PROCUREUR-GENERAAL

ONDERZOEK IN EEN

BIJ DE HOGE RAAD

GEAUTOMATISEERD

DER NEDERLANDEN

WERK

EINDRAPPORTAGE

Over de toepassing van opsporings-bevoegdheden als bedoeld in de artikelen 126nba lid 1, 126uba lid 1 en 126zpa lid 1 van het Wetboek van Strafvordering door het Openbaar Ministerie

Een rapport van de procureur-generaal bij de Hoge Raad der Nederlanden in het kader van het toezicht als bedoeld in artikel 122 lid 1 van de Wet op de rechterlijke organisatie

ONDERZOEK IN EEN GEAUTOMATISEERD WERK

Over de toepassing van opsporingsbevoegdheden als bedoeld in de artikelen 126nba lid 1, 126uba lid 1 en 126zpa lid 1 van het Wetboek van Strafvordering door het Openbaar Ministerie

EINDRAPPORTAGE

Een rapport van de procureur-generaal bij de Hoge Raad der Nederlanden in het kader van het toezicht als bedoeld in artikel 122 lid 1 van de Wet op de rechterlijke organisatie

Onderzoekers
D.J.C. Aben, advocaat-generaal bij de Hoge Raad,
E.T. Luining, medewerker wetenschappelijk bureau van de Hoge Raad

Den Haag, september 2022

Woord vooraf

Dit rapport is de weergave van een onderzoek in het kader van de toezichthoudende taak die uit artikel 122 lid 1 van de Wet op de rechterlijke organisatie (Wet RO) voortvloeit. In die bepaling staat vermeld dat de procureur-generaal bij de Hoge Raad de minister in kennis kan stellen van het feit dat naar zijn oordeel het Openbaar Ministerie bij de uitoefening van zijn taak de wettelijke voorschriften niet naar behoren handhaaft of uitvoert. Aan de toezichthoudende taak wordt invulling gegeven door thematische onderzoeken.

Met de Wet computercriminaliteit III is beoogd het juridisch instrumentarium voor de opsporing en vervolging in het kader van cybercriminaliteit te versterken. De wet geeft opsporingsambtenaren onder meer de bevoegdheid tot het op afstand heimelijk binnendringen in geautomatiseerde werken. De toepassing en reikwijdte van deze bevoegdheden en de omvang van de gegevensverwerking vragen vanuit een rechtsstatelijk oogpunt om waarborgen die ervoor zorgen dat burgers kunnen blijven vertrouwen in de overheid. Toezicht is één van die waarborgen. Als het gaat om toezicht op de verwerking van persoonsgegevens door de politie en het Openbaar Ministerie heeft de Autoriteit persoonsgegevens een belangrijke taak. Verder zorgt de Inspectie Justitie en Veiligheid voor structureel systeemtoezicht dat ziet op het optreden van de politie bij de uitvoering van onderzoeken in een geautomatiseerd werk. De procureur-generaal bij de Hoge Raad biedt op basis van artikel 122 lid 1 Wet RO aanvullend toezicht in de vorm van thematische, probleemgerichte onderzoeken.

Dit onderzoek heeft zich gericht op de vraag of de wijze waarop het Openbaar Ministerie toepassing geeft aan de bevoegdheid tot onderzoek in een geautomatiseerd werk, voldoet aan de daarvoor geldende wettelijke voorschriften en de beginselen van proportionaliteit, subsidiariteit en behoorlijkheid en of het toezicht op de uitvoering daarvan toereikend is.

De onderzoekers hebben onder meer literatuur-, wetgevings- en jurisprudentieonderzoek verricht en interviews en gesprekken gevoerd met – onder meer – de functionarissen die in dit rapport worden aangemerkt als zaaksofficieren, rechercheofficieren, cyberofficieren, de landelijke cyberofficier, de digit-officieren en de parketsecretaris die de digit-officier van justitie bijstaat. Daarbij zijn negen zaken waarin in de periode 2019 tot en met 2021 is besloten tot uitvoering van onderzoek in een geautomatiseerd werk uitvoerig bestudeerd. De wijze waarop het Openbaar Ministerie ten aanzien van de onderzochte gevallen toepassing heeft gegeven aan de bevoegdheid tot het uitvoeren van onderzoek in een geautomatiseerd werk voldoet grosso modo aan de wettelijke voorschriften. In beginsel is in de onderzochte zaken voldaan aan de beginselen van proportionaliteit en subsidiariteit. Niettemin zijn er enkele onvolkomenheden en knelpunten geconstateerd. In het rapport worden in dat verband de nodige aanbevelingen gedaan.

Het onderzoek is uitgevoerd door mr. D.J.C. Aben, advocaat-generaal bij de Hoge Raad, die de leiding over het onderzoek had, en door mr. drs. E.T. Luining, medewerker van het wetenschappelijk bureau van de Hoge Raad. Ik ben hen zeer erkentelijk voor hun bereidheid dit onderzoek uit te voeren en voor hun grote inzet en toewijding bij de uitvoering van het onderzoek.

Mijn dank gaat verder uit naar de Inspectie Justitie en Veiligheid voor de goede samenwerking. Ook dank ik degenen binnen het Openbaar Ministerie die hun medewerking aan dit onderzoek hebben verleend door gegevens te verstrekken en hun kennis over de toepassing van de bevoegdheid tot onderzoek in een geautomatiseerd werk met de onderzoekers te delen.

Mr. F.W. Bleichrodt
Procureur-generaal bij de Hoge Raad der Nederlanden

Inhoudsopgave

1. Inleiding

Deze rapportage betreft een eindrapport met een verslag van bevindingen. Eerder is een (niet gepubliceerde) tussenrapportage verschenen. In dit hoofdstuk wordt een toelichting gegeven op het toezicht dat door de procureur-generaal bij de Hoge Raad (PG-HR) wordt uitgeoefend op de voet van artikel 122 van de Wet op de rechterlijke organisatie (RO) in het algemeen, en de keuze voor het onderzoeksthema in het bijzonder.
Na een inleiding in paragraaf 1.1, wordt in paragraaf 1.2 stilgestaan bij de aard van het toezicht dat de PG-HR uitoefent. Vervolgens wordt in paragraaf 1.3 het juridische kader van de bevoegdheid van de artikelen 126nba, 126uba en 126zpa Sv slechts globaal geschetst.
In hoofdstuk 2 komen de onderzoeksvragen aan de orde. In hoofdstuk 3 wordt ter beantwoording van de hieronder te formuleren eerste deelvraag meer uitvoerig stilgestaan bij het normatieve kader van de bevoegdheid tot binnendringen en het verrichten van onderzoekshandelingen in een geautomatiseerd werk. Hoofdstuk 3 vormt daarmee tevens de verantwoording van de bij het toezichtonderzoek getoetste items. De daaropvolgende twee hoofdstukken (4 en 5) bevatten een beschrijving van de onderzoeksresultaten aan de hand van bepaalde deelonderwerpen. Het rapport wordt afgesloten met een samenvatting, conclusies en aanbevelingen (hoofdstuk 6).

1.1. Ontwikkelingen in de taakuitoefening door het OM

Algemeen
In het kader van de uitoefening van toezicht op het Openbaar Ministerie (OM) op de voet van artikel 122 RO heeft de PG-HR besloten het onderwerp van de wetshandhaving op het terrein van computercriminaliteit en de toepassing van digitale opsporingsmethoden ter hand te nemen. Deze beslissing vloeit voort uit verscheidene ontwikkelingen die zich op dit terrein hebben voorgedaan. Die ontwikkelingen zijn onder meer de volgende.
Het zwaartepunt van de kerntaak van het OM, de strafrechtelijke handhaving van de rechtsorde, is al enige tijd niet meer alleen het – als poortwachter – aanbrengen van zaken voor de strafrechter. Er is reeds enkele decennia een trend gaande waarin het OM zijn kerntaak in toenemende mate beleidsmatig benadert, en dit vanwege de schaarste van de middelen die voor de rechtshandhaving beschikbaar zijn.[1] Voor een effectieve aanpak van criminaliteit acht het OM een gecombineerde en onderling samenhangende inzet van preventieve, bestuurlijke en strafrechtelijke interventies nodig.[2] Een programmatische of geïntegreerde aanpak van criminaliteit vormt tegenwoordig het uitgangspunt.
In het bestek van deze meer beleidsmatige aanpak van de strafrechtelijke handhaving van de rechtsorde is het OM bij de bestrijding van computercriminaliteit[3] intensief gaan samenwerken met andere publiekrechtelijke en privaatrechtelijke partijen. De samenwerkingsverbanden waarin het OM opereert breiden zich in een rap tempo uit. Samen met verschillende partners probeert het OM te kiezen voor interventies die een maximaal effect sorteren. Het strafrecht wordt hierbij ingezet als 'optimum remedium' en als instrument dat in verbinding staat

[1] N. Jörg, C. Kelk & A. Klip, *Strafrecht met mate,* Deventer: Wolters Kluwer 2019, hoofdstuk 7, IX.3.2 en IX.3.4.
[2] Openbaar Ministerie, *Twee weten meer dan één. Intensief samenwerken tegen de ondermijnende en georganiseerde criminaliteit*, Den Haag: Openbaar Ministerie 2012.
[3] Onder 'computercriminaliteit' wordt verstaan de criminaliteit die is gepleegd tegen en/of met behulp van informatie- en communicatietechnologie (ICT), dat wil zeggen: informatiesystemen, computers, netwerken van computers en telecommunicatievoorzieningen. De term 'computercriminaliteit' is hier inwisselbaar voor 'cybercrime'. Zie onder meer: S. Furnell, *Cybercrime. Vandalizing the information society*, Boston: Addison-Wesley 2002; B.J. Koops & R. Kaspersen, 'Computercriminaliteit in historisch perspectief', in: B.J. Koops & J.J. Oerlemans (red.), *Strafrecht & ICT*, Den Haag: Sdu 2019, 15-28, met name p. 17-18, en J. van Erp, W. Stol & J. van Wilsem, 'Criminaliteit en criminologie in een gedigitaliseerde wereld', *TvC* 2013, afl. 4, p. 327-341. In de geschiedenis van de Wet computercriminaliteit III, *Stb.* 2018, 322, maakt de minister van Justitie en Veiligheid doorgaans onderscheid tussen 'cybercriminaliteit in enge zin' en 'gedigitaliseerde criminaliteit'. Het eerste betreft misdrijven die worden gepleegd met een geautomatiseerd werk en die een geautomatiseerd werk als doelwit hebben. Het tweede betreft commune delicten die door de opkomst van ICT in toenemende mate een digitale component hebben gekregen. Zie onder meer *Kamerstukken II* 2017/18, 34 372, nr. 27 (verslag van een schriftelijk overleg), p. 5-6; *Kamerstukken I* 2018/19, 34 372, L (verslag van een schriftelijk overleg), p. 6-7.

met andere vormen van handhaving en toezicht. Bij deze andere vormen van handhaving en toezicht is de strafrechter niet de eerst aangewezene om controle uit te oefenen. Een substantieel deel van het werk van het OM onttrekt zich daardoor aan het gezichtsveld van de strafrechter.
Vanuit rechtsstatelijk oogpunt is het wenselijk en noodzakelijk dat de controle en het toezicht op de uitoefening van bevoegdheden door of onder verantwoordelijkheid van het OM worden versterkt, vooral voor zover de uitoefening van die bevoegdheden slechts in beperkte mate aan rechterlijk toezicht is onderworpen.

De aanpak van computercriminaliteit

De digitalisering van de samenleving doet zich gelden op het terrein van computercriminaliteit en dus ook op het gebied van de preventie en bestrijding ervan. Computercriminaliteit legt nu al een steeds groter beslag op de capaciteit van het OM. Het OM verwachtte in 2017 dat binnen een beperkt aantal jaren ongeveer 50% van de criminaliteit een digitale component heeft.[4] Het Centraal Bureau voor de Statistiek (CBS) schatte het aandeel van 'criminaliteit met een digitale component' onder delicten van de categorie 'bedrog' op maar liefst 96%.[5] Uit aangiftecijfers van de politie valt af te leiden dat gedurende de eerste vier maanden van 2021 bij de politie 78% meer meldingen van computercriminaliteit binnenkwamen dan in dezelfde periode in 2020, terwijl het aantal meldingen van computercriminaliteit ten opzichte van de eerste vier maanden van 2019 bijna verviervoudigd is.[6]
Een succesvolle aanpak van het uitdijende fenomeen van computercriminaliteit vereist in de eerste plaats samenwerking tussen publieke en private partijen en de wetenschap.[7] Zo zit het OM samen met de Nationale politie, de AIVD, de NCTV, het ministerie van Defensie en verscheidene private partijen die nationale belangen vertegenwoordigen in de *Cyber Security Raad* (CSR).[8] Bovendien neemt het OM deel in een publiek-private Nederlandse organisatie die sinds 1 januari 2012 de weerbaarheid van de Nederlandse samenleving in het digitale domein tracht te vergroten, het *Nationaal Cyber Security Centrum* (NCSC),[9] en

---

4 Zie 'Cybersecurity moet vanzelfsprekend zijn. Streef ketensamenwerking na' (interview met Gerrit van der Burg), *CSR Magazine* 2017, afl. 1 (maart), p. 58-60, met name p. 58.

5 'Cybercrime achterhalen in aangiften', *CBS.nl* 4 juni 2021. Het ging hier om onderzoek aan de hand van een experimentele methode van tekstanalyse uit een steekproef van processen-verbaal van aangifte uit het jaar 2016. Zie: https://www.cbs.nl/nl-nl/over-ons/innovatie/project/cybercrime-achterhalen-in-aangiften.

6 D. Janssen, 'Cybercrime blijft toenemen in 2021', *VPNgids.nl* 26 mei 2021. Zie: https://www.vpngids.nl/nieuws/cybercrime-blijft-toenemen-statistieken-mei-2021/.

7 Zie hierover meer uitgebreid: C.A.J. van den Eeden, J.J. van Berkel, C.C. Lankhaar & C.J. de Poot, *Opsporen, vervolgen en tegenhouden van cybercriminaliteit* (Cahier 2021), Den Haag: WODC 2021. Zie met name hoofdstuk 5.

8 "*De Cyber Security Raad (CSR) is een nationaal en onafhankelijk adviesorgaan van het kabinet en is samengesteld uit hooggeplaatste vertegenwoordigers van publieke en private organisaties en de wetenschap. De CSR zet zich op strategisch niveau in om de cybersecurity in Nederland te verhogen*", aldus leert informatie op de website van de CSR, www.cybersecurityraad.nl.

9 "*Het Nationaal Cyber Security Centrum (NCSC) is het centrale informatieknooppunt en expertisecentrum voor cybersecurity in Nederland. De missie van het NCSC is het bijdragen aan het vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein, en daarmee aan een veilige, open en stabiele informatiesamenleving. Het NCSC is internationaal het Nederlandse aanspreekpunt op het gebied van ICT-dreigingen en cybersecurity-incidenten. Ook is het NCSC een sleutelfiguur in de operationele coördinatie bij een grote ICT-crisis en de Computer Emergency Response Team (CERT) voor de Rijksoverheid. (…). Het NCSC valt onder verantwoordelijkheid van het ministerie van Justitie en Veiligheid*", aldus leert informatie op de website van het NCSC, www.ncsc.nl. De Wet beveiliging netwerk- en informatiesystemen (Wbni), die sinds 9 november 2018 van kracht is, regelt de wettelijke taken van het NCSC op het terrein van cybersecurity. Organisaties in vitale sectoren zijn verplicht om ernstige digitale veiligheidsincidenten te melden bij het NCSC. De website van het NCSC vormt een rijke bron aan informatie over cybercrime en de verschillende vormen van bestrijding ervan.

in het 'Bankenteam', de *Electronic Crimes Taskforce* (ECTF).[10] Er zijn landelijke meldpunten opgericht, zoals het *Landelijke Meldpunt Internetoplichting*, het *Meldpunt Kinderporno op Internet*[11] en het *Meldpunt Internet Discriminatie*. Deze meldpunten toetsen meldingen op strafbaarheid en sturen verwijderingsverzoeken aan beheerders of moderators van websites, ook wel bekend als *notice-and-take-down*-verzoeken (NTD). Met de inwerkingtreding van de Wet computercriminaliteit III, *Stb*. 2018, 322,[12] verleent artikel 125p van het Wetboek van Strafvordering (Sv) de officier van justitie de bevoegdheid een aanbieder van een communicatiedienst te bevelen om terstond alle maatregelen te nemen die redelijkerwijs van hem kunnen worden gevergd om bepaalde gegevens die worden opgeslagen of doorgegeven, ontoegankelijk te maken, voor zover dit noodzakelijk is ter beëindiging van een strafbaar feit of ter voorkoming van nieuwe strafbare feiten.[13]
In de tweede plaats vergt een effectieve bestrijding van computercriminaliteit de toepassing van alternatieve interventies, zoals preventieve of verstorende maatregelen richting cybercriminelen, digitale infrastructuur of facilitators.[14]
Tot slot leidt het toenemend gebruik van de telefoon- en internettap, de opslag van verkeersgegevens omtrent internet- en telefoongebruik, de registratie en opslag van kentekengegevens (ANPR), de toepassing van gezichts- en gedragsherkenningssoftware bij het cameratoezicht, en de overige toepassingen van digitale opsporingsmethoden tot de verwerking (registratie, opslag en afgifte) van een immense hoeveelheid (persoons) gegevens.
Op al deze terreinen is controle door de strafrechter onvolledig of zelfs nagenoeg afwezig.

De noodzaak van toezicht op de aanpak van computercriminaliteit

Het voorgaande brengt mee dat vanuit een rechtsstatelijk oogpunt noodzakelijk zijn: (1) garanties tegen misbruik, (2) toezicht op het gebruik van de hiervoor bedoelde opgeslagen gegevens, en (3) toezicht op de toepassing van uiteenlopende opsporingsmethoden.Tegen die achtergrond is de PG-HR in 2015 gevraagd aanvullend toezicht te houden op de rechtmatigheid van de toepassing van de wettelijke voorschriften ten aanzien van dataretentie. In de memorie van toelichting bij de Wet aanpassing bewaarplicht telecommunicatiegegevens is in overleg met de PG-HR opgenomen dat de PG-HR zich daartoe bereid heeft verklaard.[15] Daarnaast rijst vooral in die gevallen waarin achteraf niet tot vervolging wordt overgegaan en toetsing door de strafrechter ontbreekt de vraag of op correcte wijze toepassing is gegeven aan (digitale) opsporingsbevoegdheden. Een voorbeeld daarvan is de vraag of de plicht tot notificatie van

[10] De *Electronic Crimes Taskforce* (ECTF), ook wel het 'Bankenteam' genoemd, is een samenwerkingsverband tussen de landelijke eenheid van de Nationale politie, het landelijk parket van het OM, en de banken. Doel van de gezamenlijke aanpak is het voorkomen en aanpakken van digitale criminaliteit in het bancaire verkeer, zoals fraude met internetbankieren. De informatie in de voorgaande twee volzinnen is ontleend aan: Openbaar Ministerie, *Jaarbericht 2016,* Den Haag: Openbaar Ministerie 2017. Zie ook de website van het OM op het onderwerp cybercrime: https://www.om.nl/onderwerpen/cybercrime/.

[11] Website: https://www.meldpunt-kinderporno.nl/.

[12] Volledig: Wet van 27 juni 2018 tot wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III), *Stb.* 2018, 322, in werking getreden op 1 maart 2019.

[13] Zie ook art. 54a Sr, zowel oud als de vigerende bepaling.

[14] Zie 'Cybersecurity moet vanzelfsprekend zijn. Streef ketensamenwerking na' (interview met Gerrit van der Burg), *CSR Magazine* 2017, afl. 1 (maart), p. 58-60, met name p. 59.

[15] *Kamerstukken II* 2015/16, 34 537, nr. 3 (MvT), onder 9.3.

het binnendringen in een geautomatiseerd werk[16] afdoende wordt nageleefd. Bij de *notice-and-take-down*-procedures komen vragen op over de bevoegdheidsgrondslag en over de proportionaliteit en subsidiariteit.[17]
Bovendien kunnen ook op een heel ander gebied juridische vragen rijzen. Internet (cyberspace) houdt bijvoorbeeld geen rekening met landsgrenzen en maakt grensoverschrijdende opsporing en bewijsgaring eenvoudig mogelijk. De genoemde opsporingsactiviteiten kunnen echter leiden tot een inbreuk op de territoriale soevereiniteit van andere staten en kunnen de rechtszekerheid en de privacy van de betrokken individuen aantasten.[18]

De Wet computercriminaliteit III

Met de Wet computercriminaliteit III wordt beoogd het juridische instrumentarium voor de opsporing en vervolging van cybercriminelen te versterken. De wet sluit aan bij de snelle ontwikkelingen van de technologie en zet de lijn voort die is ingezet met de Wet computercriminaliteit (1993)[19] en de Wet computercriminaliteit II (2006).[20] De afdeling advisering van de Raad van State (verder: de Afdeling) constateerde in haar advies over het voorstel tot de Wet computercriminaliteit III, dat onder meer de bevoegdheid geeft tot het op afstand heimelijk binnendringen in geautomatiseerde werken: "*De toepassing en reikwijdte van deze bevoegdheden en met name de omvang van de gegevensverwerking kan daarbij van invloed zijn op het vertrouwen van burgers in de overheid. Dit vertrouwen is naar het oordeel van de Afdeling mede afhankelijk van het toezicht dat wordt gehouden*

---

16 In het Wetboek van Strafrecht (Sr), art. 80sexies Sr, worden alle vormen van zelfstandig werkzame hardware (computers) een 'geautomatiseerd werk' genoemd. 'Zelfstandig werkzaam' is een computer indien het apparaat in staat is tot opslag, verwerking én overdracht van gegevens. Dat zijn computers als servers, pc's, modems, routers, tablets en smartphones, kortweg alle elektronica waarin zich ten minste een processor bevindt, maar ook een groep van (eventueel draadloos) verbonden computers of telecommunicatievoorzieningen, oftewel een netwerk. Met de inwerkingtreding van de Wet computercriminaliteit III op 1 maart 2019, luidt art. 80sexies Sr: "*Onder geautomatiseerd werk wordt verstaan een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken.*" Elektronische gegevens c.q. computergegevens (met inbegrip van computersoftware) worden in art. 80quinquies Sr als volgt gedefinieerd: "*Onder gegevens wordt verstaan iedere weergave van feiten, begrippen of instructies, op een overeengekomen wijze, geschikt voor overdracht, interpretatie of verwerking door personen of geautomatiseerde werken.*"

17 Zie M.H.M. Schellekens, B.J. Koops & W.G. Teepe, *Wat niet weg is, is gezien. Een analyse van art. 54a Sr in het licht van een Notice-and-Take-Down-regime*, Tilburg: TILT/Cycris 2007, p. 42 e.v.

