250.

380 Er bestaan wel de nodige technieken, maar niet of nauwelijks formele regelingen voor het veiligstellen van digitale sporen. Richtlijnen zijn beschikbaar in de vorm van (niet-openbare) Forensisch-Technische normen van het NFI (2009) en door het Lectoraat Cybersafety ontwikkelde handreikingen (*Alledaags politiewerk in een gedigitaliseerde wereld*; *Herkennen en veiligstellen van digitale apparatuur*; *Opsporing in een gedigitaliseerde samenleving*). Niet-naleving van de Forensisch-Technische norm 1300.01 betekent niet als zodanig dat het onderzoek onbetrouwbaar is; daarvoor moet de verdediging enigszins aannemelijk maken dat er fouten zijn gemaakt bij het veiligstellen van gegevens die de betrouwbaarheid aantasten, zie Rb. Limburg 7 juni 2013, ECLI:NL:RBLIM:2013:CA3726. Internationaal zijn meer richtlijnen en literatuur beschikbaar over forensisch digitaal onderzoek, zie bijvoorbeeld Casey 2011 en Mason & Seng 2017.

381 Het belang van adequate vastlegging van gegevens blijkt bijvoorbeeld uit Rb. Gelderland 8 mei 2013, ECLI:NL:RBGEL:2013:BZ9697. In deze zaak werd het OM niet-ontvankelijk verklaard mede omdat er fouten waren gemaakt bij het kopiëren van gegevensbestanden, waardoor de verdediging geen tegenonderzoek kon (laten) verrichten.

wifi-netwerken[382] waarmee mobiele telefoons verbinding maken en Bluetooth-verbindingen[383] met de apparaten waar een verdachte gebruik van maakt. Deze informatie kan een verdachte op een bepaald tijdstip op een bepaalde plaats positioneren, wat ondersteunend bewijs kan opleveren in strafzaken.
Wat betreft de juistheid, actualiteit en volledigheid van elektronische gegevens die door derden zijn uitgeleverd of overgedragen, valt niet veel meer te zeggen dan dat de rechter deze gegevens zelf op hun betrouwbaarheid zal moeten schatten, zoals hij ook van een getuige niet weet of deze de waarheid spreekt. Zoals rechtspsychologen soms een vraagteken plaatsen bij het vertrouwen van rechters in hun eigen kunnen in dezen, zo zullen computerexperts zich wellicht ook verbazen over het vertrouwen van de partijen in het strafproces in de betrouwbaarheid van digitaal bewijs.
Veelal wordt wel de rechtmatigheid van verkregen bewijs betwist, maar niet de betrouwbaarheid van digitaal bewijs als zodanig. En voor zover de betrouwbaarheid van digitaal bewijs wordt betwist door de verdediging, gebeurt dit vaak op basis van algemene argumenten, zonder specifiek te onderbouwen waarom die argumenten bij het onderhavige bewijs opgaan en dat bewijs dus in casu onbetrouwbaar maken. Dat geeft onvoldoende aanknopingspunten om het bewijs als onbetrouwbaar terzijde te stellen.[384]
Voor een betrouwbare rechtsgang zou het wellicht goed zijn als er meer rechtsontwikkeling plaatsvond over forensische vraagstukken rond digitaal bewijs. Zo'n rechtsontwikkeling zou gebaat zijn met advocaten die kritische vragen stellen over digitaal bewijs, onderbouwd met argumenten die specifiek toegesneden zijn op de bewijsgaring en mogelijke onvolkomenheden daarin in de concrete zaak.

3.11 Blik op de toekomst

3.11.1 *Modernisering Wetboek van Strafvordering*[385]

In dit hoofdstuk is her en der al verwezen naar de voorstellen voor het gemoderniseerde Wetboek van Strafvordering. De achtergrond van de moderniseringsoperatie is dat het huidige wetboek uit 1926 stamt, waarbij diverse delen uit het wetboek van 1838

382 Rb. Limburg 13 maart 2018, ECLI:NL:RBLIM:2018:2399, waarbij het een rol speelde in een brandstichtingzaak.
383 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 rol in strafzaken hebben gespeeld.
384 Zie bijvoorbeeld Rb. Amsterdam 19 april 2018, ECLI:NL:RBAMS:2018:2504 ('Tandem II'), r.o. 7.3 ("Door de verdediging zijn op dit punt veel (technische) vragen en kritiekpunten opgeworpen, maar zij heeft geen concreet onderbouwd standpunt met betrekking tot bepaalde zoekresultaten ingenomen of concrete onderzoeksresultaten betwist").
385 Zie https://www.rijksoverheid.nl/onderwerpen/modernisering-wetboek-van-strafvordering (algemeen) en https://www.rijksoverheid.nl/documenten/publicaties/2017/11/13/documenten-modernisering-wetboek-van-strafvordering (overzicht van documenten) (laatst geraadpleegd 1 juli 2018). Zie ook het Platform Modernisering Strafvordering, http://www.moderniseringstrafvordering.nl/ (laatst geraadpleegd 1 juli 2018) (literatuuroverzicht en artikelen).