18 Op dit terrein is veel literatuur beschikbaar, zodat hier wordt volstaan met een selectie. Zie B.J. Koops & M. Goodwin, *Cyberspace, de cloud, en grensoverschrijdende opsporing: De grenzen en mogelijkheden van internationaal recht*, Tilburg: TILT 2014; B.J. Koops, C. Conings & F. Verbruggen, *Zoeken in computers naar Nederlands en Belgisch recht. Welke plaats hebben de 'digitale plaatsen' in de systematiek van opsporingsbevoegdheden?* (Preadvies voor de jaarvergadering van de NVVS 2016), Oisterwijk: Wolf Legal Publishers 2016, p. 137 e.v.; J.J. Oerlemans, *Investigating cybercrime* (diss. Leiden), z.p., z.u., 2017, p. 416-417; J.J. Oerlemans, 'Jurisdictie en grensoverschrijdende digitale opsporing', in: B.J. Koops & J.J. Oerlemans (red.), *Strafrecht & ICT*, Den Haag: Sdu 2019, p. 209-232. Zie voorts Y. Buruma, 'International Law and Cyberspace - Issues of Sovereignty and the Common Good', in: M. Busstra, W. Theeuwen e.a., *International Law for a Digitalised World* (Preadviezen voor de Koninklijke Nederlandse Vereniging voor Internationaal Recht), Den Haag: Asser Press 2020, m.n. p. 95 e.v. Toegesneden op territorialiteit van clouddiensten is: J.W. van den Hurk & S.J. de Vries, 'Waar worden gegevens in de 'cloud' opgeslagen en welke juridische consequentie heeft het antwoord op die vraag? Een speurtocht langs het traditionele juridisch kader en actuele wetgeving en jurisprudentie leidt tot een opmerkelijke conclusie', *Strafblad* 2019, afl. 4, p. 34-44. Zie de opiniebijdrage: M. Zoetekouw, 'Internationaalrechtelijke aspecten van het wetsvoorstel Computercriminaliteit III', *Tijdschrift voor Internetrecht* 2017, afl. 1, p. 30-33. De conclusie van Zoetekouw is dat het standpunt van de Nederlandse regering over grensoverschrijdende inzet van de bevoegdheden die met de Wet computercriminaliteit III in het leven zijn geroepen niet valt te verenigen met de huidige stand van zaken in het internationale recht, waar de norm is: soevereiniteit en non-interventie. Zie over deze twee beginselen van internationaal publiekrecht meer in het algemeen: M.N. Shaw, *International Law*, Cambridge: Cambridge University Press 2021, p. 555-559.

19 Volledig: Wet van 23 december 1992 tot wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de voortschrijdende toepassing van informatietechniek (Wet computercriminaliteit), *Stb.* 1993, 33, in werking getreden op 1 maart 1993.

20 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 2. De volledige naam van de Wet computercriminaliteit II luidt: Wet van 1 juni 2006 tot wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en enige andere wetten in verband met nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II), *Stb.* 2006, 300, in werking getreden op 1 september 2006.

op de toepassing van deze bevoegdheden."[21] In dit verband wijst de Afdeling erop dat ook het Europees Hof voor de Rechten van de Mens (EHRM) het belang heeft onderstreept van adequate en effectieve garanties tegen misbruik. Toezicht is wenselijk in de fase voorafgaand, tijdens en na de toepassing van bevoegdheden. De Afdeling merkt op dat in een substantieel deel van de gevallen niet tot vervolging wordt overgegaan en de toetsing achteraf beperkt blijft tot een mededeling (notificatie) dat in een geautomatiseerd werk is binnengedrongen. De plicht tot notificatie wordt echter reeds lange tijd slechts op beperkte schaal nageleefd.[22] Volgens de Afdeling kan niet worden heengegaan om de vraag naar de wenselijkheid van aanvullend toezicht op de toepassing van opsporingsbevoegdheden door politie en justitie in zaken die niet hebben geleid tot een procedure voor de strafrechter. "*Dit geldt temeer, daar de technologie zich verder zal blijven ontwikkelen en het van belang is dat het juridisch instrumentarium daarmee gelijke tred houdt. Juist om politie en justitie te kunnen blijven voorzien van adequate opsporings- en vervolgingsbevoegdheden, dienen – ook vanwege het vertrouwen van burgers in de overheid – de waarborgen navenant te zijn. Daarbij zij herhaald dat het in dezen niet alleen gegevens van en informatie over verdachten betreft maar ook van en over onschuldige burgers*", aldus de Afdeling.[23]

Met andere woorden, de ontwikkelingen op het gebied van computercriminaliteit en de toepassing van digitale opsporingsbevoegdheden zorgen voor verscheidene juridische probleemvelden waarmee het OM in zijn werk wordt geconfronteerd, terwijl het werk van het OM op deze gebieden zich in voorkomende gevallen aan het zicht van de rechter onttrekt. Vanwege de voortschrijdende technologische ontwikkelingen heeft het OM gaandeweg meer bevoegdheden toebedeeld gekregen die vaker leiden tot een inbreuk op de privacy van – onschuldig veronderstelde – burgers, zowel binnen onze landsgrenzen als daarbuiten. Om die redenen moet goed worden nagedacht over garanties tegen misbruik en is toezicht op het gebruik van die gegevens vanuit een rechtsstatelijk oogpunt noodzakelijk.[24] In dit verband is van belang om op te merken dat hoewel de opkomst van computercriminaliteit de aanleiding was voor de invoering van de Wet computercriminaliteit (1993) en voor de toekenning van bevoegdheden aan justitie en politie op het terrein van digitale opsporing en bewijsgaring, de uitoefening van die digitale bevoegdheden niet gelimiteerd hoeft te blijven tot de bestrijding van computercriminaliteit. Die bevoegdheden kunnen in beginsel ook worden ingezet bij de opsporing van andere delicten dan computercriminaliteit, bijvoorbeeld ingeval het vermoeden bestaat dat die andere delicten digitale sporen (elektronisch bewijsmateriaal) hebben achtergelaten. De toepassing van digitale opsporingsmethoden valt dus niet per definitie samen met rechtshandhaving op het terrein van computercriminaliteit.

---

21 *Kamerstukken II* 2015/16, 34 372, nr. 4 (Advies RvS), p. 6-7.

22 Zie o.m. het door de Afdeling vermelde rapport van T. Spapens, M. Siesling & E. de Feijter, *Brandstof voor de opsporing. Evaluatie Wet bevoegdheden vorderen gegevens*, Den Haag: BJu 2011, p. 99.

23 *Kamerstukken II* 2015/16, 34 372, nr. 4, p. 9.

24 Zie in dit kader ook de vragen en opmerkingen van leden van de vaste commissie voor Veiligheid en Justitie, *Kamerstukken I* 2016/17, 34 372, B (VV I), p. 9-10.

1.2. Toezicht

Volgens de Afdeling is structureel systeemtoezicht[25] nodig op de rechtmatige uitoefening van opsporingsbevoegdheden waarbij gebruik wordt gemaakt van ICT in zaken die niet aan de strafrechter zijn voorgelegd. De PG-HR onderschrijft dit oordeel. In dat verband kan allereerst worden gewezen op de toezichthoudende taken van de Inspectie Justitie en Veiligheid en de Autoriteit persoonsgegevens op dit gebied. Het systeemtoezicht door de Inspectie Justitie en Veiligheid ziet echter alleen op het optreden van de politie en strekt zich niet uit tot vraagstukken die de rechtmatigheid van het optreden van de justitiële autoriteiten betreffen.[26] De toezichthoudende taak van de Autoriteit persoonsgegevens is beperkt tot de verwerking van persoonsgegevens.[27]

Structureel systeemtoezicht op de rechtmatige uitoefening van taken van het OM op het terrein van opsporingsbevoegdheden zal de PG-HR niet kunnen bieden. De PG-HR is wel in staat (en bereid) tot het bieden van aanvullend toezicht in de vorm van thematische, probleemgerichte onderzoeken. Thema's die zich op het gebied van de bestrijding van computercriminaliteit en toepassing van digitale opsporingsmethoden lenen voor toezichthoudend onderzoek betreffen onder andere:

- de wijze waarop het OM uitvoering geeft aan *notice-and-take-down* (NTD) procedures;
- de naleving door het OM van de in de artikelen 126bb, 126cc en 126dd Sv neergelegde

---

[25] "*Systeemtoezicht of systeemgericht toezicht is het toezicht door de overheid dat gebruikmaakt van zelfregulerende systemen binnen organisaties of branches. Systeemtoezicht is een benadering van de onder toezicht staande waarbij in het toezicht gebruik wordt gemaakt van de eigen activiteiten van deze onder toezicht staande die gericht zijn op het systematisch vergroten van de eigen kwaliteit en regelnaleving. Het betreft al het toezicht waarbij de opzet, reikwijdte en werking van (kwaliteits)systemen en (bedrijfs)processen bij organisaties worden vastgesteld. Dit wordt gedaan door audit achtige onderzoeken met reality checks uit te voeren, waarbij gebruik wordt gemaakt van de interne borgingssystemen binnen organisaties of sectoren.*" Zie het lemma 'systeemtoezicht' (onderdeel Rijksoverheid, begrippenkader rijksinspecties) in de Eerste Nederlandse Systematisch Ingerichte Encyclopaedie (E.N.S.I.E.), elektronische versie (bijgewerkt tot 2022). Zie bovendien: J. Helderman & M.E. Honingh, *Systeemtoezicht. Een onderzoek naar de condities en werking van systeemtoezicht in zes sectoren*, Den Haag: WODC 2009.

[26] *Handelingen I* 2017/18, nr. 34, item 5, p. 19. Zie wat betreft de taak van de Inspectie Justitie en Veiligheid ook de nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb.* 2018, 340, p. 23-24. Zie bovendien: *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 81-83, en *Kamerstukken I* 2017/18, 34 372, G (NMvA I), p. 2 en 14. Over de aard en reikwijdte van het toezicht van de Inspectie Justitie en Veiligheid (hierna: Inspectie JenV) merkt de Inspectie in haar *Verslag toezicht wettelijke hackbevoegdheid politie 2019*, Den Haag: Ministerie van Justitie en Veiligheid 2020, p. 4-5, het volgende op: "*De Inspectie JenV houdt toezicht op het functioneren van het wettelijk systeem rond het toepassen van de hackbevoegdheid door de politie. Toepassing van deze bevoegdheid vindt plaats binnen de grenzen van het bevel van de officier van justitie en de machtiging van de rechter-commissaris. De oordeelsvorming door de officier van justitie en de rechter-commissaris valt buiten de reikwijdte van het toezicht door de Inspectie JenV. Het toezicht van de Inspectie JenV is niet beperkt tot toezicht achteraf. De Inspectie JenV kan zich te allen tijde vergewissen van een juiste uitvoering van het bevel van de officier van justitie. De Inspectie JenV kan, in het kader van het systeemtoezicht, toezicht houden tijdens de uitvoering van het bevel. Het toezicht heeft ook betrekking op de inzet van de bevoegdheid in gevallen die niet leiden tot een strafvervolging. De Inspectie JenV houdt tevens toezicht op de naleving van de regels en procedures voor de keuring en inzet van software waarmee op apparaten gegevens worden verzameld en de vastlegging van gegevens op een beveiligde technische infrastructuur. Indien de Inspectie tijdens de uitoefening van het toezicht in aanraking komt met mogelijke schendingen van de wettelijke voorschriften door of in opdracht van een officier van justitie of in aanraking komt met mogelijke schendingen van de regels rond de bescherming van persoonsgegevens kan de Inspectie JenV de procureur-generaal bij de Hoge Raad (PG-HR) respectievelijk de Autoriteit Persoonsgegevens (AP) informeren.*"

[27] Voor de goede orde, de toezichthoudende bevoegdheid van de Autoriteit persoonsgegevens strekt zich *niet* uit tot de verwerking van persoonsgegevens door gerechten (als bedoeld in art. 2 RO) "*bij de uitoefening van rechterlijke taken*". Zie art. 55 lid 3 van de Algemene verordening gegevensbescherming (AVG): "*Toezichthoudende autoriteiten zijn niet competent toe te zien op verwerkingen door gerechten bij de uitoefening van hun rechterlijke taken.*" Zie ook art. 51h lid 7 Wet justitiële en strafvorderlijke gegevens (Wjsg): "*In afwijking van het eerste lid, is de Autoriteit persoonsgegevens niet belast met het toezicht op de verwerking van gerechtelijke strafgegevens door de gerechten, bedoeld in artikel 2 van de Wet op de rechterlijke organisatie, in het kader van de uitoefening van hun rechterlijke taken.*" Wat in dit verband onder 'rechterlijke taken' dient te verstaan is nog niet volledig uitgekristalliseerd. Voor de gegevenswerking die niet onder 'rechterlijke taken' valt, is de Autoriteit persoonsgegevens wél de toezichthoudende instantie en zijn – in het politiële en justitiële domein – de Wet politiegegevens (Wpg) en de Wjsg van toepassing.

verplichtingen met betrekking tot de notificatie, de bewaring, de vernietiging en het gebruik van gegevens door het OM;
- de wijze waarop het OM toepassing geeft aan de artikelen 126nba lid 1, 126uba lid 1 en 126zpa lid 1 Sv (binnendringen en het verrichten van onderzoekshandelingen in een geautomatiseerd werk).

Het is binnen het bestek van het OM-toezicht geen voornemen van de PG-HR deze onderzoeksthema's tegelijkertijd ter hand te nemen, maar mogelijk wel successievelijk en voortbouwend op eerdere ervaringen. Als eerste stap is besloten het toezicht te richten op de vraag of en zo ja in hoeverre het OM bij het uitoefenen van de bevoegdheid tot binnendringen en het verrichten van onderzoekshandelingen in een geautomatiseerd werk de wettelijke voorschriften naar behoren in acht neemt, met inbegrip van de wijze waarop de zodoende door (of onder verantwoordelijkheid van) het OM verkregen gegevens worden vastgelegd, verwerkt en/of gebruikt.

1.3. Het onderwerp van toezicht

Onderzoek in een geautomatiseerd werk

De bevoegdheid tot het uitvoeren van onderzoek in een geautomatiseerd werk, ook wel de 'hackbevoegdheid' genoemd, is geregeld in de artikelen 126nba lid 1, 126uba lid 1 en 126zpa lid 1 Sv. Aan de officier van justitie is in die bepalingen de bevoegdheid toegekend om – onder strikte voorwaarden – te bevelen dat een opsporingsambtenaar:

1. een geautomatiseerd werk dat in gebruik is bij een verdachte, respectievelijk een persoon (op afstand heimelijk) *binnendringt*, en
2. hierin, al dan niet met een technisch hulpmiddel, *onderzoekshandelingen verricht* met het oog op bepaald omschreven onderzoeksdoelen.

De bevoegdheid tot binnendringen en het verrichten van onderzoekshandelingen in een geautomatiseerd werk is ingevoerd omdat volgens de minister van Justitie en Veiligheid[28] de bestaande opsporingsbevoegdheden in toenemende mate tekortschieten om wezenlijke problemen en gebleken knelpunten op het gebied van de bestrijding van computercriminaliteit te adresseren. Het gaat hierbij onder andere om de (toenemende mate van) versleuteling (encryptie) van elektronische gegevens (door criminelen)[29] en het gebruik van draadloze netwerken[30] en cloudcomputingdiensten.[31]

Van 'binnendringen' is in dit verband in ieder geval sprake indien de toegang tot het geautomatiseerde werk wordt verworven door het doorbreken van een beveiliging, door een technische ingreep, met behulp van valse signalen of een valse sleutel, of door het aannemen van een valse hoedanigheid.[32]

Het doel van het binnendringen is het verrichten van onderzoekshandelingen in het binnengedrongen geautomatiseerde werk. De wet omschrijft – limitatief – de volgende mogelijke onderzoeksdoelen:

a. de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of van de

[28] Tijdens de parlementaire behandeling van het voorstel tot de Wet computercriminaliteit III heeft (bij de meeste gelegenheden) de toenmalige staatssecretaris van Justitie en Veiligheid het wetsvoorstel verdedigd. In dit rapport zal evenwel steeds zonder onderscheid tussen de minister en de staatssecretaris worden gesproken van 'de minister' (van Justitie, van Veiligheid en Justitie, dan wel van Justitie en Veiligheid).

[29] *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 7-10.

[30] *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 10-11.

[31] *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 11 e.v.

[32] Voor de regeling van het binnendringen in een geautomatiseerd werk is aangesloten bij de regeling van de computervredebreuk in het Wetboek van Strafrecht, art. 138ab lid 1 Sr. Zie *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 15.

gebruiker, zoals de identiteit of locatie, en de vastlegging daarvan;[33]
b. de uitvoering van een bevel tot het aftappen en opnemen van telecommunicatie (ex artikel 126m Sv) of het opnemen van vertrouwelijke communicatie met een technisch hulpmiddel (ex artikel 126l Sv);[34]
c. de uitvoering van een bevel tot stelselmatige observatie (ex artikel 126g Sv);[35]
d. de vastlegging van gegevens die in het geautomatiseerde werk zijn opgeslagen, of die eerst na het tijdstip van afgifte van het bevel worden opgeslagen, voor zover redelijkerwijs nodig om de waarheid aan de dag te brengen;[36]
e. de ontoegankelijkmaking van gegevens (zoals bedoeld in artikel 126cc lid 5).[37]

Onder een 'technisch hulpmiddel' wordt in dit verband verstaan: een softwareapplicatie die gegevens detecteert, registreert en transporteert en waarmee onderzoekshandelingen worden verricht ter uitvoering van een bevel.[38] De toepassing van een technisch hulpmiddel is niet altijd nodig voor het verrichten van onderzoekshandelingen in een geautomatiseerd werk. Onderzoekshandelingen kunnen ook 'ad hoc en handmatig' worden verricht.[39]

Waarborgen en de verantwoordelijkheid van het OM

Het bevel tot binnendringen en het verrichten van onderzoekshandelingen in een geautomatiseerd werk kent een aantal wettelijke vereisten, zoals:

1. het bevel betreft een geval waarin een verdenking is gerezen ter zake van een misdrijf van een bepaalde aard en ernst. Indien het bevel wordt gegeven met het oog op de onderzoeksdoelen die hierboven zijn genoemd onder a, b en c dient de verdenking een misdrijf te betreffen als omschreven in artikel 67 lid 1 Sv dat gezien zijn aard of samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert.[40] Indien het bevel wordt gegeven met het oog op de onder d en e genoemde onderzoeksdoelen dient de verdenking een misdrijf te betreffen waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaren of meer is gesteld, dan wel een misdrijf dat bij het Besluit onderzoek in een geautomatiseerd werk[41] specifiek is aangewezen;
2. het onderzoek naar het misdrijf vordert dringend de uitoefening van deze bevoegdheid, en
3. voorafgaand aan het bevel verleent de rechter-commissaris aan de officier van justitie daartoe een machtiging.

Bovendien heeft de minister gewezen op een aantal aanvullende waarborgen om de kwaliteit en de rechtmatigheid van de uitoefening van de bevoegdheid te garanderen en de inbreuk op grondrechten te beperken. Het gaat onder meer om de volgende waarborgen:

---

33 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), paragraaf 2.3.1.
34 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), paragraaf 2.3.4.
35 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), paragraaf 2.3.5.
36 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), paragraaf 2.3.2.
37 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), paragraaf 2.3.3.
38 Zie art. 1 onder f van het Besluit onderzoek in een geautomatiseerd werk (dat hieronder meer volledig wordt genoemd).
39 Zie de nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk, *Stb.* 2018, 340, p. 16.
40 Met het oog op de onder a, b en c genoemde onderzoeksdoelen opent art. 126uba lid 1 Sv de mogelijkheid het bevel te geven in die gevallen waarin in georganiseerd verband misdrijven als omschreven in art. 67 lid 1 Sv worden beraamd of gepleegd die gezien hun aard of de samenhang met andere misdrijven die in dat georganiseerd verband worden beraamd of gepleegd een ernstige inbreuk op de rechtsorde opleveren. Art. 126zpa Sv opent met het oog op die onderzoeksdoelen de mogelijkheid het bevel te geven in geval van aanwijzingen voor een terroristisch misdrijf. Deze artikelen komen in hoofdstuk 3 meer uitgebreid aan bod.
41 Volledig: Besluit van 28 september 2018, houdende regels over de uitoefening van de bevoegdheid tot het binnendringen in een geautomatiseerd werk en het al dan niet met een technisch hulpmiddel onderzoek doen als bedoeld in de artikelen 126nba, eerste lid, 126uba, eerste lid, en 126zpa, eerste lid van het Wetboek van Strafvordering (Besluit onderzoek in een geautomatiseerd werk), *Stb.* 2018, 340.

1. Allereerst dient de officier van justitie niet alleen voorafgaand aan de uitoefening van de bevoegdheid daartoe door de rechter-commissaris te worden gemachtigd, maar moet ook binnen de organisatie van het OM zelf goedkeuring worden verkregen.[42] De voorgenomen toepassing van de bevoegdheid dient namelijk door de officier van justitie aan de Centrale toetsingscommissie (CTC)[43] voor advies te worden voorgelegd. Dit advies wordt vervolgens voorgelegd aan het College van procureurs-generaal, dat over de voorgenomen toepassing beslist.[44] Pas daarna benadert de officier van justitie de rechter-commissaris met een vordering tot het verkrijgen van een machtiging voor het verlenen van een bevel tot binnendringen en het verrichten van onderzoekshandelingen in een geautomatiseerd werk.

2. Wanneer het OM heeft besloten tot de uitoefening van deze bevoegdheid dient het bevel van de officier van justitie aan een aantal nauwkeurig omschreven inhoudelijke eisen te voldoen. Deze eisen komen voor een belangrijk deel overeen met de eisen aan het bevel tot de toepassing van andere bijzondere opsporingsbevoegdheden. Doel van deze eisen is om de rechter-commissaris afdoende in staat te stellen tot toetsing van de proportionaliteit en subsidiariteit van de uitoefening van de bevoegdheid.

3. Binnendringen en het verrichten van onderzoekshandelingen in een geautomatiseerd werk is nader genormeerd in het Besluit onderzoek in een geautomatiseerd werk (hierna ook: het Besluit, of: Bogw).[45] Die normen houden onder meer het volgende in:
   a. Het daadwerkelijke binnendringen ter uitvoering van het bevel van de officier van justitie wordt uitsluitend verricht door daartoe aangewezen opsporingsambtenaren van een 'technisch team'.[46] De opsporingsambtenaren van het technische team behoren niet tot het rechercheteam dat het tactische onderzoek uitvoert. Met deze functiescheiding wordt beoogd het risico op tunnelzicht te verminderen.[47]
   b. Nadere eisen worden gesteld aan het technisch hulpmiddel (de softwareapplicatie) met gebruik waarvan onderzoekshandelingen in een geautomatiseerd werk worden verricht.[48]
   c. Door de geautomatiseerde vastlegging (logging) van gegevens over de verwerking van gegevens bij het verrichten van onderzoekshandelingen in een geautomatiseerd werk kan worden gecontroleerd welke handelingen al dan niet met gebruik van een technisch hulpmiddel in het desbetreffende geautomatiseerde werk hebben plaatsgehad, zodat op een later moment geen twijfel kan bestaan over de aard en consequenties van de onderzoekshandelingen die zijn verricht bij de uitvoering van het bevel.[49]

4. Ingevolge de artikelen 132a en 148 Sv en artikel 12 Politiewet 2012 (hierna: Politiewet) komt het gezag over de verrichtingen van opsporingsambtenaren toe aan de officier van justitie. De opsporingsambtenaar van het technische team maakt van de door hem

---

42 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 37 e.v.

43 De CTC, samengesteld uit leden van het OM en de Nationale politie, is een intern adviesorgaan van het OM, dat het College van procureurs-generaal adviseert omtrent de voorgenomen inzet van bepaalde bijzondere opsporingsbevoegdheden en methodieken. Zie de Aanwijzing opsporingsbevoegdheden, 2014A009, van het College van procureurs-generaal, *Stcrt.* 2014, 24442, paragraaf 5.1.

44 Zie de Aanwijzing opsporingsbevoegdheden, 2014A009, van het College van procureurs-generaal, *Stcrt.* 2014, 24442.

45 Volledig: Besluit van 28 september 2018, houdende regels over de uitoefening van de bevoegdheid tot het binnendringen in een geautomatiseerd werk en het al dan niet met een technisch hulpmiddel onderzoek doen als bedoeld in de artikelen 126nba, eerste lid, 126uba, eerste lid, en 126zpa, eerste lid van het Wetboek van Strafvordering (Besluit onderzoek in een geautomatiseerd werk), *Stb.* 2018, 340. De wettelijke grondslag van dit besluit is gelegen in art. 126nba lid 1 en lid 8 Sv, art. 126uba lid 1 en lid 3 Sv, art. 126zpa lid 1 en lid 3 Sv, art. 126ee Sv, en art. 18 lid 1 van de Wet politiegegevens.

46 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 30.

47 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 31. Zie in het bijzonder artt. 3, 4 en 24 Bogw.

48 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 31. Zie in het bijzonder de hoofdstukken 5 en 6 Bogw.

49 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 14 en 31. Zie in het bijzonder artt. 5, 6 en 7 Bogw.

verrichte handelingen ten spoedigste proces-verbaal op (artikel 152 Sv).[50] Ingevolge lid 2 van artikel 152 Sv kan het opmaken van proces-verbaal onder verantwoordelijkheid van de officier van justitie achterwege worden gelaten.

5. In afwachting van de verdere ontwikkeling van het internationaalrechtelijke kader voor de uitoefening van rechtsmacht bij de bestrijding van computercriminaliteit zal naar het oordeel van de minister van Justitie en Veiligheid zelfstandig opgetreden moeten kunnen worden om te voorkomen dat het internet een vrijplaats wordt voor criminaliteit. Dit kan met zich brengen dat opsporingshandelingen worden verricht met betrekking tot gegevens die niet in Nederland zijn opgeslagen.[51] Er zijn toetsingscriteria opgesteld voor dit optreden. Deze criteria zijn neergelegd in de Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex artikel 126nba Sv, die in paragraaf 4.2 uitgebreid aan bod komt. Indien dat bekend is dient in het bevel te worden vermeld dat de gegevens niet in Nederland zijn opgeslagen, zodat van dit optreden rekenschap kan worden afgelegd bij de rechter-commissaris.[52]

Zoals gezegd wordt het hiervoor globaal omschreven kader nader uitgewerkt in hoofdstuk 3. Daarin worden ook de getoetste items verantwoord. Nog drie opmerkingen van meer algemene aard.

Een sleepnetmethode?

De inzet van de bevoegdheid tot het heimelijk binnendringen in een geautomatiseerd werk is op grond van de Wet computercriminaliteit III beperkt tot individuele gevallen, namelijk gevallen waarin een verdenking van betrokkenheid van een verdachte bij ernstige strafbare feiten is gerezen, aldus de minister. Het betreft hier geen bevoegdheid op grond waarvan gegevens worden verzameld van grote groepen van personen jegens wie er op het moment van het verzamelen van de gegevens geen aanwijzingen zijn van betrokkenheid bij een strafbaar feit.[53]

Rechtmatigheidstoets achteraf

Uit de parlementaire geschiedenis van de Wet computercriminaliteit III en het Besluit onderzoek in een geautomatiseerd werk, alsook uit wetenschappelijke literatuur, blijkt dat bij verscheidene Tweede Kamerleden en juridische auteurs niet alleen de rechtmatigheidstoets van het inzetten van de bevoegdheid *vooraf*, maar ook de rechtmatigheidstoets *achteraf*

---

50 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 39. Zie ook art. 24 Bogw.

51 In dit verband wordt gewezen op art. 32 van het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, Boedapest, 23 november 2001, *Trb.* 2002, 18, en *Trb.* 2004, 290, verkort: het Cybercrime Verdrag. De toepassingsmogelijkheden van art. 32 zijn echter beperkt. Deze bepaling reikt niet verder dan (a) het zich toegang verschaffen tot opgeslagen publiekelijk toegankelijke (open bron) computergegevens, ongeacht waar deze zich in geografisch opzicht bevinden (maar dan wél op het territoir van een partij bij dit verdrag), of (b) het via een computersysteem dat zich op Nederlands grondgebied bevindt, zich toegang verschaffen tot of de beschikking krijgen over opgeslagen computergegevens die zich bevinden in een andere staat (die partij is bij dit verdrag), indien Nederland de rechtmatige en vrijwillige instemming verkrijgt van de persoon die gerechtigd is de gegevens via dat computersysteem aan Nederland te verstrekken. Zie B.J. Koops, C. Conings & F. Verbruggen, *Zoeken in computers naar Nederlands en Belgisch recht. Welke plaats hebben de 'digitale plaatsen' in de systematiek van opsporingsbevoegdheden?* (Preadvies voor de jaarvergadering van de NVVS 2016), Oisterwijk: Wolf Legal Publishers 2016, p. 137 e.v.; J.J. Oerlemans, *Investigating cybercrime* (diss. Leiden), z.p., z.u., 2017, p. 416-417; J.J. Oerlemans, 'Jurisdictie en grensoverschrijdende digitale opsporing', in: B.J. Koops & J.J. Oerlemans (red.), *Strafrecht & ICT*, Den Haag: Sdu 2019, p. 209-232, en zie de opiniebijdrage: M. Zoetekouw, 'Internationaalrechtelijke aspecten van het wetsvoorstel Computercriminaliteit III', *Tijdschrift voor Internetrecht* 2017, afl. 1, p. 30-33.

52 Zie ook *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 44-50, en de nota van toelichting bij het Bogw, p. 11.

53 *Kamerstukken I* 2018/19, 34 372, M (Verslag van een nader schriftelijk overleg), p. 5. Zie ook *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 27-28.

een punt van zorg is.[54] Hoewel voorzien is in systeemtoezicht door de Inspectie Justitie en Veiligheid, strekken onderzoeken van de Inspectie Justitie en Veiligheid zich niet uit tot vraagstukken over de rechtmatigheid van het optreden door het OM.[55] De minister heeft te kennen gegeven waarde te hechten aan een onafhankelijke rechterlijke toetsing *vooraf*, namelijk door de rechter-commissaris, en hij is van oordeel dat de rechtmatigheidstoets daarmee voldoende is gecodificeerd.[56] Het blijft echter de vraag of en in hoeverre ook tijdens en na het toepassen van de bevoegdheid de controle op de rechtmatigheid ervan wordt geborgd. Hier ligt in elk geval een taak voor het OM, dat immers is belast met het gezag en de controle op opsporingsactiviteiten van de politie.

Binnendringen en onderzoek in een geautomatiseerd werk voorafgaand aan de invoering van een specifieke wettelijke grondslag

Jurisprudentie en vakliteratuur wijzen uit dat reeds voorafgaand aan de invoering van de bevoegdheid tot (op afstand heimelijk) binnendringen en het verrichten van onderzoekshandelingen in een geautomatiseerd werk dergelijke, althans (enigszins) vergelijkbare opsporingsmethoden werden toegepast. Het gaat dan bijvoorbeeld om zaken waarin de politie zich toegang had verworven tot een online (e-mail)account,[57] een router van een hostel, een *command-and-control-server* van een botnet,[58] en tot verborgen diensten op het Tor-netwerk,[59] alsmede om zaken waarin de politie spionagesoftware op

---

54 Een amendement met de strekking om een commissie van toezicht op de opsporingsdiensten in te richten met als taak de inzet van de hackbevoegdheid achteraf te toetsen (zie *Kamerstukken II* 2016/17, 34 372, nr. 12) is in de Tweede Kamer niet aangenomen (zie Overzicht van stemmingen in de Tweede Kamer, artikel II, onderdeel U). Zie ook de (afgewezen) motie van het Kamerlid Strik met de strekking dat een onafhankelijke commissie in het leven wordt geroepen die een hackoperatie achteraf toetst op noodzaak, rechtmatigheid, doelmatigheid en proportionaliteit, *Kamerstukken I* 2017/18, 34 372, J; en in dat verband: *Handelingen I* 2017/18, nr. 34, item 5, p. 20. Zie voorts S.J. Eskens, O.L. van Daalen & N.A.N.M. van Eijk, *Geheime surveillance en opsporing. Richtsnoeren voor de inrichting van wetgeving,* Amsterdam: Instituut voor Informatierecht (UvA) 2016.

55 *Handelingen I* 2017/18, nr. 34, item 5, p. 19.

56 Zie bijv. *Handelingen I* 2017/18, nr. 34, item 5, p. 35-36, waarin de minister een motie tot instellen van een onafhankelijke commissie ontraadt.

57 Zie rechtbank Rotterdam 26 maart 2010, ECLI:NL:RBROT:2010:BM2520, en (het daaropvolgend hoger beroep): gerechtshof Den Haag 27 april 2011, ECLI:NL:GHSGR:2011:BR6836.

58 Een 'bot' (afkorting van softwarerobot) is een geautomatiseerd werk van een willekeurige (onwetende) gebruiker die door een infectie met malware door de 'inbreker' kan worden gecontroleerd en waaraan de inbreker buiten de gebruiker om opdrachten kan geven. Een 'bot*net*' is een grootschalig en wereldwijd netwerk van semiautonoom werkende bots, die op afstand kunnen worden bediend om illegale acties uit te voeren, zoals het versturen van spam, het verzamelen van (bedrijfs)geheimen en andere vertrouwelijke informatie zoals creditcardgegevens en wachtwoorden, het uitvoeren van DDoS-aanvallen en het verspreiden van malware zoals ransomware (een infectie die de computer blokkeert en pas vrijgeeft nadat losgeld is betaald). Na een succesvolle besmetting kan ongemerkt meer kwaadaardige software worden geïnstalleerd, waaronder sniffers (computerprogramma's waarmee het dataverkeer op het netwerk kan worden bekeken en geanalyseerd) en keyloggers (computerprogramma's die toetsaanslagen vastleggen). Om een botnet onschadelijk te kunnen maken, is het noodzakelijk om toegang te verkrijgen tot de servers die onderdeel vormen van het botnet. Zo heeft de Nationale Recherche in 2010 het Bredolab-botnet offline gehaald door een groot aantal 'command and control'-servers af te sluiten die bij een Nederlandse hostingprovider stonden. Vanuit dit botnet zijn vanaf 2009 naar schatting dagelijks 3,6 miljard e-mails verstuurd. Het botnet werd daarnaast ook verhuurd aan andere cybercriminelen voor onder meer DDoS-aanvallen en het verspreiden van malware. Zie *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 21-22. Zie voor een ouder geval van een botnet: G. Keizer, 'Dutch Botnet Suspects Ran 1.5 Million Machines', *Techweb Network* 21 oktober 2005, http://www.techweb.com/wire/security/172303160. Zie voor meer recente gevallen waarin een botnet offline is gehaald, te weten het Mirai-botenet: https://www.om.nl/actueel/nieuws/2021/02/11/om-eist-15-maanden-tegen-host-van-agressief-mirai-botnet; en het Emotet-botnet: https://www.agconnect.nl/artikel/politie-legt-groot-emotet-botnet-plat, en Internationale politieoperatie LadyBird: botnet Emotet wereldwijd ontmanteld | Nieuwsbericht | Openbaar Ministerie (om.nl).

59 Zie bijv. J.J. Oerlemans, *Investigating cybercrime* (diss. Leiden), z.p., z.u., 2017, p. 270.

een computer had geplaatst.[60] Deze opsporingsactiviteiten waren gegrond op de indertijd vigerende wettelijke bepalingen, te weten de computerdoorzoeking (artikel 125i Sv), de netwerkdoorzoeking (artikel 125j Sv) en het opnemen van vertrouwelijke communicatie met een technisch hulpmiddel (artikel 126l Sv). Mogelijk waren (enkele van) deze vormen van binnendringen en onderzoek in het kader van de opsporing naar ernstige misdrijven wettelijk gelegitimeerd.[61] Zeker is dat echter niet. De vraag is of het gebruik van die methoden berustte op een toereikende wettelijke grondslag en of die methoden onder de verantwoordelijkheid van het OM ook overigens rechtmatig zijn toegepast.[62] Uit de naslag van jurisprudentie blijkt dat die wettelijke grondslag niet altijd als toereikend werd beoordeeld.[63]

[60] Zie bijv. de brief van de minister van Veiligheid en Justitie van 7 oktober 2014 in antwoord op Kamervragen van het lid Gesthuizen over het gebruik van omstreden spionagesoftware door de politie, *Aanhangsel Handelingen II* 2013/14, 202, waarin de minister meedeelde: "*De politie beschikt over software die fysiek geïnstalleerd kan worden op de computer van een verdachte, waarmee ten behoeve van opsporingsdiensten toegang kan worden verkregen tot die computer en waarmee gegevens daarvan kunnen worden overgenomen. De inzet van dit middel beperkt zich, gelet op de bepalingen van het Wetboek van Strafvordering, tot het opnemen van vertrouwelijke communicatie (op basis van artikel 126l van het Wetboek van Strafvordering). Inzet ten behoeve van een heimelijke doorzoeking van gegevensdragers is binnen de wettelijke kaders niet toegestaan. Voorts is het onder bepaalde omstandigheden op basis van artikel 125i van het Wetboek van Strafvordering op basis van een machtiging van de rechter-commissaris mogelijk om op afstand een computersysteem te betreden, met als uitsluitende doel de computer te doorzoeken op vooraf bepaalde gegevensbestanden en deze zo nodig in beslag te nemen door ze vast te leggen.*" Zie M. Persson, 'Politie gebruikt mogelijk omstreden spionagesoftware', *Volkskrant* 8 augustus 2014, https://www.volkskrant.nl/cultuur-media/politie-gebruikt-mogelijk-omstreden-spionagesoftware-~be396101/.

[61] Zie ook reeds eerder J.J. Oerlemans, 'Hacken als opsporingsbevoegdheid', *DD* 2011, afl. 8/62, p. 888-908.

[62] Zie J.J. Oerlemans, *Investigating cybercrime* (diss. Leiden), z.p., z.u., 2017, die deze vraag uitgebreid behandelt ten aanzien van de inzet van verschillende digitale opsporingsmethoden.

[63] Zie bijv. rechtbank Rotterdam 1 januari 2018, ECLI:NL:RBROT:2018:10895, in welke zaak de RC de vordering van de OvJ – die in feite neerkwam op het (doen) inloggen op het Telegram-account van de verdachte en op het vastleggen van de daarin opgenomen gegevens – afwees omdat de wet hiervoor geen grondslag bood. Deze afwijzende beslissing van de RC is door de raadkamer vernietigd; de machtiging is alsnog verleend (rechtbank Rotterdam 22 februari 2019, ECLI:NL:RBROT:2019:2712). Zie verder: rechtbank Rotterdam 1 januari 2018, ECLI:NL:RBROT:2018:8017 (RC wijst vordering inzage web-e-mail af), en zie: rechtbank Den Haag 11 januari 2019, ECLI:NL:RBDHA:2019:1329 (RC wijst vordering tot het inloggen op de e-mailadressen en websites met vooraf beschikbare gebruikersnamen en wachtwoorden toe).
Zie ook gerechtshof Den Haag 19 december 2018, ECLI:NL:GHDHA:2018:3529, waarin een netwerkdoorzoeking op een andere plaats dan waar de doorzoeking had plaatsgevonden onrechtmatig werd geoordeeld.

2. Het toezichtonderzoek

2.1. De onderzoeksdoelstelling en de onderzoeksvraag

De hierboven geschetste ontwikkelingen en bevindingen ondersteunen de noodzaak van empirisch-juridisch toezichtonderzoek naar het functioneren van het OM met betrekking tot het (doen) uitvoeren van onderzoek in een geautomatiseerd werk en het toezicht door het OM op de daadwerkelijke uitvoering daarvan. De doelstelling van het toezichtonderzoek in het kader van artikel 122 RO is om na te gaan of het OM hierbij de geldende rechtsregels in acht neemt. Daartoe hoeft geen integrale praktijkevaluatie plaats te vinden. Met empirisch-juridisch toezichtonderzoek dat een signaleringsfunctie heeft, kan afdoende worden vastgesteld of er tekortkomingen zijn dan wel aspecten bestaan die voor verbetering vatbaar zijn. Zo dit het geval is, kunnen aanbevelingen worden gedaan over de wijze waarop het functioneren van het OM op dit terrein kan worden verbeterd.[64]

Het toezichtonderzoek spitst zich toe op de volgende centrale probleemstelling:

> Voldoet de wijze waarop het OM toepassing geeft aan de bevoegdheid tot onderzoek in een geautomatiseerd werk aan de daarvoor geldende wettelijke voorschriften en de beginselen van proportionaliteit, subsidiariteit en behoorlijkheid, en is het toezicht op de uitvoering daarvan toereikend?

De nadruk van het empirisch-juridisch toezichtonderzoek ligt op de rol van de officier van justitie en de wijze waarop binnen de organisatie van het OM de besluitvorming over het toepassen van de bevoegdheid plaatsvindt, alsmede de wijze waarop het toezicht en de controle van het OM op de daadwerkelijke uitvoering daarvan zijn geoperationaliseerd. Met de onderzoeksvraag is tevens een afbakening van het toezichtonderzoek gegeven.

Het daadwerkelijk uitvoeren van onderzoek in een geautomatiseerd werk door de politie, alsook de rol van andere actoren daarbij wordt vanwege de taakopvatting van de PG-HR op zichzelf niet betrokken in het empirisch-juridisch toezichtonderzoek, behoudens over de band van de taken en verantwoordelijkheden van het OM. Bij deze keuze heeft de PG-HR in aanmerking genomen dat de Inspectie Justitie en Veiligheid zelfstandig onderzoek heeft verricht en nog steeds verricht naar het uitvoeren van onderzoek in een geautomatiseerd werk door het technische team van de politie. Met inachtneming van de voorschriften die gelden op het terrein van de bescherming van politiegegevens en van justitiële en strafvorderlijke gegevens heeft de PG-HR kennisgenomen van en acht geslagen op de (tussentijdse) resultaten van dit onderzoek door de Inspectie Justitie en Veiligheid. De PG-HR heeft deze (tussentijdse) bevindingen bovendien in aanmerking genomen bij het toezichtonderzoek en daarin aanleiding gevonden zijn onderzoek bij te sturen.

Geen onderwerp van het toezichtonderzoek van de PG-HR is de beslissing van de rechter-commissaris op de vordering van de officier van justitie tot het verlenen van een machtiging voor het bevel tot het uitvoeren van onderzoek in een geautomatiseerd werk. Bij die gelegenheid toetst de rechter-commissaris de proportionaliteit en subsidiariteit, en meer in het algemeen de rechtmatigheid van het door de officier van justitie voorgenomen bevel. De uitkomst van die toets is in dit toezichtonderzoek een gegeven. Wel wordt in het toezichtonderzoek separaat stilgestaan bij de vraag of de rechter-commissaris die toets daadwerkelijk heeft uitgevoerd, of het OM hem daartoe heeft voorzien van adequate informatie en of het OM zelf op behoorlijke wijze vorm en inhoud heeft gegeven aan de rechtmatigheidstoets.