waren overgenomen, en dat de samenleving inmiddels ingrijpend is veranderd "door nationale en internationale ontwikkelingen, door de opkomst van andere soorten criminaliteit en door nieuwe technische mogelijkheden".[386] Met de vele wijzigingen is het wetboek minder overzichtelijk en toegankelijk geworden, terwijl ontwikkelingen in jurisprudentie nog niet altijd in de wet worden gereflecteerd.[387] Het gaat overigens niet om een integrale herziening: belangrijke uitgangspunten en goed functionerende onderdelen blijven gehandhaafd. Het gaat vooral om het systematischer, overzichtelijker en geactualiseerd regelen van het strafproces.

Voor de regeling van opsporingsbevoegdheden zijn in 2014 de eerste discussiestukken gepubliceerd, onder andere over doorzoeking en beslag (waaronder onderzoek van gegevensdragers en in geautomatiseerde werken)[388] en over bijzondere opsporingsbevoegdheden.[389] Mede op basis hiervan bevat de Contourennota uit 2015 de nodige voorstellen, waarbij voor ICT-opsporing vooral de regeling rond voorwerpen en gegevens en de regeling van heimelijke bevoegdheden relevant zijn.[390] In februari 2017 werd vervolgens een conceptwetsvoorstel tot vaststelling van Boek 2 van het nieuwe Wetboek van Strafvordering in consultatie gegeven.[391] Belangrijke onderdelen van het conceptwetsvoorstel zijn een regeling van doorzoeking en beslag waarin digitaal onderzoek is geïntegreerd (met een regeling van 'beslag' op gegevens en een eis van een bevel van de officier van justitie voor elke inbeslagneming van gegevensdragers), gekoppeld aan een licht herziene regeling van de vordering van gegevens (hoofdstuk 7 van Boek 2) en een wijziging van de term 'bijzondere' in 'heimelijke' opsporingsbevoegdheden, met introductie van nieuwe bevoegdheden tot stelselmatig vastleggen van persoonsgegevens uit open bronnen en tot stelselmatige locatiebepaling (hoofdstuk 8 van Boek 2).

Omdat uit de eerste reacties hierop al duidelijk werd dat sommige onderdelen van het conceptwetsvoorstel, zoals de regeling rond 'beslag' op gegevens, op substantiële kritiek stuitten, is in juni 2017 de Commissie modernisering opsporingsonderzoek in het digitale tijdperk ('Commissie-Koops') ingesteld.[392] Daarbij werd ook de vraag betrokken of het *smartphone*-arrest[393] aanleiding gaf tot aanpassing van het wetsvoorstel. De commissie bracht in juni 2018 haar advies uit, met diverse voorstellen voor onder andere aanpassing van definities en van meerdere bepalingen. De aanbevelingen hebben onder andere betrekking op: 1) de regeling van 'beslag' op gegevens, 2) het invoeren

386 Kamerstukken II 2015/16, 29279, 278 (Contourennota), p. 2.
387 *Ibid.*
388 Discussiestuk 2014.
389 https://www.rijksoverheid.nl/onderwerpen/modernisering-wetboek-van-strafvordering/documenten/publicaties/2014/06/06/discussiestukken-1e-congres-modernisering-wetboek-van-strafvordering (laatst geraadpleegd 1 juli 2018).
390 Kamerstukken II 2015/16, 29279, 278 (Contourennota), p. 60-67.
391 Conceptwetsvoorstel Boek 2 (2017). De memorie van toelichting is beschikbaar op https://www.rijksoverheid.nl/onderwerpen/modernisering-wetboek-van-strafvordering/documenten/kamerstukken/2017/02/07/memorie-van-toelichting-vaststellingswet-boek-2-van-het-nieuwe-wetboek-van-strafvordering-het-opsporingsonderzoek (laatst geraadpleegd 1 juli 2018).
392 *Stcrt.* 12 juli 2017, nr. 39081, verlengd per *Stcrt*. 28 december 2017, nr. 73969.
393 HR 4 april 2017, ECLI:NL:HR:2017:592.

van een algemeen normeringscriterium van (ingrijpende) stelselmatigheid, 3) de introductie van schakelbepalingen voor analoge en met het lichaam verbonden gegevensdragers en 4) de bevoegdheden tot onderzoek van inkomende berichten na beslag en het vorderen van data-analyse door private partijen.[394]
Het wetsvoorstel voor Boek 2 zal (vermoedelijk substantieel) worden herzien op basis van de op de consultatie binnengekomen reacties en het advies van de Commissie-Koops, waarbij ook een effectonderzoek van de ketenpartijen nodig zal zijn. Op moment van schrijven (juli 2018) is de verwachting dat het nieuwe wetsvoorstel in de tweede helft van 2019 bij de Tweede Kamer zou kunnen worden ingediend. De inwerkingtreding, als onderdeel van het gehele gemoderniseerde wetboek, zal waarschijnlijk op zijn vroegst kunnen geschieden in 2024.
Voorlopig zal de praktijk het daarom met de huidige wet moeten doen, waarbij het wel mogelijk is dat enkele onderdelen uit het moderniseringstraject worden gelicht en mogelijk eerder via zelfstandige wetgevingstrajecten binnen het huidige Wetboek van Strafvordering worden geregeld. Ook kunnen ondertussen bepaalde normen via jurisprudentie verder worden ontwikkeld en ingevuld.