[64] Zie ook het art. 122 RO-onderzoek naar de strafbeschikking: G. Knigge & C.H. de Jonge van Ellemeet (onderzoekers), *Beschikt en gewogen. Over de naleving van de wet door het openbaar ministerie bij het uitvaardigen van strafbeschikkingen,* Den Haag: 2014, p. 21.

Aandacht verdient dus de vraag hoe het OM in de praktijk invulling heeft gegeven aan de hem toebedeelde verantwoordelijkheid voor de effectuering van de waarborgen die in het wettelijke kader zijn omschreven.
In dit verband kunnen bij de uitoefening van de bevoegdheid grofweg de volgende drie fasen worden onderscheiden:

a. *de fase van besluitvorming*, te weten de fase waarin wordt overwogen om aan de bevoegdheid toepassing te geven, waarin eventueel wordt getracht daartoe een machtiging van de rechter-commissaris te verkrijgen, tot en met de beslissing van de officier van justitie om – al dan niet na verkregen machtiging van de rechter-commissaris – onderzoek in een geautomatiseerd werk te bevelen (de voorfase);
b. *de fase van executie*, waarin al dan niet na een bevel van de officier van justitie uitvoering wordt gegeven aan binnendringen en het verrichten van onderzoekshandelingen in een geautomatiseerd werk en waarin eventueel verkregen gegevens worden vastgelegd (de uitvoeringsfase);
c. *de fase na de beëindiging* van de uitvoering van het onderzoek in een geautomatiseerd werk, waarin de daarbij verkregen gegevens al dan niet worden verwerkt, met inbegrip van het ter beschikking stellen van de gegevens aan het tactisch team (de verwerkingsfase).

2.2. Deelvragen

De deelvragen die bijdragen aan de beantwoording van bovenstaande hoofdvraag zijn de volgende:

1. Welk normatief kader is op basis van relevante verdragsbepalingen, het Wetboek van Strafvordering en overige wet- en regelgeving, jurisprudentie, literatuur alsmede de beginselen van proportionaliteit en subsidiariteit, van toepassing op de beslissing tot het uitvoeren van onderzoek in een geautomatiseerd werk en het toezicht van de zijde van het OM daarop? Deze deelvraag zal hieronder in hoofdstuk 3 worden besproken.

2. In hoeverre en op welke gronden wordt tot toepassing van de bevoegdheid tot het uitvoeren van onderzoek in een geautomatiseerd werk overgegaan en wat zijn hierbij de gehanteerde criteria en procedurele waarborgen? Deze deelvraag strekt zich uit over het door het OM geformuleerd algemene beleid[65] aangaande de beslissing om tot uitoefening van de bevoegdheid over te gaan en betreft daarmee een beleidstoets. Van belang hierbij is in welke mate het beleid voldoet aan de procedurele waarborgen zoals vervat in de toepasselijke wettelijke voorschriften. Het gaat hierbij onder meer om de rol van het College van procureurs-generaal en van de Centrale toetsingscommissie (CTC). Deze deelvraag zal hieronder worden besproken in hoofdstuk 4.

3. Hoe wordt door het OM de controle (tijdens en achteraf) op de inzet van de bevoegdheid nader vormgegeven? Deze deelvraag heeft betrekking op het door het OM geformuleerde algemene beleid aangaande het monitoren van de bevoegdheidsuitoefening en betreft daarmee een beleidstoets. Van belang is in welke mate wordt voldaan aan de procedurele waarborgen zoals vervat in de toepasselijke wettelijke voorschriften. Daarnaast is bijvoorbeeld van belang in hoeverre de rechtmatigheid van het onderzoek in een geautomatiseerd werk wordt gewaarborgd door een toets achteraf.

[65] Hierbij kan onder andere gedacht worden aan aanwijzingen, (interne) beleidsstukken of richtlijnen en procesbeschrijvingen.

4. Op welke wijze wordt de verantwoordelijkheid van de officier van justitie voor het onderzoek in een geautomatiseerd werk en het toezicht op de uitvoering daarvan in de praktijk en in het concrete geval vormgegeven? Anders dan in de voorgaande twee deelvragen, gaat het bij deze deelvraag om een praktijktoets op zaaksniveau. Van belang hierbij is in welke mate in het concrete geval conform de wettelijke voorschriften en het beleid van het OM dienaangaande wordt besloten tot het uitvoeren van onderzoek in een geautomatiseerd werk en vervolgens daarop controle wordt gehouden. Worden bij de besluitvorming bijvoorbeeld bepaalde alternatieven overwogen en wordt er zorgvuldig op toegezien dat alleen die onderzoekshandelingen worden verricht die de rechter-commissaris heeft omschreven in de machtiging en die de officier van justitie heeft bevolen?

5. Welke rol speelt de politie, in het bijzonder het technische team, in de praktijk bij de beslissing tot het uitvoeren van onderzoek in een geautomatiseerd werk en het toezicht daarop? Hoe verhoudt deze rol zich tot de taakverdeling tussen politie en OM, waarbij de officier van justitie de leiding heeft over en toezicht houdt op het opsporingsonderzoek dat wordt uitgevoerd door opsporingsambtenaren?

6. Hoe geeft de officier van justitie vorm en inhoud aan zijn schakelfunctie tussen enerzijds het technische team dat daadwerkelijk binnendringt en onderzoekshandelingen verricht in het geautomatiseerde werk en anderzijds het tactische team van de politie dat het opsporingsonderzoek verricht in de strafzaak in het kader waarvan wordt binnengedrongen in het geautomatiseerde werk? Bij deze deelvraag gaat het zowel om een algemene beleidstoets als om een praktijktoets op zaaksniveau.

2.3. De onderzoeksmethode

Het vooronderzoek

Ten behoeve van het toezichtonderzoek is reeds vooronderzoek verricht teneinde afgebakende en concrete onderzoeksvragen te formuleren en de uitvoering van het onderzoek voor te bereiden. Onderdeel van het vooronderzoek waren verkennende gesprekken met het OM over het onderzoeksonderwerp. Deze gesprekken werden gevoerd met mr. R. Otte, procureur-generaal van het OM, mr. F. Westerbeke, (destijds) hoofdofficier van justitie van het landelijk parket, en (meermalen) met de senior-officier van justitie die als liaison is verbonden aan het Parket-Generaal. Daardoor is een eerste beeld ontstaan van het probleemveld en is besloten op welk thema het toezichtonderzoek zich zal richten.
Vervolgens is een oriënterend gesprek gevoerd met de landelijke cyberofficier, met de toenmalige digit-officier en met de parketsecretaris die de digit-officier van justitie bijstaat.[66] Bovendien is een eerste inzage verkregen in het dossier van een zaak waarbij de bevoegdheid ex artikel 126nba Sv is ingezet. Tot het vooronderzoek behoorden bovendien het verrichten van wetgevings-, jurisprudentie- en literatuuronderzoek. Het verslag daarvan is te vinden in hoofdstuk 3.

Het vervolg: de opzet van het onderzoek en de daarbij gebruikte methoden

De methoden voor toezichtonderzoek naar de rol van het OM bij het (doen) uitvoeren van onderzoek in een geautomatiseerd werk zijn divers. Het betreft uitsluitend kwalitatief onderzoek waarvan het literatuur-, wetgevings- en jurisprudentieonderzoek onderdeel is. Daarnaast is het antwoord op de onderzoeksvragen gezocht met behulp van zelfrapportage door het OM en door bestudering van een aantal zaken waarvan dossiers zijn samengesteld

[66] De rol van deze functionarissen wordt nader beschreven in hoofdstuk 4 van deze rapportage.

door de digit-officier en de digit-parketsecretaris, hier ook de 'nba-dossiers' genoemd.[67] Daarmee wordt inzicht verkregen in de besluitvorming met betrekking tot het uitvoeren van onderzoek in een geautomatiseerd werk en in de resultaten ervan. Deze nba-dossiers betreffen niet het strafdossier van de strafzaak in het kader waarvan de bevoegdheid is toegepast. De nba-dossiers zijn samengesteld ten behoeve van het toezichtonderzoek. Deze nba-dossiers bevatten zowel méér informatie als minder informatie dan de strafdossiers. Het meerdere betreft informatie over de fase van besluitvorming en uitvoering; in de nba-dossiers zijn echter niet alle resultaten van het tactisch opsporingsonderzoek opgenomen.

De uitvoering van het toezichtonderzoek

Deze eindrapportage betreft (uitsluitend) de werkwijze van het OM over de jaren 2019, 2020 en 2021, alsmede de zaken in die jaren waarin is besloten tot de uitvoering van onderzoek in een geautomatiseerd werk. Wat betreft de bestudeerde dossiers het volgende. In het jaar 2019 heeft het technische team van de politie in acht zaken (met vaak meer verdachten) een aanvang gemaakt met de uitvoering van een bevel op grond van artikel 126nba lid 1 Sv. In drie zaken hebben de onderzoekers de dossiers uitvoerig bestudeerd. De selectie van de zaken vond plaats door de onderzoekers. Van de overige zaken uit 2019 is (op basis van andere informatie dan dossieronderzoek) meer globaal kennisgenomen.[68]
In het jaar 2020 is de bevoegdheid in veertien zaken ingezet, waarvan in twee zaken de inzet reeds was aangevangen in 2019. De onderzoekers hebben in vijf zaken de dossiers bestudeerd.
In het jaar 2021 heeft de inzet van de bevoegdheid in 28 zaken plaatsgevonden, waarvan in vijf zaken de inzet reeds in een eerder jaar is aangevangen. De onderzoekers hebben van één zaak het dossier bestudeerd.
Uiteindelijk zijn dus in negen zaken de 'nba-dossiers' onderzocht. Drie van deze zaken zijn door de onderzoekers geselecteerd om nader te onderzoeken aan tactische zijde, dat wil zeggen dat ook de relevante informatie en stukken die zijn ondergebracht bij het tactisch team en de zaaksofficier zijn bestudeerd. Ten aanzien van deze drie zaken zijn ook semigestructureerde interviews gevoerd met de betrokken officieren van justitie. Het gaat daarbij om de zaaksofficier, de (aan het desbetreffende parket verbonden) rechercheofficier en de (aan het desbetreffende parket verbonden) cyberofficier. In de overige zes zaken zijn schriftelijke vragen gesteld aan de zaaksofficieren om ook in die zaken inzicht te verkrijgen in de tactische zijde van de inzet van de bevoegdheid.

De naleving van de toepasselijke voorschriften is in de nba-dossiers getoetst aan de hand van een checklist. De items op de checklist hebben hoofdzakelijk betrekking op de toelaatbaarheid van de uitvoering van onderzoek in een geautomatiseerd werk, de wijze waarop daarover wordt beslist en door wie, alsmede de inhoud en motivering van deze beslissing. Het gaat daarbij onder meer om de vraag of de geldende criteria in acht zijn genomen en of is gehandeld in overeenstemming met het beleidskader dat het OM voor zichzelf heeft opgesteld. Vervolgens wordt aan de hand van andere items nagegaan hoe in concrete gevallen het toezicht tijdens de uitvoering van het onderzoek in een geautomatiseerd werk gestalte heeft gekregen, in hoeverre is voorzien in een toets achteraf en in hoeverre uitvoering is gegeven aan normen die betrekking hebben op de verwerkingsfase.
Meermalen zijn gesprekken gevoerd met de digit-officier van justitie, zowel met de eerste als met de opvolgende, en met de digit-parketsecretaris, en is informatie (hoofdzakelijk mondeling) opgevraagd en verkregen. Dit betroffen telkens semigestructureerde interviews.

[67] De letters 'nba' verwijzen naar de extensie van art. 126nba Sv, zonder daarbij onderscheid te maken met eventuele gevallen waarin toepassing is gegeven aan de artikelen 126uba Sv of 126zpa Sv.

[68] Gelet op de vertrouwelijke aard van de materie en de daaraan verbonden afbreukrisico's zijn de nba-dossiers in beginsel ter plekke ingezien op een van de kantoren van het landelijk parket van het OM. Zoveel mogelijk zijn de dossiers door beide onderzoekers bestudeerd, en in elk geval zijn de bevindingen voor elk dossier door beide onderzoekers met elkaar besproken.

Zij strekten ertoe informatie te verkrijgen over de relevante werkprocessen binnen het OM op het gebied van de toepassing van de bevoegdheid en de controle daarop. Daarnaast zijn tijdens en na het dossieronderzoek voorlopige resultaten voorgelegd, waarbij ook mogelijke vragen of verklaringen daaromtrent zijn voorgelegd.
Behalve door de interviews met zaaksofficieren, rechercheofficieren en cyberofficieren is ook door deze interviews meer zicht verkregen op de rollen van de onderscheidene functionarissen die betrokken zijn bij de uitvoering van het onderzoek in een geautomatiseerd werk en het toezicht daarop. Tot slot is ook een semigestructureerd interview gevoerd met de voorzitter van de Centrale toetsingscommissie (CTC) en een secretaris teneinde meer zicht te krijgen op de procedure bij de CTC.

3. Het normatief kader

3.1. Inleidende verkenningen

De eerste deelvraag
In dit hoofdstuk staat de eerste deelvraag, die het normatief kader betreft, centraal:

Welk normatief kader is op basis van relevante verdragsbepalingen, het Wetboek van Strafvordering en overige wet- en regelgeving, jurisprudentie, literatuur alsmede de beginselen van proportionaliteit en subsidiariteit, van toepassing op de beslissing tot het uitvoeren van onderzoek in een geautomatiseerd werk en het toezicht van de zijde van het OM daarop?

De bevoegdheid
De bevoegdheid tot het uitvoeren van onderzoek in een geautomatiseerd werk is verankerd in de artikelen 126nba, 126uba en 126zpa Sv. Aan de officier van justitie is in die bepalingen de bevoegdheid toegekend om te bevelen dat een opsporingsambtenaar:
1. een geautomatiseerd werk dat in gebruik is bij een persoon (op afstand heimelijk) *binnendringt*, en
2. hierin, al dan niet met een technisch hulpmiddel, *onderzoekshandelingen verricht* met het oog op specifiek omschreven onderzoeksdoelen.

De eerstgenoemde wettelijke bepaling (artikel 126nba Sv) kent de officier van justitie deze bevoegdheid toe ten aanzien van het geautomatiseerde werk dat in gebruik is bij de verdachte van een misdrijf als omschreven in artikel 67 lid 1 Sv dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert.[69]
Artikel 126uba Sv kent de officier van justitie deze bevoegdheid toe met betrekking tot een geautomatiseerd werk dat in gebruik is bij een persoon ten aanzien van wie uit feiten of omstandigheden een redelijk vermoeden voortvloeit dat hij betrokken is bij het in georganiseerd verband beramen of plegen van misdrijven.
Wanneer aanwijzingen bestaan van het begaan van een terroristisch misdrijf roept artikel 126zpa Sv deze bevoegdheid in het leven ten aanzien van het geautomatiseerde werk dat in gebruik is bij 'een persoon'.
Het toepassingsbereik van de bevoegdheid beperkt zich dus niet tot gevallen van computercriminaliteit. De bevoegdheid kan ook ten aanzien van andere (ernstige) vormen van criminaliteit worden ingezet.[70] De wettelijke voorwaarde van de verdenking van betrokkenheid van een persoon bij een ernstig strafbaar feit staat in de weg aan de inzet van deze bevoegdheid in de vorm van een zogenaamde 'sleepnetmethode'.[71]

De verdachte en het geautomatiseerde werk in kwestie
Hierna wordt omwille van de leesbaarheid meestal alleen gesproken over 'de verdachte' en niet steeds over de in de artikelen 126uba en 126zpa Sv bedoelde personen. De beschouwingen hieronder zijn echter mutatis mutandis van toepassing op de personen die zijn bedoeld in de twee laatstgenoemde bepalingen.
Voor de toepassing van artikel 126nba Sv is niet vereist dat de verdachte van het geautomatiseerde werk de enige gebruiker is. Toepassing is ook mogelijk in het geval waarin

[69] Art. 67 lid 1 Sv bepaalt voor welke misdrijven voorlopige hechtenis mogelijk is. Dat betreft misdrijven waarop naar de wettelijke omschrijving een gevangenisstraf van vier jaar of meer is gesteld, alsook een reeks van andere specifiek genoemde misdrijven.
[70] *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 15. Wel is de bevoegdheid binnen de kring van de misdrijven waarvoor voorlopige hechtenis mogelijk is nader ingekaderd, afhankelijk van de aard van de te verrichten onderzoekshandelingen; zie de bespreking van de onderzoekshandelingen als bedoeld in lid 1 van de artikelen 126nba, 126uba en 126zpa Sv onder d en e verderop.
[71] *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 27-28. Zie ook *Kamerstukken I* 2018/19, 34 372, M (Verslag van een nader schriftelijk overleg), p. 5.

de verdachte gebruikmaakt van het geautomatiseerde werk van een huisgenoot of partner. Het kan tevens gaan om geleende of gestolen geautomatiseerde werken, of om een computer in een internetcafé.[72] Ook kan het gaan om een geautomatiseerd werk waarvan de verdachte in het verleden gebruik heeft gemaakt. Daarnaast houdt de uitoefening van de bevoegdheid in dat ook een geautomatiseerd werk dat in verbinding staat met het geautomatiseerde werk dat in eerste instantie is binnengedrongen, kan worden binnengedrongen en onderzocht, mits dit geautomatiseerde werk bij de verdachte in gebruik is en een bevel tot binnendringen van dat tweede geautomatiseerde werk is afgegeven. De bevoegdheid kan echter niet worden ingezet om te onderzoeken *of* de verdachte daadwerkelijk de gebruiker is van een geautomatiseerd werk. Wel kan de methode worden ingezet om de identiteit van de – op dat moment nog onbekende – verdachte te achterhalen.[73]

Op afstand heimelijk binnendringen

Zoals gezegd kennen de artikelen 126nba, 126uba en 126zpa Sv aan de officier van justitie de bevoegdheid toe om te bevelen dat een geautomatiseerd werk dat in gebruik is bij een verdachte, c.q. een persoon wordt binnengedrongen, waarbij dit volgens de totstandkomingsgeschiedenis van deze wet (i) *heimelijk* en (ii) *op afstand* plaatsvindt.[74, 75]

---

[72] Vgl. *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 133: "*Voor wat betreft het afwisselend gebruik van verschillende geautomatiseerde werken, zoals bijvoorbeeld computers van een internetcafé of van familieleden vormen niet zozeer de wettelijke criteria een belemmering als wel het feitelijk binnendringen in het geautomatiseerde werk, dat een zorgvuldige voorbereiding en uitvoering vergt. Het behoeft nauwelijks betoog dat dit wordt bemoeilijkt als afwisselend gebruik wordt gemaakt van verschillende geautomatiseerde werken.*"

[73] *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 98-99, en *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 41 en 132.

[74] Met 'heimelijk' wordt kennelijk bedoeld dat de gebruiker van het geautomatiseerde werk op het moment van het binnendringen daarvan in het ongewisse wordt gelaten; met 'op afstand' wordt kennelijk bedoeld dat het geautomatiseerde werk fysiek niet binnen het bereik is van degene die binnendringt en dat de toegang tot het geautomatiseerde werk wordt verkregen via een netwerk.
De eis dat het binnendringen in het geautomatiseerde werk 'heimelijk' en 'op afstand' plaatsvindt is niet met zoveel woorden in de artikelen 126nba, 126uba en 126zpa Sv opgenomen; de wettekst sluit het zodoende alleen niet uit. De twee predicaten 'heimelijk' en 'op afstand' worden wel vermeld in de considerans bij het oorspronkelijke wetsvoorstel (*Kamerstukken II* 2015/16, 34 372, nr. 2), alsook – veelvuldig – in de totstandkomingsgeschiedenis van de wet en in de nota van toelichting op het Besluit onderzoek in een geautomatiseerd werk (Bogw). De volgorde van de twee predicaten verschilt daarbij nog wel. De minister heeft een sterke voorkeur voor het gebruik van de terminologie 'op afstand heimelijk', al komt 'heimelijk op afstand', 'heimelijk en op afstand', 'op afstand en heimelijk' sporadisch ook voor. Daaruit kan worden opgemaakt dat de twee predicaten nevengeschikt zijn en dat zij beide betrekking hebben op 'het binnendringen', en niet op elkaar. Of deze predicaten eveneens betrekking hebben op 'het verrichten van onderzoekshandelingen in het (op afstand heimelijk binnengedrongen) geautomatiseerde werk' wordt in de wetsgeschiedenis in het midden gelaten, al lijkt dat wel een veronderstelling te zijn. Al met al is hierdoor niet uitgesloten dat de bevoegdheid van art. 126nba Sv toepassing vindt in een geval waarin het geautomatiseerde werk, bijvoorbeeld een laptop of een mobiele telefoon, heimelijk wordt binnengedrongen op een moment dat het zich fysiek in handen bevindt van een lid van het technisch team (en dus niet 'op afstand' is), het geautomatiseerde werk daarna wordt geretourneerd aan de verdachte, waarna de onderzoekshandelingen weer wél op afstand (en heimelijk) worden verricht.

[75] Vanwege de toegestane heimelijkheid van het binnendringen is artikel 11.7a van de Telecommunicatiewet buiten toepassing verklaard. Zie *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 101: "*In artikel 11.7a van de Telecommunicatiewet (Tw) is kort gezegd geregeld dat indien iemand door middel van elektronische communicatienetwerken toegang wenst te verkrijgen tot gegevens die zijn opgeslagen in de randapparatuur van een gebruiker dan wel gegevens wenst op te slaan in de randapparatuur van die gebruiker, deze daaraan voorafgaand de gebruiker dient te informeren omtrent de doeleinden waarvoor men toegang wenst te verkrijgen tot de desbetreffende gegevens en van de gebruiker toestemming dient te hebben verkregen voor de desbetreffende handeling. Het vooraf informeren en verkrijgen van toestemming bij een onderzoek in een geautomatiseerd werk van iemand die verdacht wordt van een misdrijf als omschreven in artikel 67, eerste lid, Sv zou vanzelfsprekend onwenselijk zijn, omdat dit het onderzoek in gevaar zou brengen. Daarom wordt artikel 11.7a Tw buiten toepassing verklaard op handelingen ter uitvoering van een bevel van de officier van justitie.*"

Voor zover dat binnendringen in een geautomatiseerd werk *niet* heimelijk, dan wel *niet* op afstand plaatsvindt, laat de introductie van deze bepalingen in het Wetboek van Strafvordering andere of eventueel reeds bestaande bevoegdheden ongemoeid.[76]
Van 'binnendringen' is in ieder geval sprake wanneer de toegang tot het geautomatiseerde werk wordt verworven door het doorbreken van een beveiliging, door een technische ingreep, met behulp van valse signalen of een valse sleutel, of door het aannemen van een valse hoedanigheid.[77] Concreet kan het daarbij gaan om de toepassing van softwareapplicaties, maar ook om het eenvoudig inloggen op het geautomatiseerde werk met inloggegevens van de gebruiker die voorafgaand aan de toepassing van de bevoegdheid zijn verkregen door middel van bijvoorbeeld *social engineering* (ontfutselen).

Het technisch hulpmiddel

Onder een 'technisch hulpmiddel' waarmee na het binnendringen in het geautomatiseerde werk onderzoek kan worden verricht, wordt in dit verband verstaan: een softwareapplicatie die gegevens detecteert, registreert en transporteert en waarmee onderzoekshandelingen worden verricht ter uitvoering van een bevel.[78] De toepassing van een technisch hulpmiddel is niet altijd nodig voor het verrichten van onderzoekshandelingen in een geautomatiseerd werk. Onderzoekshandelingen kunnen ook ad hoc en handmatig worden verricht.[79]
Bij het begrip 'technisch hulpmiddel' zal hierna meer uitvoerig worden stilgestaan bij de bespreking van de nadere voorwaarden die aan het gebruik ervan worden gesteld. Over de precieze betekenis van het begrip 'technisch hulpmiddel' is in dit toezichtonderzoek veel te doen geweest.

De onderzoeksdoelen

Het onderzoek in een geautomatiseerd werk kan uitsluitend plaatsvinden met het oog op het verrichten van bepaalde onderzoekshandelingen.[80] De wet omschrijft telkens in lid 1 van de artikelen 126nba, 126uba en 126zpa Sv de volgende mogelijke onderzoeksdoelen:

a. de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of van de gebruiker, zoals de identiteit of locatie, en de vastlegging van die kenmerken.[81] Indien wordt opgetreden met dit onderzoeksdoel, wordt heimelijk toegang verkregen tot het geautomatiseerde werk teneinde informatie te vergaren die ten grondslag kan worden gelegd aan beslissingen over het verdere optreden rond het geautomatiseerde werk of de

---

[76] *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 53. Voorbeelden: art. 125i Sv (doorzoeking ter vastlegging van gegevens) biedt een wettelijke grondslag om bij een doorzoeking op een bepaalde locatie gegevens vast te leggen. Art. 125j Sv (netwerkzoeking) voorziet in de bevoegdheid om vanaf een plaats waar een doorzoeking ex 125i Sv plaatsvindt onderzoek te doen naar gegevens in een elders aanwezig geautomatiseerd werk, met dien verstande dat het onderzoek elders niet verder reikt dan voor zover de personen die plegen te werken of te verblijven op de plaats waar de doorzoeking plaatsvindt, vanaf die plaats, met toestemming van de rechthebbende tot het geautomatiseerde werk, daartoe toegang hebben. Art. 125m Sv opent de mogelijkheid om de notificatie van deze doorzoeking uit te stellen en de inzet daarmee (vooralsnog) geheim te houden. Art. 126l Sv (opnemen vertrouwelijke communicatie (OVC)) voorziet in de mogelijkheid om fysiek een 'technisch hulpmiddel' (een bug) te plaatsen dat heimelijk (maar niet op afstand) communicatie opneemt. Te wijzen valt bovendien op de bevoegdheden tot het vorderen van gegevens (artt. 126nc tot en met 126ni Sv) en op de mogelijkheid van het onderzoek van voorwerpen, met inbegrip van geautomatiseerde werken, waarin na de rechtmatige inbeslagneming ervan (art. 94 Sv) onderzoek kan worden verricht naar daarin opgeslagen gegevens.

[77] Voor de regeling rond het binnendringen van het geautomatiseerde werk is aangesloten bij de regeling van de computervredebreuk in het Wetboek van Strafrecht, art. 138ab lid 1 Sr. Zie *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 15.

[78] Zie art. 1 onder f Bogw.

[79] Zie de nota van toelichting op het Bogw, p. 16.

[80] Toegelicht in *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 19-28.

[81] Zie ook *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), paragraaf 2.3.1.

gebruiker daarvan, waaronder de hierna omschreven onderzoeksdoelen b tot en met e;[82]

b. de uitvoering van een bevel tot het opnemen van vertrouwelijke communicatie (ex artikel 126l dan wel 126s Sv),[83] of het aftappen en opnemen van telecommunicatie (ex artikel 126m dan wel 126t of 126zg Sv). Het onderzoek in een geautomatiseerd werk is in dat geval beperkt tot het uitvoeren van een dergelijk bevel tot aftappen of afluisteren en is niet gericht op andere gegevens die in het geautomatiseerde werk worden opgeslagen;[84]

c. de uitvoering van een bevel tot stelselmatige observatie (ex artikel 126g dan wel 126o of 126zd Sv), waarbij de officier van justitie kan bepalen dat ter uitvoering van het bevel een technisch hulpmiddel op een persoon wordt bevestigd (zie ook de artikelen 126g lid 3, 126o lid 3 en 126zd lid 4 Sv). Het onderzoek in een geautomatiseerd werk is in dat geval beperkt tot het gebruik van het geautomatiseerde werk ten behoeve van stelselmatige observatie. Het onderzoek strekt in dat geval tot het vergaren van gegevens omtrent de plaatsbepaling en niet tot de overige gegevens die in het geautomatiseerde werk worden opgeslagen.[85] Ook is het mogelijk een technisch hulpmiddel op een persoon te bevestigen in het kader van de stelselmatige observatie van een geautomatiseerd werk. Dit kan een technisch hulpmiddel betreffen dat reeds op de persoon aanwezig is (zoals een mobiele telefoon in de kleding) of dat op de persoon wordt bevestigd (zoals een peilzender in de kleding);[86]

d. de vastlegging van gegevens die in het geautomatiseerde werk zijn opgeslagen of die eerst na het tijdstip van afgifte van het bevel worden opgeslagen (de zogenaamde 'stromende gegevens'[87]), voor zover redelijkerwijs nodig om de waarheid aan de

---

[82] *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 19-20. Naast de hier genoemde overige onderzoeksdoelen worden door de minister nog genoemd de aanhouding van de verdachte en de inbeslagneming van voorwerpen waarvoor onderzoeksdoel a dienstig kan zijn. Als concreet voorbeeld van de inzet van onderzoeksdoel a wordt onder andere genoemd het binnendringen van een smartphone van een persoon die criminele contacten onderhoudt met een verdachte, om zijn identiteit vast te kunnen stellen.

[83] In art. 126zpa Sv (onderzoek bij terroristisch misdrijf) is in lid 1 onder b, anders dan bij de artt. 126nba en 126uba Sv, niet opgenomen het (equivalent van het) opnemen van vertrouwelijke communicatie (als bedoeld in art. 126zf Sv).

[84] Zie ook *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), paragraaf 2.3.4, p. 23-25. De inzet van deze bevoegdheden (de onderzoeksdoelen onder b) vereist een afzonderlijk bevel, op grond van de artikelen 126l, 126m, 126s, 126t of 126zg Sv.

[85] Zie ook *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), paragraaf 2.3.5. Als voorbeeld wordt genoemd het op afstand installeren van software op een smartphone waardoor de gps-functie kan worden geactiveerd. Vervolgens kunnen, bijvoorbeeld door een softwareapplicatie op de smartphone te installeren, de locatiegegevens via internet aan de ontvanger worden doorgegeven waardoor het mogelijk is een plaatsbepaling te doen (p. 26). Het verbod tot het betreden – ter uitvoering van een observatie – van een woning zonder toestemming van de rechthebbende geldt overigens onverminderd. Het permanent waarnemen van wat zich in een woning afspeelt via een op afstand geactiveerde webcam van bijvoorbeeld een smartphone of een laptop, moet als even ingrijpend worden aangemerkt als het betreden van een woning; dat is in het kader van de opsporing niet toegestaan. Zie *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 26-27, met verwijzing naar *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 71.

[86] *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 25-27. De inzet van deze bevoegdheid (de onderzoeksdoelen onder c) vereist een afzonderlijk bevel, op grond van de artikelen 126g, 126o of 126zd, eerste lid, onder a, Sv.

[87] Met 'stromende gegevens' wordt bedoeld: gegevens die in een proces zijn van verwerking of overdracht tussen geautomatiseerde werken, en dit in tegenstelling tot 'opgeslagen gegevens', waarmee wordt bedoeld: gegevens die op een gegevensdrager of opslagmedium worden bewaard. De term 'opgeslagen' brengt tot uitdrukking dat de (vaste) gegevens in het geautomatiseerde werk aanwezig zijn. Zie *Kamerstukken II* 1998/99, 26 671, nr. 3 (MvT), p. 3, en zie *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 19-20. Ter relativering valt aldaar te lezen (p. 19): "*Het onderscheid tussen de bevoegdheden met betrekking tot opgeslagen gegevens en stromende gegevens is in de praktijk echter aan het vervagen. Ook zijn de diensten van de verschillende aanbieders in elkaar over gaan lopen. Zo zijn er aanbieders van internetdiensten die opslagdiensten in de Cloud aanbieden (Google Docs, Dropbox, Skydrive). Webmaildiensten worden niet alleen gebruikt om berichten te versturen naar andere e-mailadressen maar ook voor interne communicatie binnen criminele groeperingen. Een bericht wordt dan in de concepten box geplaatst waarna verschillende personen op de dienst (Gmail of Hotmail) waarmee de inloggegevens worden gedeeld, kunnen inloggen en kennis kunnen nemen van de inhoud van het bericht zonder dat dit als e-mailbericht naar de ontvanger wordt verzonden.*"

dag te brengen.[88] Daarbij kan worden gedacht aan het vastleggen van afbeeldingen van kinderpornografie, inloggegevens van besloten *communities* of wachtwoorden waarmee de versleuteling van gegevens ongedaan kan worden gemaakt. De vast te leggen gegevens kunnen ook betrekking hebben op het internetgebruik van de gebruiker. Doordat met dit onderzoeksdoel het gehele geautomatiseerde werk kan worden doorzocht, is dit onderzoeksdoel aanzienlijk ruimer dan de vastlegging van gegevens onder onderzoeksdoel a.[89] Het aftappen of afluisteren van communicatie valt hieronder echter niet; dat betreft het onderzoeksdoel dat is omschreven onder b;[90]

e. de ontoegankelijkmaking van gegevens zoals bedoeld in artikel 126cc lid 5 Sv, met inbegrip van het (tijdelijk) verwijderen[91] daarvan.[92] Indien gegevens worden aangetroffen met betrekking tot welke of met behulp waarvan het strafbare feit is gepleegd, kan de officier van justitie bepalen dat deze gegevens ontoegankelijk worden gemaakt voor zover dit noodzakelijk is ter beëindiging van het strafbare feit of ter voorkoming van nieuwe strafbare feiten.[93] Volgens de minister kan hiermee bijvoorbeeld effectief worden opgetreden tegen zogeheten 'botnets', waarbij computers worden overgenomen door kwaadaardige software en zodoende ter beschikking komen van de beheerder van een botnet.[94] De ontoegankelijkmaking van gegevens betreft een voorlopige maatregel. Bij de einduitspraak over het strafbaar feit of bij afzonderlijke beschikking neemt de rechter een beslissing over de ontoegankelijk gemaakte gegevens (overeenkomstig de artikelen 354 en 552fa Sv).

Het onderzoek in een geautomatiseerd werk is beperkt tot de in lid 1 van de artikelen 126nba, 126uba en 126zpa Sv opgenomen onderzoeksdoelen. Deze doelen zijn dus limitatief

---

88 Zie o.a. *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 100: "*De informatietechnologie biedt de mogelijkheid om stromende gegevens op te slaan zonder dat er sprake is van communicatie. Daarvoor kan worden gedacht aan het uitwisselen van strafbare afbeeldingen, zoals kinderpornografie. Het is voor de criminaliteitsbestrijding van essentieel belang dat ook dergelijke gegevens kunnen worden vastgelegd ten behoeve van de waarheidsvinding. Daarbij geldt onverkort dat voor het opnemen van communicatie altijd een afzonderlijk bevel is vereist, op grond van de bevoegdheid tot het aftappen van communicatie of het direct afluisteren.*"

89 Zie *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), paragraaf 2.3.2: "*Met speciale software kan het internetgebruik van de verdachte worden gevolgd of met zijn emailverkeer worden meegekeken. Langs deze weg kunnen inlogcodes en wachtwoorden, die toegang geven tot versleutelde gegevens, worden verkregen. Voor het vastleggen van de gegevens kan gebruik worden gemaakt van een «keylogger»*, die de toetsaanslagen op een toetsenbord vastlegt."
Zie ook *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 15.

90 Zie o.a. *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 100.

91 Als de gegevens worden verwijderd, dan dienen zij te worden behouden ten behoeve van de strafvordering. In het kader van de ontoegankelijkmaking kunnen de gegevens dan ook niet worden gewist. Zodra het belang van de strafvordering zich niet meer verzet tegen opheffing van de maatregel bepaalt de officier van justitie dat de gegevens weer ter beschikking worden gesteld van de beheerder van het geautomatiseerde werk. Zie *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 44-45.

92 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), paragraaf 2.3.3. De definitie van 'ontoegankelijkmaking' laat ook de mogelijkheid van andere maatregelen open. Deze regeling sluit aan bij de regeling van de ontoegankelijkmaking van gegevens als bedoeld in art. 125o Sv. In iedere situatie zal moeten worden beoordeeld welke maatregel het meest effectief is, rekening houdend met de eisen van proportionaliteit en subsidiariteit. In de memorie van toelichting wordt daarvoor verwezen naar *Kamerstukken II* 1998/99, 26 671, nr. 3, p. 21. De officier van justitie bepaalt welke specifieke maatregelen worden getroffen om de gegevens ontoegankelijk te maken. Zie *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 44.

93 De bevoegdheid van het ontoegankelijk maken van gegevens laat zich op hoofdlijnen vergelijken met de bevoegdheid tot de inbeslagneming van een voorwerp met het oog op de onttrekking ervan aan het verkeer. Voor deze beide bevoegdheden geldt dat het gaat om een maatregel ter bescherming van de maatschappij. Zie *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 43.

94 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 21-22. Naar aanleiding van Kamervragen wordt overigens opgemerkt dat het toepassen van deze bevoegdheid voor het doen stoppen van een voertuig niet voor de hand ligt, vanwege het beperkte verband tussen de gegevens van een boordcomputer van een voertuig en het plegen van een strafbaar feit. Bovendien vormen de gegevens van een boordcomputer geen gegevens waarvan het bezit of de verspreiding minder wenselijk is vanuit het oogpunt van de bescherming van slachtoffers of van kwetsbare groepen in de samenleving. Zie *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 32.

omschreven.[95] De onderzoekshandelingen die in deze bepalingen van een wettelijke basis zijn voorzien betreffen enerzijds de toepassing van bestaande bevoegdheden zoals het aftappen van telecommunicatie en het direct afluisteren. In deze gevallen is het binnendringen voorwaardelijk om de reeds bestaande opsporingsbevoegdheid te kunnen uitoefenen. Het onderzoek in een geautomatiseerd werk betreft anderzijds nieuwe bevoegdheden, zoals het vastleggen of ontoegankelijk maken van gegevens.[96]

Gevallen waarin de methode is toegestaan

Indien het bevel het oog heeft op de onderzoeksdoelen die hierboven zijn genoemd onder a, b en c dient de verdenking een misdrijf te betreffen als omschreven in artikel 67 lid 1 Sv dat gezien zijn aard of samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert. Bij artikel 126uba Sv gaat het, zoals gezegd, om de verdenking dat in georganiseerd verband ernstige misdrijven beraamd of gepleegd worden en bij artikel 126zpa Sv om aanwijzingen van een terroristisch misdrijf.
Voor onderzoek dat strekt tot de hiervoor onder d en e omschreven doeleinden stellen de genoemde drie wetsbepalingen bovendien een strengere eis. Het onderzochte delict dient een misdrijf te betreffen waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaren of meer is gesteld, dan wel een misdrijf dat bij het Besluit onderzoek in een geautomatiseerd werk is aangewezen. De bij dit besluit aangewezen misdrijven betreffen misdrijven waarop weliswaar geen gevangenisstraf van acht jaar of meer is gesteld, maar die worden gepleegd met behulp van een geautomatiseerd werk en waarbij er een duidelijk maatschappelijk belang is bij de beëindiging van de strafbare situatie en de vervolging van de daders. Voorbeelden zijn het gebruik van een botnet (artikel 138ab lid 3 Sr), het aanbieden, verspreiden of bezitten van kinderpornografie (artikel 240b Sr), de verleiding van een minderjarige tot ontucht (artikel 248a Sr), grooming (artikel 248e Sr) en andere ernstige delicten waarbij het gebruik van een geautomatiseerd werk instrumenteel is en de inzet van deze bevoegdheid aangewezen is op basis van een afweging van belangen en met inachtneming van beginselen van proportionaliteit en subsidiariteit.[97]

Beginselen van proportionaliteit en subsidiariteit

Afgezien van de aard van de verdenking die wordt vereist, zijn de overige materiële voorwaarden voor toepassing van de bevoegdheid omschreven in de drie genoemde wetsbepalingen dezelfde. Dat zijn: (1) het misdrijf levert een 'ernstige inbreuk' op de rechtsorde op,[98] en (2) het onderzoek vordert het binnendringen van het geautomatiseerde werk 'dringend'.
Het laatstgenoemde vereiste van 'een dringend onderzoeksbelang' brengt tot uitdrukking dat de inzet van de bevoegdheid moet voldoen aan de vereisten van proportionaliteit en subsidiariteit, aldus de minister.[99] De inhoud van die eisen hangt af van de omstandigheden van het geval, zo vervolgt hij.

---

95 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 53. Zie bovendien de definitie van 'onderzoekshandeling' in art. 1 onder d Bogw: "*handeling van een opsporingsambtenaar van een technisch team met het oog op een doel als bedoeld in de artikelen 126nba, eerste lid, onder a tot en met e, 126uba, eerste lid, onder a tot en met e, en 126zpa, eerste lid, onder a tot en met e, van het Wetboek van Strafvordering ter uitvoering van een bevel*".

96 *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 30; vgl. *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 3, 6-7.

97 *Kamerstukken II* 2016/17, 34 372, nr. 3 (MvT), p. 30.

98 In art. 126uba lid 1 Sv is die eerste eis opgenomen door te verwijzen naar art. 126o lid 1 Sv (stelselmatige observatie bij georganiseerde criminaliteit). Die bepaling luidt volledig: "*Indien uit feiten of omstandigheden een redelijk vermoeden voortvloeit dat in georganiseerd verband misdrijven als omschreven in artikel 67, eerste lid, worden beraamd of gepleegd die gezien hun aard of de samenhang met andere misdrijven die in dat georganiseerd verband worden beraamd of gepleegd een ernstige inbreuk op de rechtsorde opleveren, kan de officier van justitie in het belang van het onderzoek bevelen dat een opsporingsambtenaar stelselmatig een persoon volgt of stelselmatig diens aanwezigheid of gedrag waarneemt.*"
In art. 126zpa Sv is niet met zoveel woorden de eis opgenomen dat het misdrijf een ernstige inbreuk op de rechtsorde oplevert. De aard van het misdrijf ter zake waarvan aanwijzingen bestaan, namelijk terroristisch, brengt de ernstige inbreuk op de rechtsorde vanzelf mee.

99 *Kamerstukken II* 2016/17, 34 372, nr. 3 (MvT), p. 29.

De hierna weergegeven beschrijving van de inhoud van deze eisen, toegespitst op de bevoegdheid tot het uitvoeren van onderzoek in een geautomatiseerd werk, volgt de wetsgeschiedenis. Daarbij zij aangetekend dat het onderscheid tussen het proportionaliteitsbeginsel en het subsidiariteitsbeginsel daarin niet altijd strikt is uitgewerkt.[100]
Het beginsel van proportionaliteit houdt in dat het belang dat wordt gediend met de bevoegdheid in verhouding moet staan tot de omvang van de beperking van de persoonlijke levenssfeer.
Voor de beoordeling van de omvang van deze beperking is ten eerste van belang dat de voorgestelde bevoegdheid een aanvulling vormt op de bestaande wettelijke bevoegdheden, aldus de minister.[101] Van belang is dus allereerst de vraag of de gezochte gegevens niet op een minder ingrijpende wijze kunnen worden verkregen. Afhankelijk van de omstandigheden van het geval kan de toepassing van een andere bevoegdheid minder ingrijpend zijn dan binnendringen van en het verrichten van onderzoekshandelingen in een geautomatiseerd werk.[102] Daarbij moet rekening worden gehouden met de gevolgen van de toepassing van de bevoegdheid voor het desbetreffende geautomatiseerde werk en de betrokken personen.[103] Daarbij kan ook het type van het geautomatiseerde werk van belang zijn; betreft het bijvoorbeeld een server van een bedrijf of een smartphone van een particulier?[104] De reden waarom niet met toepassing van een andere wettelijke opsporingsbevoegdheid kan worden volstaan, dient in het bevel te worden vermeld.
In de tweede plaats is de inzet van de bevoegdheid beperkt tot de doelen die in de artikelen 126nba lid 1, 126uba lid 1 en 126zpa lid 1 Sv limitatief zijn omschreven.[105]
In de derde plaats dient de bevoegdheid te worden toegepast in een zo beperkt mogelijk deel van een geautomatiseerd werk. Deze beperking moet in het bevel worden omschreven; zij waarborgt dat de overheid geen onbegrensde toegang heeft tot gegevens die zijn opgeslagen in een geautomatiseerd werk. Wanneer tijdens de toepassing van de bevoegdheid blijkt dat de bevoegdheid in een ander deel van het geautomatiseerde werk moet worden toegepast, dan is daarvoor een aangepast bevel en de uitdrukkelijke toestemming van de rechter-commissaris nodig.[106] Volgens de minister mag van de officier van justitie worden verwacht dat hij kenbaar kan maken in hoeverre gegevens van derden zijn betrokken bij het onderzoeken van het werk en op welke wijze de onderzoekshandelingen worden verricht opdat zoveel mogelijk[107] wordt voorkomen dat daarbij wordt kennisgenomen van gegevens die niet relevant of noodzakelijk zijn voor het onderzoek.[108]

---

100 Zie voor een uitwerking van deze beginselen (met voorbeelden) binnen het bestek van de opsporing: G.J.M. Corstens, *Het Nederlands strafprocesrecht*, bewerkt door M.J. Borgers en T. Kooijmans, Deventer: Wolters Kluwer 2021, p. 66: "*Van de strafrechtsfunctionarissen mag worden verlangd dat zij de in aanmerking komende belangen behoorlijk tegen elkaar afwegen. Dat houdt in dat op een voor de betrokkenen minst bezwarende wijze moet worden opgetreden (subsidiariteit) en dat er een redelijke verhouding moet zijn tussen die wijze van optreden en het beoogde doel (proportionaliteit). (...).*"

101 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 53.