3.11.2 *Voorzienbare ontwikkelingen*

Dit hoofdstuk beoogt, als onderdeel van een handboek, vooral handvatten te geven voor het verkrijgen van een overzicht en begrip van de wettelijke regeling betreffende opsporing in een digitale omgeving naar huidig (en aanhangig komend) recht. Het is moeilijk te voorzien welke verdere aanpassingen in wet- of regelgeving in de toekomst nodig zullen zijn in het licht van de technische ontwikkelingen die zich de komende decennia zullen voordoen. De rechtspraktijk en wetgever zullen naar bevind van zaken moeten handelen bij nieuwe ontwikkelingen, door bestaande wetgeving te (her)interpreteren en gesignaleerde lacunes te dichten.
Binnen het bestek van dit hoofdstuk kunnen we slechts wijzen op enkele ontwikkelingen waarvan wij verwachten dat die significante invloed zullen hebben op het opsporingsonderzoek, mede in het licht van uitdagingen die ontstaan of uitvergroot worden door moeilijke toepasbaarheid van de wet.[395] Te denken valt bijvoorbeeld aan:

- grootschalige data-analyse door het koppelen van bestanden (Big Data Analytics) en geautomatiseerd analyseren van gegevens (*data analytics*, *machine learning*). Dit wordt niet of nauwelijks als zodanig geregeld in Sv (waarin vooral het *vergaren*, niet het gebruik, van gegevens wordt genormeerd) maar valt onder de Wet politiegegevens;[396] geautomatiseerde gegevensverwerking komt wel aan bod in de (herziene) Wpg (zie artikel 7a en 24b lid 2 onder e), maar zal de nodige vragen oproepen over de inzichtelijkheid van opsporingsprocessen en uitlegbaarheid van beslissingen;

394 Commissie-Koops 2018.
395 Voor een uitgebreider overzicht van ontwikkelingen die relevant zijn voor de opsporing, zie ook Commissie-Koops 2018, p. 11-21.
396 Wet van 21 juli 2007, *Stb.* 2007, 300; *Kamerstukken I* 2017/18, 34889, A (implementatie Richtlijn 2016/680/EU). Zie in dit kader ook Schermer 2017.

- verstoren door de politie (bijvoorbeeld het offline halen van botnets of het aanpakken van *bullet-proof* hostingaanbieders). Dit komt steeds meer voor (omdat klassieke opsporing en vervolging van daders bij cyberdelicten lang niet altijd haalbaar is), maar past als zodanig niet goed in het systeem van Sv, waarbij de normering deels gebaseerd blijft op toetsing tijdens het onderzoek ter zitting. Het roept vragen op in hoeverre strafvorderlijke bevoegdheden gebruikt mogen worden voor verstoringsdoeleinden;
- de opkomst van het Internet of Things, waarbij allerlei apparaten onder het begrip 'geautomatiseerd werk' zullen vallen en onderling zullen communiceren. Dit roept vragen op over de toepassing van bevoegdheden rond onderzoek in of aan geautomatiseerde werken en onderzoek van communicatie;
- de opkomst van robotica en autonome software, waarbij materieelrechtelijke vragen (aan wie valt een handeling verricht door een robot toe te rekenen) ook een opsporings-technische component zullen hebben. Ook ontstaan daarbij (in elk geval op langere termijn) interpretatievragen over hoe autonome systemen moeten worden gekwalificeerd (als voorwerp/geautomatiseerd werk, als getuige, als (rechts)persoon of als sui generis-entiteit). Valt het bevragen van een persoonlijke slimme assistent (zoals Alexa of Siri) bijvoorbeeld onder onderzoek aan een geautomatiseerd werk of onder getuigenverhoor?
- de opkomst van virtual reality en augmented reality. Hierbij doemen vragen op over reconstructie en reconstrueerbaarheid van misdrijven en loci delicti, waarvoor met terugwerkende kracht toegang tot gegevens over de exacte situatie ten tijde van een strafbaar feit nodig zal zijn om materieelrechtelijke vragen (zoals: was er sprake van opzet?) te beantwoorden, terwijl het de vraag is of opsporingsmethoden voorhanden zijn om een voldoende exacte reconstructie van een (deels) virtuele historische toestand te maken;
- de toenemende verwevenheid van digitale apparatuur met het menselijk lichaam, bijvoorbeeld via geïmplanteerde of met het zenuwstelsel verbonden chips. Dit roept vragen op of en wanneer het onderzoek in of aan computers overgaat in onderzoek in of aan het lichaam.