102 Wanneer het gaat om cloudcomputingdiensten kan bijvoorbeeld een minder ingrijpende bevoegdheid voorhanden zijn, zoals het vorderen van gegevens bij de dienstverlener (art. 126nd Sv) of het vastleggen van gegevens tijdens een doorzoeking ter vastlegging van gegevens (art. 125i Sv of art. 125j Sv). De inzet van de bevoegdheid op een wijze die de bedrijfsvoering van een clouddienstverlener ernstig aantast zal niet snel als proportioneel en subsidiair worden goedgekeurd. Daarop zijn uiteraard uitzonderingen mogelijk. Zie *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 22.

103 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 30. Zie ook p. 79: "*De voorgestelde bevoegdheid dient als een laatste redmiddel, als andere opsporingsbevoegdheden tekort schieten.*" Zie daarnaast *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 10-11, 18-19 en 101.

104 *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 32.

105 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 53.

106 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 53-54.

107 Het is niet bij voorbaat uitgesloten dat bij het onderzoek in een geautomatiseerd werk dat bij de verdachte in gebruik is, ook gegevens van anderen in beeld komen. Zie *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 28. Voorkomen moet worden dat het tactische team de beschikking krijgt over deze bijvangst. De minister noemt o.a. het voorbeeld van mailverkeer. Wanneer in het bevel naar de correspondentie tussen de verdachte en een andere verdachte wordt gevraagd, zal het tactische team die gevraagde correspondentie verkrijgen, maar niet eventuele andere correspondentie vanuit hetzelfde emailadres. Zie *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 40.

108 *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 132 en 133.

Het beginsel van subsidiariteit houdt in dat het beoogde doel niet kan worden bereikt met een andere maatregel die minder ingrijpend is voor de persoonlijke levenssfeer. Hierover kan worden opgemerkt dat er geen andere opsporingsbevoegdheid is waarmee toegang kan worden gekregen tot gegevens die een vaste opslaglocatie ontberen, of waarmee het hoofd kan worden geboden aan de knelpunten in de opsporing die samenhangen met de toenemende mobiele toepassingen van internetgebruik en de versleuteling van gegevens (zie hieronder). De bevoegdheid draagt daarmee bij aan het vergaren van digitaal bewijs en het opsporen van strafbare feiten. Zoals hiervoor al is beschreven dient – naar het oordeel van de minister – in het bevel de reden te worden opgenomen waarom niet met toepassing van een andere wettelijke bevoegdheid kan worden volstaan. Daarmee wordt de rechter-commissaris in staat gesteld om deze voorwaarde te toetsen. De voorgestelde bevoegdheid voldoet daarmee aan het subsidiariteitsvereiste, aldus de minister.[109]

Tot slot komen in het kader van de proportionaliteits- en subsidiariteitstoets die de officier van justitie aanlegt ook de technische risico's aan de orde. Wat is het afbreukrisico van de operatie? Wat is de kans dat bij de operatie nevenschade ontstaat aan het geautomatiseerde werk? Het door een verdachte gebruikte geautomatiseerde werk zou immers een vitale functie kunnen vervullen binnen bijvoorbeeld een ziekenhuis, bank of cruciaal beveiligingssysteem.[110] Voor de inschatting van het risico is de deskundigheid van de gespecialiseerde opsporingsambtenaren van het technische team van groot belang. Zij beschikken bij uitstek over de technische expertise en dienen de officier van justitie in staat te stellen een afweging te maken. Net als bij andere afwegingen zal de officier van justitie daarom – voor de informatie op basis waarvan de afweging wordt gemaakt – steunen op de expertise van opsporingsambtenaren.[111]

De plaatsing in het wetboek en de daaruit voorvloeiende rechtswaarborgen

Vanwege de nauwe samenhang met de bestaande bevoegdheid van de doorzoeking ter vastlegging van gegevens, zoals geregeld in artikel 125i Sv, had de minister aanvankelijk voorgesteld de bevoegdheid in de zevende afdeling van titel IV ('Eenige bijzondere dwangmiddelen') van het eerste boek van het Wetboek van Strafvordering op te nemen. Na het advies van de afdeling advisering van de Raad van State (hierna wederom: de Afdeling) heeft de minister echter besloten dat de bevoegdheid van artikel 126nba moet worden geplaatst in titel IVa ('Bijzondere bevoegdheden tot opsporing') van het eerste boek van het Wetboek van Strafvordering, vanwege de omstandigheid dat deze bevoegdheid heimelijk wordt toegepast (dus zonder dat de betrokkene daarvan weet heeft), en omdat de bevoegdheid inhoudelijk overeenkomsten vertoont met de bijzondere opsporingsbevoegdheden van titel IVa van het eerste boek.[112] De plaatsing in deze titel van het Wetboek van Strafvordering impliceert dat de rechtswaarborgen waarop de Afdeling in haar advies heeft gewezen, ook van toepassing zijn op het onderzoek in een geautomatiseerd werk. Die waarborgen betreffen onder andere de notificatieplicht, de voeging van processen-verbaal bij de processtukken en de vernietiging van processen-verbaal of andere voorwerpen die het verschoningsrecht van functioneel verschoningsgerechtigden raken.[113] Op deze waarborgen zal hieronder dieper worden ingegaan.

De primaire uitgangspunten van de regeling van onderzoek in een geautomatiseerd werk

In het normatieve kader dat in dit hoofdstuk is omschreven is primair tot uitgangspunt genomen dat het door de officier van justitie bevolen onderzoek in een geautomatiseerd werk zodanig is omgeven met waarborgen en (mede daardoor) op een zodanige wijze wordt uitgevoerd dat

---

109 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 54.
110 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 32-33.
111 *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 61.
112 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 7 en p. 53.
113 Het voorgaande heeft betrekking op art. 126nba Sv. De artt. 126uba en 126zpa Sv zijn opgenomen in titel V, resp. titel Vb van het eerste boek van het Wetboek van Strafvordering. Ook op die titels zijn de bedoelde rechtswaarborgen mutatis mutandis van toepassing.

de betrouwbaarheid, de integriteit en de herleidbaarheid van de bij dit onderzoek verkregen gegevens is gegarandeerd. Dat is zowel in het belang van de verdachte als in het belang van de opsporing.[114] Die gegevens kunnen immers dienen tot het bewijs van het strafbare feit ter zake waarvan een verdenking is gerezen. Daarnaast had de minister oog voor het belang van afscherming van gevoelige methodieken en geavanceerde technologieën die bij het binnendringen en/of het verrichten van onderzoekshandelingen worden toegepast.

3.2. Omstandigheden die de introductie van de bevoegdheid rechtvaardigen

De toelichting van de minister

De introductie van de bevoegdheid tot onderzoek in een geautomatiseerd werk vult – naar het oordeel van de minister – een leemte in het assortiment van de voordien bestaande (digitale) opsporingsbevoegdheden.[115] De bevoegdheid is ingevoerd omdat volgens de minister de overige opsporingsbevoegdheden in toenemende mate tekortschieten om wezenlijke problemen en gebleken knelpunten op het gebied van de bestrijding van computercriminaliteit te adresseren. Zij schieten tekort omdat die overige opsporingsbevoegdheden ofwel zijn gekoppeld aan een bepaalde fysieke plaats ofwel niet zijn gericht op de toegang tot elektronische gegevens die zich in een geautomatiseerd werk of op een gegevensdrager elders bevinden.[116] Bij de geconstateerde wezenlijke problemen en knelpunten gaat het onder andere om de (toenemende mate van) versleuteling (encryptie) van elektronische gegevens (door criminelen),[117] het gebruik van draadloze netwerken[118] en cloudcomputingdiensten.[119] Deze ontwikkelingen brengen met zich dat met de bestaande wettelijke bevoegdheden het doel, namelijk het vergaren van gegevens die mogelijk als bewijs kunnen dienen, niet kan worden bereikt.

Versleuteling (encryptie)

Wat betreft de toenemende mate van versleuteling van elektronische gegevens, het eerste knelpunt, het volgende. Niet alleen opgeslagen gegevens kunnen worden versleuteld, zoals gegevens op een harde schijf, maar ook de communicatie (het transport van gegevens) via bijvoorbeeld het internet. Een goed voorbeeld van dat laatste betreft hetTor-netwerk.[120] De andere opsporingsbevoegdheden, zoals doorzoeking van een plaats ter vastlegging van gegevens of een decryptiebevel,[121] bieden volgens de minister in dat kader onvoldoende soelaas voor een

---

114 Zie onder meer: nota van toelichting op het Bogw, p. 21, p. 38; *Kamerstukken I* 2017/18, 34 372, G (NMvA I), p. 14, p. 15; *Kamerstukken II* 2018/19, 34 372, nr. 29 (verslag van een schriftelijk overleg), p. 7, p. 12, p. 13.

115 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 16.

116 Vgl. *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 1-4.

117 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 7-10.

118 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 10-11.

119 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 11 e.v. Vgl. *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 18-19.

120 'Tor' is de afkorting van: *The Onion Router*. Dit betreft een wereldwijd netwerk van verschillende door vrijwilligers aangeboden computers (*onion servers* of *nodes*) die fungeren als tussenstation waarlangs de communicatie – bij iedere stap versleuteld – verloopt. In ieder tussenstation bevindt zich in onversleutelde vorm uitsluitend de routinginformatie van de voorafgaande en de volgende server. Daardoor is het tijdens het communicatietraject niet goed mogelijk om de oorsprong en de eindbestemming van het bericht te achterhalen. Zie ook *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 7-8.

121 De minister noemt de volgende bevoegdheden: doorzoeking van een plaats ter vastlegging van gegevens die op deze plaats op een gegevensdrager zijn vastgelegd (art. 125i Sv), een bevel tot ontsleuteling gericht tot degene die kennis draagt van de wijze van versleuteling van de gegevens (art. 125k lid 2 Sv), een decryptiebevel (dat niet aan de verdachte kan worden gericht, art. 125k lid 3 Sv), een vordering gegevens te verstrekken gericht tot de aanbieder van een dienst voor de opslag van gegevens (art. 126ng lid 2 Sv), een verzoek tot afgeven van gegevens aan een aanbieder in het buitenland (art. 32 onder b van het Cybercrimeverdrag), verzoeken om rechtshulp (waarbij alleen opgeslagen en niet-stromende gegevens kunnen worden gevraagd), het aftappen en opnemen van communicatie door middel van een telefoon-, e-mail-, of internettap (artt. 126m, 126t en 126zg Sv), het vorderen van opgeslagen communicatie van de aanbieder (art. 126ng Sv), het bevelen medewerking te verlenen aan het ontsleutelen van gegevens aan degene van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van versleuteling van de gegevens (artt. 126m lid 1 en 126nh lid 1 Sv). Zie *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 8-9.

effectieve opsporing. De minister heeft laten weten dat de opsporing dringend behoefte heeft aan de mogelijkheid om communicatie te onderscheppen *voor*dat deze wordt versleuteld of *na*dat deze is ontsleuteld.[122] Met de nu gecreëerde bevoegdheid kan de communicatie worden afgetapt en opgenomen op het geautomatiseerde werk hetzij *voor*dat de te communiceren gegevens op het geautomatiseerde werk van de verzender worden versleuteld en verzonden, hetzij *na*dat deze op het geautomatiseerde werk van de ontvanger zijn binnengekomen en door de software zijn ontsleuteld. Daardoor verschuift de oriëntatie van het aftappen van de verbinding waarover de communicatie tussen de deelnemers verloopt, naar het aftappen van de bron of de bestemming van de communicatie, te weten de computers of de mobiele telefoons met behulp waarvan de gegevens worden verzonden of ontvangen. In dat verband wordt wel gesproken van 'aftappen op het apparaat'.[123, 124]

Draadloze netwerken

Het tweede knelpunt betreft het toenemende gebruik van draadloze netwerken. Doordat personen (kunnen) gebruikmaken van verschillende toegangspunten tot het internet wordt het aftappen van de volledige communicatie van een betrokkene vrijwel onmogelijk. Indien toch

---

[122] *Handelingen I* 2017/18, nr. 34, item 5, p. 14: "*(…). Ik noem een praktijkvoorbeeld: een criminele groepering communiceert via een afgeschermd netwerk van mobiele telefoons. De communicatie is goed versleuteld, dus aftappen is niet effectief. Alleen door binnen te dringen in één van de telefoons zelf, kan de communicatie in niet-versleutelde vorm worden ingezien of uitgelezen.*" Zie meer uitgebreid *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 2-4.

[123] *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 9-10, p. 23-25.

[124] De stelling dat de opsporing dringend behoefte heeft aan de mogelijkheid om communicatie te onderscheppen voordat deze wordt versleuteld of nadat deze is ontsleuteld, is in de uitvoeringspraktijk geïllustreerd door de wijze waarop de politie in Nederland en in het buitenland erin is geslaagd om kennis te nemen van de inhoud van versleuteld berichtenverkeer dat verliep over cryptotelefoons of via crypto-applicaties van leveranciers als PGP Safe, Ennetcom, MPC en IronChat. Zo is vanaf servers die waren opgesteld in Costa Rica, respectievelijk Canada de inhoud veiliggesteld van berichten die werden verzonden met behulp van speciaal daartoe vervaardigde PGP-beveiligde BlackBerry's en Androidtelefoons die waren ontdaan van onveilige functionaliteiten, en die aan de gebruikers waren geleverd door PGP Safe, respectievelijk Ennetcom. Zodoende is de politie bekend geworden met (naar verluidt) 3,7 miljoen berichten die door criminelen die zich met behulp van deze cryptotelefoons onbespied waanden naar elkaar waren verstuurd.
Zie over het gebruik van dergelijke Ennetcom-berichten tot het bewijs o.m.: rechtbank Midden-Nederland 29 maart 2021, ECLI:NL:RBMNE:2021:1213; rechtbank Amsterdam 21 mei 2021, ECLI:NL:RBAMS:2021:2732; rechtbank Noord-Holland 19 januari 2022, ECLI:NL:RBNHO:2022:315; gerechtshof Arnhem-Leeuwarden 3 maart 2021, ECLI:NL:GHARL:2021:1917; gerechtshof Arnhem-Leeuwarden 23 december 2021, ECLI:NL:GHARL:2021:11610; gerechtshof Arnhem-Leeuwarden 23 december 2021, ECLI:NL:GHARL:2021:11625; de conclusie van A-G Harteveld van 8 maart 2022, ECLI:NL:PHR:2022:219, en zie HR 28 juni 2022, ECLI:NL:HR:2022:900.
In het gat in de markt dat na het ontmantelen van Ennetcom in 2016 en PGP Safe in 2017 ontstond, stapte een nieuwe leverancier van cryptotelefoons, EncroChat. In juli en in oktober 2020 maakten justitie en politie veruit de grootste vangst aan (crimineel) berichtenverkeer ooit bekend. In samenwerking met de Franse politie, Europol en Eurojust was in operatie 'Lemont' de inhoud achterhaald van ongeveer 20 miljoen berichten die OTR-beveiligd waren verzonden met de cryptotelefoons van EncroChat, terwijl gedurende enkele maanden berichtenverkeer live kon worden meegelezen.
Zie over het gebruik van EncroChat-berichten tot het bewijs: rechtbank Limburg 26 januari 2022, ECLI:NL:RBLIM:2022:558 en ECLI:NL:RBLIM:2022:571; rechtbank Gelderland 8 december 2021, ECLI:NL:RBGEL:2021:6584, en de tussenbeslissingen van rechtbank Amsterdam van 8 juli 2021, ECLI:NL:RBAMS:2021:3524, gerechtshof Arnhem-Leeuwarden van 24 februari 2022, ECLI:NL:GHARL:2022:1741, en rechtbank Oost-Brabant van 10 maart 2022, ECLI:NL:RBOBR:2022:856.
Inmiddels is het succes van de ontmanteling van EncroChat overtroffen door de buitenbedrijfstelling op 9 maart 2021 van Sky Global, de wereldwijde provider van Sky ECC, een applicatie voor cryptocommunicatie met gebruikmaking van *elliptic curve cryptography* (ECC). Daarbij waren ongeveer 70 duizend klanten aangesloten (waarvan elfduizend actief in Nederland). Binnen het bestek van een politieoperatie ('Argus') zijn ongeveer 80 miljoen berichten onderschept en werd het door deze provider gefaciliteerde berichtenverkeer een kleine maand live meegelezen.
Voor zover bekend is het in geen van deze hier genoemde gevallen mogelijk gebleken om het cryptografisch algoritme, bijvoorbeeld (maar niet uitsluitend) *pretty good privacy* (PGP), zelf te kraken. De onderschepping en het leesbaar maken van berichtenverkeer vond op andere wijze plaats, namelijk vóór encryptie of ná decryptie, of met behulp van veiliggestelde (cryptografische) geheime sleutels.
Vermeldenswaard is ten slotte de onthulling op 8 juni 2021 van operatie 'Trojan Shield'. In dat kader bracht de FBI zelf heimelijk een onkraakbaar geachte applicatie voor cryptocommunicatie, Anom, op de markt. Daarop stapten voormalige gebruikers van Sky ECC, na het opdoeken ervan, massaal over. In samenwerking met andere politiediensten werd het berichtenverkeer live meegelezen. Hierbij werden 27 miljoen berichten bemachtigd afkomstig van twaalfduizend cryptotoestellen. (De informatie in deze voetnoot is louter ter illustratie en is uitsluitend afkomstig uit openbare bronnen, niet van het OM).

wordt gekozen voor bijvoorbeeld een tap op een router, betekent dit dat zonder onderscheid ook de gegevens worden getapt van personen die gebruikmaken van dezelfde router en voor wie de politie geen professionele belangstelling heeft. Dat is niet proportioneel, aldus de minister. Bovendien biedt een internettap geen soelaas als de gegevens zijn versleuteld. Met de invoering van de artikelen 126nba/uba/zpa Sv wordt voor dit knelpunt een oplossing geboden. Met de in deze bepalingen toegekende bevoegdheid kan een geautomatiseerd werk worden binnengedrongen met het oog op de identificatie van een geautomatiseerd werk of van de gebruiker. Op basis van de identificerende gegevens kan dan, meer gericht, een geautomatiseerd werk worden onderzocht.[125]

Cloud computing

Het derde knelpunt betreft cloudcomputingdiensten.[126]Tegenwoordig worden gegevens door particulieren en bedrijven niet altijd meer op de harde schijf van een computer in het eigen netwerk opgeslagen, maar wordt in toenemende mate gebruikgemaakt van zogenaamde cloudcomputingdiensten. Voorbeelden zijn *Hotmail*, *Dropbox*, *Googledocs* en *Mega*. De gegevens worden langs geautomatiseerde weg door de aanbieder van de desbetreffende dienst op verschillende servers opgeslagen elders in Nederland of in het buitenland, zonder dat de gebruiker daarop invloed heeft. De locatie van de servers en de daarop bewaarde gegevens zijn soms ook voor de aanbieder niet te achterhalen.[127] De ervaring leert volgens de minister dat de aanbieder van dergelijke webdiensten veelal is gevestigd in een land waarmee Nederland niet of nauwelijks een rechtshulprelatie onderhoudt. Anonimisering en afscherming van gegevens voor politie en justitie vormen essentiële elementen van het bedrijfsmodel van deze aanbieders. De opsporing heeft behoefte aan de mogelijkheid om heimelijk toegang te verkrijgen tot gegevens die in de cloud zijn opgeslagen, zonder dat de verdachte of de aanbieder daarbij worden betrokken.[128]

Samenvatting

De opsporingsbevoegdheden die zijn gericht op het vastleggen van elektronische gegevens of het aftappen en opnemen van communicatie voldoen volgens de minister niet langer omdat in toenemende mate gebruik wordt gemaakt van versleuteling, omdat de geautomatiseerde werken onderdeel vormen van een netwerk of omdat de gegevens worden opgeslagen in de cloud. Tegelijkertijd zijn volgens de minister zwaarwegende bezwaren verbonden aan het alternatief waarin andere bestaande opsporingsbevoegdheden worden ingezet. Deze worden thans geschetst.[129]

De afweging van de nadelen van de alternatieven voor onderzoek in een geautomatiseerd werk

Voor het opnemen van vertrouwelijke communicatie op basis van de bevoegdheden die in de artikelen 126l, 126s en 126zf Sv zijn opgenomen kan het noodzakelijk zijn om fysiek toegang

---

125 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 10-11.

126 *Cloud computing*, ook wel: clouddiensten of cloudcomputingdiensten, is het op aanvraag beschikbaar stellen van opslagcapaciteit voor gegevens en computerapplicaties via internet. Het beheer van de gegevens en applicaties wordt in dat geval door de afnemer van deze diensten uitbesteed aan de dienstverlener. Daarbij worden de gegevens en applicaties – geautomatiseerd, en (dus) meestal zonder regie over de precieze locatie – verspreid over verschillende servers van de dienstverlener en op verschillende geografische locaties opgeslagen. Voor de afnemer van deze diensten zijn de door hem opgeslagen gegevens toegankelijk via internet, zonder dat voor hem kenbaar is op welke locaties de gegevens en applicaties zich bevinden. Zie hierover het volgende rapport: B.J. Koops, R. Leenes, P. De Hert & S. Olislaegers, *Misdaad en opsporing in de wolken. Knelpunten en kansen van cloud computing voor de Nederlandse opsporing,* Tilburg/Den Haag: TILT/ WODC, oktober 2012, en zie bijvoorbeeld: J.W. van den Hurk & S.J. de Vries, 'Waar worden gegevens in de 'cloud' opgeslagen en welke juridische consequentie heeft het antwoord op die vraag? Een speurtocht langs het traditionele juridisch kader en actuele wetgeving en jurisprudentie leidt tot een opmerkelijke conclusie', *Strafblad* 2019, afl. 4, p. 34-44.

127 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 11. Zie ook *Kamerstukken I* 2016/17, 34 372, D (MvA I), p. 13.

128 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 12.

129 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 12.

te krijgen tot een kantoor of een woning, namelijk om aldaar een bug[130] te plaatsen. Bij de uitvoering van onderzoek in een geautomatiseerd werk, dat een wettelijke basis geeft om het een en ander heimelijk en op afstand te doen, is het niet nodig een woning te betreden om zo'n bug te plaatsen, zodat er geen inbreuk hoeft te worden gemaakt op het grondwettelijk beschermde recht van onschendbaarheid van de woning (artikel 12 Grondwet).[131]
Tegelijkertijd biedt de inzet van andere opsporingsbevoegdheden dan de bevoegdheden die zien op het vergaren of vorderen van gegevens, zoals de observatie (artikelen 126g, 126o en 126zd lid 1, onderdeel a, Sv), het stelselmatig inwinnen van informatie (artikelen 126j, 126qa en 126zd lid 1, onderdeel c, Sv) of de inkijkoperatie (artikelen 126k, 126r en 126zd lid 1, onderdeel d, Sv) ook onvoldoende soelaas voor de opsporing. De inzet van deze bevoegdheden is namelijk niet gericht op de toegang tot gegevens die langs elektronische weg worden verwerkt en biedt dan ook weinig kans op kennisneming van de inhoud van de gegevens die de verdachte heeft ontvangen of verzonden, of van de communicatie waarbij hij is betrokken.[132]
Tot slot bestaat er op basis van andere wettelijke bevoegdheden de mogelijkheid een geautomatiseerd werk in beslag te nemen en daaraan onderzoek te verrichten, zodat van de daarin bewaarde gegevens kan worden kennisgenomen (artikelen 95, 96, 96c, 97, 98 en 99 Sv).[133] Een belangrijk bezwaar van inbeslagneming is echter dat de verdachte hierdoor kan vernemen dat politie en justitie in hem zijn geïnteresseerd en dat zij kunnen beschikken over alle gegevens die op het geautomatiseerde werk of de gegevensdrager zijn opgeslagen. Het kennisnemen van een grote hoeveelheid persoonsgegevens met het oog op het selecteren van voor de opsporing relevante gegevens zal volgens de minister voorts veelal als disproportioneel moeten worden aangemerkt in gevallen waarin een voorwerp uitsluitend in beslag wordt genomen om bepaalde gegevens te verkrijgen.[134]

Nogmaals de maatstaven van proportionaliteit en subsidiariteit

De bespreking van de bovenstaande knelpunten en bezwaren in de wetsgeschiedenis vormt niet alleen een onderbouwing van de noodzaak van de invoering van de bevoegdheid tot het uitvoeren van onderzoek in een geautomatiseerd werk. De bespreking verschaft tevens een uitwerking van de maatstaven van proportionaliteit en subsidiariteit die gelden bij de oordeelsvorming omtrent de toepassing van de bevoegdheid. Zo kan uit die bespreking worden opgemaakt dat uit het oogpunt van proportionaliteit en subsidiariteit in het ene geval één van de andere opsporingsbevoegdheden de voorkeur geniet, terwijl in een ander geval de voorkeur uitgaat naar binnendringen in het geautomatiseerde werk. Het tappen van een router heeft bijvoorbeeld als nadeel dat noodzakelijkerwijze ook de communicatie van niet-betrokken derden wordt onderschept. Het heimelijk en op afstand plaatsen van een bug[135] ten behoeve van het opnemen van vertrouwelijke communicatie kan de voorkeur hebben boven het fysieke betreden van een woning.

---

130 Een 'bug' betreft in dit verband een kleine draadloze microfoon die op een locatie kan worden verborgen met het oog op het heimelijk opnemen van vertrouwelijke communicatie (OVC).
131 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 12-13.
132 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 13.
133 Dat de content van de opslagmedia waarmee een geautomatiseerd werk is uitgerust na inbeslagneming voor de politie voor kennisneming beschikbaar komt is overigens allerminst gegarandeerd. Na inbeslagneming van het geautomatiseerde werk moet vervolgens nog toegang worden verkregen tot de opgeslagen gegevens door de eventuele beveiliging ervan te doorbreken of te omzeilen. Afhankelijk van de kwaliteit van de beveiliging vergt dat de medewerking van de gebruiker of de toepassing van een list.
134 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 13, met verwijzing naar *Kamerstukken II* 1998/99, 26 671, nr. 3, p. 19.
135 In dit geval gaat het bij een 'bug' om het heimelijk activeren van de microfoon van een computer, laptop, tablet of mobiele telefoon, waarmee vervolgens omgevingsgeluiden (eventueel gesprekken) kunnen worden opgevangen.

3.3. De procedure en de daaraan gestelde eisen

De besluitvorming

De besluitvorming over de uitvoering van onderzoek in een geautomatiseerd werk vangt aan met een projectvoorstel (een proces-verbaal van aanvraag) dat afkomstig is van een tactisch (recherche)team en is gericht aan de officier van justitie.[136] Daarin wordt voorgesteld om de bevoegdheid in te zetten in het opsporingsonderzoek dat het tactische team in een bepaalde zaak verricht. Het projectplan bevat onder meer een beschrijving van de verdachte, de verdenking, de noodzaak om de onderzoeksbevoegdheid toe te passen en de gewenste resultaten ervan.

Vervolgens vraagt de officier van justitie het technische team om advies over de haalbaarheid van het onderzoek. Daartoe stelt het technische team op basis van de intakegegevens en overige relevante gegevens een rapport haalbaarheidsonderzoek op.[137] Het rapport bevat de te bereiken doelen, de beschikbare technieken en middelen (capaciteit en kennis), de mogelijke alternatieve middelen en de risico's die aan de inzet zijn verbonden. Wat betreft de risico's moet worden gedacht aan elementen als: de mate van inbreuk op de persoonlijke levenssfeer van de verdachte(n), de eventuele gevolgen voor de kwetsbaarheid van het systeem waarin de bevoegdheid zou moeten worden toegepast, de kans op ontdekking van de inzet van de software door de betrokkene, de kosten van de inzet en de kans op nadeel of schade bij derden.[138] In het rapport wordt onder meer opgenomen welke bevelen nodig zijn, alsmede of en zo ja welke software van derden moet worden aangeschaft. Bovendien wordt in het rapport een plan van aanpak voor de uitvoering van een onderzoek in het geautomatiseerde werk uitgewerkt.[139]

Op basis van deze informatie maakt de officier van justitie zijn afwegingen. De officier van justitie weegt daarbij de noodzaak van de toepassing van de bevoegdheid zorgvuldig af tegen de inbreuk die deze toepassing maakt op de persoonlijke levenssfeer van de verdachte of van derden, de risico's voor het geautomatiseerde werk en de afbreukrisico's van de operatie.[140]

De officier van justitie gebruikt het rapport haalbaarheidsonderzoek vervolgens voor het verkrijgen van toestemming voor de inzet van de opsporingsbevoegdheid binnen de organisatie van het OM, namelijk van het College van procureurs-generaal.[141] Daartoe moet de voorgenomen toepassing van de bevoegdheid eerst door de (hoofd)officier van

---

136 Nota van toelichting op het Bogw, onder 3.1.2, p. 14 e.v.

137 *Kamerstukken II* 2018/19, 34 372, nr. 29 (verslag van een schriftelijk overleg), p. 10: "*Het (…) rapport haalbaarheidsonderzoek wordt ter voorbereiding van het bevel opgesteld door het technische team, op basis van de intakegegevens en overige relevante gegevens. Hierin wordt het plan van aanpak voor de uitvoering van een onderzoek in het geautomatiseerde werk uitgewerkt. In het rapport wordt onder meer opgenomen welke bevelen nodig zijn, of en zo ja welke software van derden moet worden aangeschaft. Binnen dit haalbaarheidsonderzoek wordt de effectiviteit van de beschikbare middelen afgewogen. In een specifieke zaak is het bijvoorbeeld mogelijk dat social engineering wordt afgewogen, maar de effectiviteit ervan negatief wordt beoordeeld, alsook andere alternatieve middelen en over wordt gegaan tot het adviseren van de aanschaf van een licentie van binnendringsoftware. Een negatieve beoordeling kan voortkomen uit het feit dat de kans van slagen nihil is of dat de inzet onaanvaardbare grote risico's meebrengt voor het opsporingsonderzoek.*" Zie ook de nota van toelichting op het Bogw, p. 16 en p. 44.

138 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 33.

139 Het plan van aanpak voor de uitvoering van een onderzoek in het geautomatiseerde werk, dat onderdeel is van het rapport haalbaarheidsonderzoek en dat mede dient voor de aanvraag van een bevel ex art. 126nba/uba/zpa Sv, moet worden onderscheiden van het plan van aanpak voor het binnendringen in het geautomatiseerde werk, dat door het technische team wordt opgesteld nádat een bevel ex art. 126nba/uba/zpa Sv is afgegeven en dat onderdeel is van de verkennende fase.

140 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 33-34. Zie ook *Kamerstukken II* 2018/19, 34 372, nr. 29 (verslag van een schriftelijk overleg), p. 10; *Kamerstukken I* 2018/19, 34 372, L (verslag van een schriftelijk overleg), p. 8-9.

141 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 37 e.v.

justitie aan de Centrale toetsingscommissie (CTC)[142] voor advies worden voorgelegd.[143] Het advies van de CTC wordt vervolgens door tussenkomst van de PG-portefeuillehouder aan het College van procureurs-generaal overgebracht.[144] Het College van procureurs-generaal beslist daarna over de voorgenomen toepassing.[145]
Er is tevens voorzien in een spoedprocedure. De CTC toetst de zaak dan zo spoedig mogelijk en legt haar (mondelinge) advies voor aan (een lid) van het College van procureurs-generaal. Hierop kan het College een (mondelinge) beslissing nemen.[146]
Pas nadat binnen het OM toestemming is verkregen, benadert de officier van justitie de rechter-commissaris voor het vorderen van een machtiging tot het bevelen van binnendringen en het verrichten van onderzoekshandelingen in een geautomatiseerd werk. Ook hiertoe maakt de officier van justitie gebruik van het door het technische team opgestelde rapport haalbaarheidsonderzoek. Bij de aanvraag van een machtiging wordt informatie verstrekt aan de rechter-commissaris over de beoogde functionaliteiten van het technisch hulpmiddel.[147]

De nadere toelichting van de minister op het onderwerp van de besluitvorming

Volgens de minister is administratieve voorbereiding van de bevoegdheidsuitoefening van essentieel belang voor een afgewogen en zorgvuldige oordeelsvorming in het kader van een strafzaak en voor een transparant strafproces.[148] De inzet van de bevoegdheid wordt getoetst aan de wet- en regelgeving, de jurisprudentie, de proportionaliteit en subsidiariteit en de afbreukrisico's. Daarnaast worden de effectiviteit van de bevoegdheid en het afbreukrisico afgewogen tegen het belang van de uitoefening van de bevoegdheid in het concrete geval.[149]
Bij deze toets en afweging is het nodig dat het geautomatiseerde werk in voldoende mate identificeerbaar is, zodat de reikwijdte van de toepassing van de bevoegdheid voldoende kan worden begrensd.
De risico's van de inzet worden voorafgaand mondeling besproken met de officier van justitie in het zogenaamde juridisch-operationeel overleg. Deelnemers aan het overleg zijn de officier van justitie, de teamleider, een jurist van het technische team en een technisch opsporingsambtenaar. Tijdens het overleg wordt mondeling uitleg gegeven over eventueel gevaarzettende situaties. Tot slot zal tijdens de inzet voortdurend overleg worden gevoerd.[150]

3.4. Het bevel en de daaraan te stellen eisen

Het bevel

Het bevel tot het uitvoeren van onderzoek in een geautomatiseerd werk moet voldoen aan de eisen zoals genoemd in lid 2 van de artikelen 126nba, 126uba en 126zpa Sv. Deze eisen komen voor een groot deel overeen met de eisen die worden gesteld aan het bevel tot toepassing van andere bijzondere opsporingsbevoegdheden dan die van onderzoek in een geautomatiseerd werk.

---

142 De CTC, samengesteld uit leden van het OM en de Nationale politie, is een intern adviesorgaan van het OM dat het College van procureurs-generaal adviseert omtrent de voorgenomen inzet van bepaalde bijzondere opsporingsbevoegdheden en methodieken. Zie de Aanwijzing opsporingsbevoegdheden, 2014A009, van het College van procureurs-generaal, *Stcrt.* 2014, 24442, paragraaf 5.1.

143 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 38. De Aanwijzing opsporingsbevoegdheden, waarin is geregeld welke (bijzondere) opsporingsbevoegdheden aan de CTC dienen te worden voorgelegd, moet daarvoor (nog) worden aangepast.

144 *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 86.

145 Zie de Aanwijzing opsporingsbevoegdheden, 2014A009, van het College van procureurs-generaal, *Stcrt.* 2014, 24442.

146 *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 86.

147 Nota van toelichting op het Bogw, p. 44.

148 *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 54.

149 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 37-38.

150 *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 68-69.

Het bevel wordt gegeven voor een periode van ten hoogste vier weken. Het bevel kan slechts worden gegeven na schriftelijke machtiging op vordering van de officier van justitie te verlenen door de rechter-commissaris. De machtiging vermeldt de onderdelen van het bevel en de periode waarvoor de machtiging van kracht is.
Doel van de eisen van lid 2 van artikel 126nba, 126uba en 126zpa Sv is om de rechter-commissaris afdoende in staat te stellen tot toetsing van de proportionaliteit en subsidiariteit van de uitoefening van de bevoegdheid.[151] Daarbij is essentieel dat de rechter-commissaris zich op basis van de gegeven omschrijving van het geautomatiseerde werk een goed beeld kan vormen van de reikwijdte van het binnendringen en dat hij kan beoordelen in hoeverre dit door de omstandigheden wordt gerechtvaardigd.[152]

De eisen houden in dat het bevel schriftelijk is en het volgende vermeldt:

a. het misdrijf en indien bekend de naam of anders een zo nauwkeurig mogelijke aanduiding van de verdachte;
b. zo mogelijk een nummer of een andere aanduiding waarmee het geautomatiseerde werk kan worden geïdentificeerd en, indien dit aan de orde is, de mededeling dat de gegevens niet in Nederland zijn opgeslagen of dat de locatie niet bekend is. Als aanduiding waarmee het geautomatiseerde werk kan worden geïdentificeerd gelden bijvoorbeeld het IP-adres,[153] het MAC-adres,[154] het IMEI-nummer, de *hardware ID* of de *User Agent*;[155]
c. de feiten of omstandigheden waaruit blijkt dat de voorwaarden, bedoeld in lid 1 van de artikelen 126nba, 126uba en 126zpa Sv, zijn vervuld;
d. een aanduiding van de aard en functionaliteit van het technisch hulpmiddel, bedoeld in lid 1, dat wordt gebruikt voor de uitvoering van het bevel.[156] Bij functionaliteiten kan in dit verband worden gedacht aan bijvoorbeeld het opnemen van geluid, het maken van schermafbeeldingen (screenshots), het vastleggen van toetsaanslagen (keylogging) of het doorzoeken van bepaalde bestandsmappen en het vastleggen van gegevens hieruit;[157]
e. het onderzoeksdoel of -doelen, genoemd in lid 1, met het oog waarop het bevel wordt gegeven en, als dit het onderzoeksdoel a, d of e betreft, een duidelijke omschrijving van de te verrichten handelingen.[158] Deze onderzoekshandelingen kunnen handmatig worden verricht, dan wel met behulp van een technisch hulpmiddel in de vorm van een softwareapplicatie. Daarbij kan het bijvoorbeeld gaan om het doorzoeken van bepaalde bestandsmappen en het vastleggen van gegevens hieruit (onderzoeksdoel d).[159] Indien het verrichten van onderzoekshandelingen plaatsvindt zonder een technisch hulpmiddel worden de onderzoekshandelingen die zullen worden verricht omschreven in het bevel;[160]
f. ten aanzien van welk deel van het geautomatiseerde werk en welke categorie van gegevens aan het bevel uitvoering wordt gegeven. Dit vereist onder meer een

---

151 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 30.
152 *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 13.
153 Daaraan is wel een waarschuwing verbonden. Zie *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 33: "*Voordat een geautomatiseerd werk wordt binnengedrongen kan de geografische locatie daarvan op verschillende manieren worden vastgesteld, bijvoorbeeld door het nagaan van de gegevens van een IP-adres in de database van beheerders als de Internet Cooperation for Assigned Names and Numbers (ICANN). Bij cybercrime is een correcte vermelding van een IP-adres in deze database echter geen vanzelfsprekendheid. Criminelen maken gebruik van diverse technieken om de feitelijke locatie van de gegevens of de identiteit en de locatie van het geautomatiseerd werk en zijn beheerder te verhullen* [Opmerking onderzoekers: bijvoorbeeld door het gebruik van de internetapplicatie Tor of van een *virtual private network* (VPN)]. *Soms kan technisch onderzoek uitkomst bieden, bijvoorbeeld door het benutten van zwakheden in de verhullingstechniek of het deconstrueren van de virtualisatieschakels bij dynamische IP-adressen. Aldus kan een virtueel dwaalspoor worden ontrafeld.*"
154 Een MAC-adres betreft een uniek nummer dat is verbonden aan de hardware, zodat deze kan worden geïdentificeerd.
155 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 20 en 30.
156 Zodat kan worden gecontroleerd of deze voorziening aan de eisen voldoet. Zie *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 30.
157 Nota van toelichting op het Bogw, p. 37.
158 Zie ook *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 102.
159 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 35.
160 Nota van toelichting op het Bogw, p. 16.

aanduiding van de aard van het geautomatiseerde werk, bijvoorbeeld een pc, een server of een smartphone.[161] Een smartphone kan worden aangeduid met het MAC-adres en een server door middel van een IP-adres dat de verbinding vormt tussen het geautomatiseerde werk en het internet.[162] Bij 'categorie van gegevens' moet worden gedacht aan de aard van de gegevens, bijvoorbeeld gegevens van een e-mailbox of van een harde schijf, msn-berichten of Skype-communicatie,[163] en aan het onderscheid tussen enerzijds opgeslagen gegevens en anderzijds stromende gegevens.[164] Een ander voorbeeld: bij de bestrijding van een botnet gaat het alleen om de gegevens op de server die van belang zijn voor de bestrijding van een botnet en niet om de (persoonlijke) gegevens van alle gebruikers van de server;[165]

g. het tijdstip waarop, of de periode waarbinnen aan het bevel uitvoering wordt gegeven;
h. in het geval het een bevel, bedoeld in lid 1, onderdeel c, betreft: een melding van het voornemen om een technisch hulpmiddel op een persoon te bevestigen.

Als het bevel betrekking heeft op de inzet van een afzonderlijke bijzondere opsporingsbevoegdheid, te weten het onderzoeksdoel in lid 1 (van de genoemde drie artikelen) onder b (direct afluisteren en het aftappen van communicatie), of het onderzoeksdoel onder c (de stelselmatige observatie), kunnen in het bevel tevens de gegevens worden opgenomen die in een afzonderlijk bevel voor de toepassing van een dergelijke bevoegdheid moeten worden opgenomen. Er is dan slechts één bevel nodig voor de toepassing van de vorenbedoelde bevoegdheden waarbij een geautomatiseerd werk op afstand heimelijk wordt binnengedrongen.[166]
Niet is vereist dat het bevel de methode vermeldt waarmee in een geautomatiseerd werk wordt binnengedrongen. Dit zou volgens de minister de opsporingsdiensten nodeloos beperken in de wijze waarop uitvoering wordt gegeven aan het bevel en overigens kunnen leiden tot extra werklast voor de rechterlijke macht vanwege de mogelijke noodzaak tot wijziging van het bevel en de daarmee samenhangende machtiging als tijdens de uitvoering van de bevoegdheid blijkt dat een aanpassing van de methode voor het binnendringen noodzakelijk is. In de praktijk zal het volgens de minister veelvuldig voorkomen dat de methode aanpassing behoeft om de beveiliging van het geautomatiseerde werk te doorbreken of te omzeilen; op dit punt dient de nodige flexibiliteit te worden geboden. Daarbij komt dat methoden voor het binnendringen in een geautomatiseerd werk niet aan de openbaarheid prijsgegeven kunnen worden, omdat deze dan niet meer kunnen worden gebruikt.[167]

---

161 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 102. Welke kenmerken het geautomatiseerde werk omschrijven kan per voorgestelde inzet verschillen. Zie *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 13.

162 *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 13.

163 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 102.

164 Zie bijv. *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 42: "*Wanneer berichten in een concept-inbox worden geplaatst kan sprake zijn van stromende gegevens, indien de gegevens bijvoorbeeld vanuit een locatie worden bekeken en daarmee (tijdelijk) worden opgehaald vanaf de server van de aanbieder van de emaildienst. In de huidige situatie zou daarvoor de bevoegdheid van het aftappen en opnemen van telecommunicatie (art. 126m/t Sv) kunnen worden ingezet. Verschillende aanbieders werken echter met een https-verbinding (zoals Google) waardoor de inhoudelijke gegevens niet inzichtelijk zijn nadat deze zijn afgetapt. In de praktijk kunnen de inhoudelijke berichten van mails die geraadpleegd worden in een concept-box veelal dus niet in leesbare vorm worden verkregen. Wanneer berichten in een concept-inbox op het geautomatiseerde werk worden bewaard, dan is er sprake van vaste gegevens. Het wetsvoorstel biedt de mogelijkheid van het op afstand binnendringen in een geautomatiseerd werk met het oog op het overnemen van gegevens die in dat werk zijn opgeslagen.*"

165 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 80.

166 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 30. In principe is voor de onderzoeksdoelen onder b en c namelijk een afzonderlijk bevel vereist, zie p. 100 en 102. Het bevel ex art. 126nba Sv dient in die gevallen immers 'ter uitvoering van' de bevelen die zijn opgesomd in de omschrijving van de onderzoeksdoelen onder b en c.

167 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 103.

De wijziging, aanvulling of verlenging van het bevel

Ingevolge lid 5 van artikel 126nba Sv kan het bevel worden gewijzigd, aangevuld, verlengd of beëindigd, met dien verstande dat de officier van justitie voor wijziging, aanvulling of verlenging een machtiging van de rechter-commissaris behoeft. Het bevel kan volgens lid 3 van artikel 126nba Sv telkens voor een periode van ten hoogste vier weken worden verlengd.[168]

Het bevel kan dus worden gewijzigd of aangevuld, bijvoorbeeld wanneer tijdens de uitvoering van de bevoegdheid blijkt dat de bevoegdheid alsnog voor een ander doel moet worden ingezet dan omschreven in het bevel waarvoor de machtiging is gegeven.[169]

De wijziging moet schriftelijk plaatsvinden en wordt met redenen omkleed. Ook dient de rechter-commissaris schriftelijk machtiging te verlenen voor de aanvulling, wijziging of verlenging van een bevel.

Net als bij andere bijzondere opsporingsbevoegdheden is voorzien in de mogelijkheid dat bij dringende noodzaak de beslissing van de officier van justitie[170] tot wijziging, aanvulling, verlenging of beëindiging van het bevel mondeling worden gegeven. Datzelfde geldt voor de machtiging tot wijziging, aanvulling of verlenging van het bevel. De officier van justitie en de rechter-commissaris stellen deze in dat geval binnen drie dagen op schrift.

Anders dan bij andere bijzondere opsporingsbevoegdheden, zoals stelselmatige observatie en het opnemen van vertrouwelijke communicatie, is de mogelijkheid van het mondeling geven van een bevel van de officier van justitie, respectievelijk een machtiging van de rechter-commissaris beperkt tot het *aanpassen* van een eerder gegeven schriftelijk bevel. Een eerste bevel tot het binnendringen en het verrichten van onderzoekshandelingen in een geautomatiseerd werk kan dus niet mondeling worden gegeven, net zomin als de machtiging daartoe. Deze beperking houdt volgens de minister verband met de procedurele eisen en waarborgen die zijn verbonden aan de inzet van het onderzoek in een geautomatiseerd werk. Dit onderzoek vereist een gedegen voorbereiding, inclusief het adviestraject van de CTC. Daarmee is volgens de minister niet goed verenigbaar dat een eerste bevel mondeling wordt gegeven.[171]

3.5. De nadere normering

Het kaderstellend karakter van het Besluit onderzoek in een geautomatiseerd werk

Binnendringen en het verrichten van onderzoekshandelingen in een geautomatiseerd werk is krachtens artikel 126nba lid 1 en lid 8 Sv, artikel 126uba lid 1 en lid 3 Sv, artikel 126zpa lid 1 en lid 3 Sv, artikel 126ee Sv,[172] en artikel 18 lid 1 van de Wet politiegegevens nader genormeerd in het Besluit onderzoek in een geautomatiseerd werk (hierna weer: het Besluit, of: het Bogw). In de nota van toelichting op het Besluit wordt hierover het volgende opgemerkt:

> *"De bestrijding van computercriminaliteit vraagt, in het licht van de snelle en voortdurende technologische ontwikkelingen, om enige flexibiliteit en abstractie van technische details. De regels in de hoofdstukken 3 tot en met 8 van dit besluit hebben gelet hierop een kaderstellend*

[168] De leden 3 tot en met 9 van art. 126nba Sv zijn in de artikelen 126uba en 126zpa Sv van overeenkomstige toepassing verklaard.

[169] Zie ook *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 104.

[170] Die ook de beëindiging van het bevel kan betekenen. Zie *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 104.

[171] *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 104.

[172] Art. 126ee Sv bevat de grondslag voor het stellen van regels omtrent: (a) de opslag, verstrekking, plaatsing en verwijdering van de technische hulpmiddelen, (b) de technische eisen waaraan de hulpmiddelen voldoen, onder meer met het oog op de onschendbaarheid van de vastgelegde waarnemingen of de vastgelegde gegevens, en met het oog op het voorkomen van misbruik door derden, en (c) de controle op de naleving van de eisen die zijn bedoeld onder (b). Zie over art. 126ee Sv meer in het bijzonder *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 109-110.

karakter. Er worden eisen gesteld aan de organisatie, inrichting en controleerbaarheid van het onderzoekproces. De uitwerking hiervan vindt plaats in de opsporingspraktijk (via handreikingen, mandaatbesluiten, keuringsprotocollen etc.)."[173]

Nadrukkelijk heeft de minister dus de nadere invulling van de normering van de uitvoeringsfase overgelaten aan de praktijk om zodoende de benodigde flexibiliteit te bieden. In deze en volgende paragrafen komen verschillende elementen uit het Bogw aan bod.

Het technische team en de strikte taakscheiding ten opzichte van het tactische team

Binnen het bestek van een opsporingsonderzoek dat door een tactisch politieteam wordt uitgevoerd, kan onder omstandigheden – naar het oordeel van de officier van justitie – noodzaak bestaan tot het verrichten van onderzoek in een geautomatiseerd werk. Het daadwerkelijke binnendringen in een geautomatiseerd werk ter uitvoering van het bevel van de officier van justitie wordt echter niet door dat tactische team uitgevoerd, maar uitsluitend verricht door daartoe aangewezen opsporingsambtenaren van een technisch team.[174] Datzelfde geldt voor de (eventuele) plaatsing van een technisch hulpmiddel, voor het verrichten van onderzoekshandelingen in het geautomatiseerde werk in kwestie, en voor het verwijderen van het technisch hulpmiddel.[175]

Een 'technisch team' is volgens de definitiebepaling van artikel 1 onder h Bogw een onderdeel van de landelijke eenheid van de Nationale politie dat kan worden belast met de uitvoering van een bevel van de officier van justitie als bedoeld in de artikelen 126nba, 126uba en 126zpa, telkens lid 1, Sv.

De regeling schrijft een duidelijke taakscheiding tussen de technische en de tactische opsporingsambtenaren voor. Alleen de technische, daartoe aangewezen ambtenaren hebben toegang tot het systeem van waaruit het onderzoek in het geautomatiseerde werk wordt uitgevoerd. De tactische opsporingsambtenaren, die feitelijk met de bewijsvergaring in het opsporingsonderzoek bezig zijn, hebben daartoe geen toegang. Zij worden voorzien van de gegevens die in het bevel zijn aangeduid waar specifiek om gevraagd is in het bevel en die via bijvoorbeeld de geplaatste software door het technische team worden aangeleverd. De tactische opsporingsambtenaren hebben zelf geen toegang tot de technische voorzieningen.[176]

Gelet op de bijzondere expertise en de technische voorzieningen die nodig zijn voor het uitvoeren van onderzoek in een geautomatiseerd werk is de organisatie van de technische teams centraal belegd binnen de politieorganisatie.[177] Hoewel hier (en ook in de wetsgeschiedenis) veelvuldig wordt gesproken over 'het' technische team, laat de wet ruimte voor het instellen van meer dan één technisch team, met dien verstande dat deze technische teams in alle gevallen deel uitmaken van de landelijke eenheid van de Nationale politie.[178]

---

[173] Nota van toelichting op het Bogw, onder 3.1, p. 13.
[174] *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 30; zie ook de nota van toelichting op het Bogw, p. 35.
[175] Art. 23 lid 1 Bogw (plaatsing), art. 24 lid 1 Bogw (onderzoekshandelingen) en art. 25 lid 2 Bogw (verwijdering).
[176] *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 52.
[177] Zie voor meer informatie de nota van toelichting op het Bogw, p. 13-14.
[178] Zie nogmaals art. 1 onder h Bogw (definitie 'technisch team'). Zie ook de nota van toelichting op het Bogw, p. 33 en 35. Zie verder: *Kamerstukken II* 2018/19, 34 372, nr. 29 (verslag van een schriftelijk overleg), p. 8, en *Kamerstukken I* 2016/17, 34 372, D (MvA I), p. 40.

Een opsporingsambtenaar[179] kan door zijn werkgever worden aangewezen voor het binnendringen en het verrichten van onderzoekshandelingen in een geautomatiseerd werk.[180] De door zijn werkgever aangewezen opsporingsambtenaar kan echter uitsluitend met de uitvoering van een hiertoe strekkend bevel van de officier van justitie worden belast indien de opsporingsambtenaar lid is van een technisch team.[181, 182] Daarvoor moet de korpschef hem als zodanig hebben aangewezen. De korpschef kan de hier bedoelde opsporingsambtenaar uitsluitend als lid van een technisch team aanwijzen indien de opsporingsambtenaar voldoet aan de hiervoor geldende kwalificatie-eisen.[183] Door het onderzoek in een geautomatiseerd werk voor te behouden aan opsporingsambtenaren die beschikken over specialistische kennis en vaardigheden op het terrein van ICT kan de kwaliteit en professionaliteit van het onderzoek worden geborgd.[184]

De opsporingsambtenaren van het technische team maken geen deel uit van het tactische team dat het opsporingsonderzoek uitvoert.[185] Met deze functiescheiding, die volgens de minister ook bij de toepassing van een telefoon- of internettap gebruikelijk is,[186] wordt beoogd het risico op tunnelzicht te verminderen.[187] De nota van toelichting op het Besluit spreekt in dit verband over een "*strikte taakverdeling en functiescheiding*" gedurende het opsporingsonderzoek dat plaatsvindt onder het gezag van de officier van justitie. Omdat het technische team niet is betrokken bij het operationele onderzoek van het tactische team, wordt voorkomen dat het technische team op oneigenlijke gronden wordt beïnvloed bij het maken van afwegingen met betrekking tot de haalbaarheid en de wijze van uitvoering van het onderzoek in een geautomatiseerd werk.[188] "*Afhankelijk van het verloop van het onderzoek kan de grens tussen het technisch optreden en het tactisch optreden verschillen,*

[179] Meer volledig: alleen de opsporingsambtenaren als bedoeld in de artt. 141, onder b, c en d, en 142 Sv. Dat zijn dus de algemene opsporingsambtenaren van de Nationale politie, van de Koninklijke marechaussee en van de bijzondere opsporingsdiensten, alsook de bijzondere opsporingsambtenaren van art. 142 Sv, maar niet de officieren van justitie.

[180] Zie art. 3 lid 1 Bogw. Zie verder: *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 30. Zie ook de uitdrukkelijke bewoordingen van de artt. 22 tot en met 26 Bogw.

[181] Zie art. 3 lid 2 Bogw.

[182] Art. 4 Bogw voorziet, in afwijking van art. 3 lid 2 Bogw, in de mogelijkheid van incidentele samenwerking met leden van een technisch team door een opsporingsambtenaar (als bedoeld in de artt. 141, onder b, c en d, en 142 Sv) die door zijn werkgever is aangewezen voor het binnendringen en het verrichten van onderzoekshandelingen in een geautomatiseerd werk, maar die zelf géén 'lid' is van een technisch team. Zo'n opsporingsambtenaar kan door de korpschef worden aangewezen als 'deelnemer' aan een technisch team, zulks voor de duur van de uitvoering van het bevel in een concrete zaak, en dit indien hij naar het oordeel van de korpschef beschikt over specifieke kennis en vaardigheden, benodigd voor de uitvoering van dat bevel. Om de kwaliteit en professionaliteit van het onderzoek te borgen bepaalt art. 4 lid 3 Bogw dat een opsporingsambtenaar die op ad-hocbasis deelneemt aan een technisch team gedurende de uitvoering van het onderzoek wordt begeleid door een lid van een technisch team. Zie de nota van toelichting op het Bogw, p. 36.

[183] Zie art. 3 lid 3 Bogw. De kwalificatie-eisen voor de opsporingsambtenaren van een technisch team zijn neergelegd in (de toelichting op) de Regeling kwalificaties opsporingsambtenaren technisch team, voluit: Regeling van de Minister van Justitie en Veiligheid van 15 februari 2019, kenmerk 2429311, houdende regels betreffende de kwalificaties van opsporingsambtenaren die door de korpschef kunnen worden aangewezen als lid van een technisch team, *Stcrt.* 2019, 10910.

[184] Zie de nota van toelichting op het Bogw, p. 13 en p. 41.

[185] *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 14 en 31; *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 28. Het tactische team zal doorgaans onderdeel zijn van de recherche van de Nationale politie, maar dat is niet noodzakelijk. Ook de Koninklijke marechaussee voert overeenkomstig art. 4 Politiewet 2012 politietaken uit, en dit op grond van art. 14 Politiewet 2012 onder gezag van het OM. Hetzelfde geldt mutatis mutandis voor bijzondere opsporingsdiensten, waarvan met name de Fiscale inlichtingen- en opsporingsdienst (FIOD), die in dit verband ook onder het gezag van het OM (het functioneel parket) opereert, vermelding verdient.

[186] *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 56.
Opmerking onderzoekers: of die vergelijking met de praktijk van de internettap en de telefoontap werkelijk helemaal opgaat is zeer de vraag. Weliswaar wordt de tap (inderdaad) geplaatst en gefaciliteerd door technici van de afdeling interceptie en sensing (I&S), maar de onderschepte telecommunicatie wordt door hen (zonder dat zij zelf kennisnemen van de inhoud van die telecommunicatie) rechtstreeks elektronisch beschikbaar gesteld aan de opsporingsambtenaren die zijn verbonden aan het tactische team dat met het opsporingsonderzoek is belast.

[187] *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 14 en 31. Zie in het bijzonder artt. 3, 4 en 24 Bogw en de nota van toelichting, onder II, artikelsgewijze toelichting, art. 3, Lidmaatschap van een technisch team.

[188] De nota van toelichting op het Bogw, onder 3.2, p. 14-15.

maar de samenwerking zal dusdanig plaatsvinden dat het tactisch team geen enkele invloed kan uitoefenen op het binnendringen in het geautomatiseerde werk en de plaatsing, inzet en verwijdering van een technisch hulpmiddel", aldus de minister.[189] Ook is er geen mogelijkheid voor de tactische medewerkers om bij de inzet eigenstandig invloed uit te oefenen op de werking van eventueel te gebruiken software.[190]
De organisatorische scheiding tussen het technische team en het tactische team behoeft de samenwerking tussen de teams niet te belemmeren. De officier van justitie onder wiens leiding het opsporingsonderzoek plaatsvindt vervult hierbij een 'schakelfunctie'.[191] Hoe de officier van justitie die schakelfunctie moet inkleden wordt in de nota van toelichting op het Bogw echter niet vermeld. Het is dan ook de vraag hoe in de praktijk het OM, en de officier van justitie in het concrete geval, deze schakelfunctie vervult om de strikte taakverdeling en functiescheiding te kunnen waarborgen. Op dit vraagstuk wordt teruggekomen onder de beschrijving van de onderzoeksbevindingen.

3.6. De uitvoering van het bevel

Een beschouwing van de fasen van de bevoegdheidsuitoefening

Behalve door de hiervoor omschreven wettelijke voorwaarden en de eis van een voorafgaande proportionaliteits- en subsidiariteitstoets, wordt de uitvoering van de bevoegdheid nader genormeerd door een stelsel van procedurele eisen en waarborgen. In dat kader is het nuttig om eerst stil te staan bij de vraag hoe de minister de uitvoering van het bevel ex artikel 126nba Sv voor ogen heeft gehad. De minister onderscheidt bij de uitvoering van het bevel drie fasen:[192]

1. een verkennende fase, waarin het onderzoek in het geautomatiseerde werk wordt voorbereid en eventuele reeds bestaande wettelijke bevoegdheden worden toegepast,
2. de fase waarin het geautomatiseerde werk heimelijk en op afstand wordt binnengedrongen en (eventueel) een technisch hulpmiddel wordt geplaatst; de fase waarin in het geautomatiseerde werk onderzoekshandelingen worden verricht, en
3. een eindfase (de afsluitingsfase) waarin de inzet van de bevoegdheid wordt beëindigd en het technisch hulpmiddel wordt verwijderd.

De verkennende fase

Na afgifte van het bevel behelst de verkennende fase het volgende:[193]

a. Het technische team zal in de praktijk eerst een voorverkenning verrichten.
b. Na analyse van de resultaten daarvan wordt een plan van aanpak voor het binnendringen in het geautomatiseerde werk opgesteld.
c. Het plan van aanpak voor het binnendringen in het geautomatiseerde werk wordt getest in een proefopstelling.

(Ad a). In een opsporingsonderzoek is het, voorafgaand aan eventuele inzet van de bevoegdheid tot onderzoek in een geautomatiseerd werk nodig om een goed beeld te verkrijgen van de mogelijkheden om daadwerkelijk toegang te verkrijgen tot het geautomatiseerde werk en de daaraan verbonden risico's. Voor het beoordelen van de risico's is het van groot belang dat de kenmerken van het geautomatiseerde werk zo goed mogelijk in kaart worden gebracht.[194]

---

189 De nota van toelichting op het Bogw, onder 3.3, p. 17. Zie ook *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 40.
190 Zie ook *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 59.
191 Zie de nota van toelichting op het Bogw, p. 17.
192 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 31-32; *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 70.
193 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 31-32; Nota van toelichting op het Bogw, p. 16 en p. 46; *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 14, p. 70-71; *Kamerstukken II* 2017/18, 34 372, nr. 27 (verslag van een schriftelijk overleg), p. 12.
194 Zie *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 32. Ook: *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 14, 70-71.

Het kan in de eerste plaats nodig zijn om het geautomatiseerde werk of de persoon die ervan gebruikmaakt te identificeren, zodat zeker is dat de voorgestelde bevoegdheid wordt uitgeoefend ten aanzien van het juiste geautomatiseerde werk of de juiste persoon.[195] Voor het identificeren van het geautomatiseerde werk of van de gebruiker kan toepassing worden gegeven aan de bevoegdheid tot het vorderen van verkeersgegevens (artikelen 126n, 126u en 126zh Sv) of van de bevoegdheid tot het opvragen van gebruikersgegevens (artikelen 126na, 126ua en 126zi Sv). De bevoegdheid tot het aftappen van communicatie (artikelen 126m, 126t en 126zg Sv) kan bijvoorbeeld worden aangewend om door middel van een internettap in kaart te brengen of de toegang tot het internet verloopt via een router van een thuisnetwerk of via een openbare hotspot.[196]
Voor de daadwerkelijke uitvoering van onderzoek in een geautomatiseerd werk is het van belang dat bekend is welke programma's zijn geïnstalleerd, welke bestandsmappen er zijn (zodat een technisch hulpmiddel onopvallend kan worden geplaatst), of er meer gebruikers zijn, hoe het beheer verloopt, welk besturingsprogramma van toepassing is en wat de risico's zijn. Aan de hand van deze informatie kan een globale inschatting worden gemaakt van de barrières voor onderzoek in het geautomatiseerde werk, in het bijzonder op het gebied van de beveiliging. Bij de inzet van de voorgestelde bevoegdheid zal dikwijls maatwerk nodig zijn om, afhankelijk van de concrete situatie, de juiste en meest doelgerichte methode ten aanzien van het geautomatiseerde werk te kunnen toepassen. Hierbij wordt informatie verzameld uit open bronnen. Ook kunnen bijzondere opsporingsbevoegdheden worden ingezet, bijvoorbeeld om te proberen inloggegevens te achterhalen.

(Ad b). Na de hiervoor bedoelde technische voorverkenningen en een analyse daarvan, zal een plan van aanpak voor het binnendringen in het geautomatiseerd werk worden opgesteld.[197] Daarin wordt een omschrijving gegeven van de wijze van binnendringen en van de methode en functionaliteiten voor het verrichten van onderzoekshandelingen. Ieder geautomatiseerd werk is vanuit technisch oogpunt anders en de beveiliging kan vele vormen aannemen. Dit betekent dat de methode voor het binnendringen nauwkeurig moet worden afgestemd op het geautomatiseerde werk in kwestie.[198] Bij de keuze van een methode van binnendringen zijn, naast proportionaliteit en subsidiariteit, aspecten als de effectiviteit van de inzet, de kans op onderkenning van het binnendringen en het risico op gevolgschade van belang.[199]

(Ad c). Het plan van aanpak voor het binnendringen in het geautomatiseerd werk wordt getest in een proefopstelling. Daarbij wordt getoetst of de gekozen methode naar verwachting functioneert. Bij de controle van het functioneren van binnendringsoftware in een (representatieve) testomgeving wordt aandacht besteed aan de risico's voor het

[195] *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 32; *Kamerstukken II* 2017/18, 34 372, nr. 27 (verslag van een schriftelijk overleg), p. 12.
[196] *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 32.
[197] Zoals reeds opgemerkt moet het eerdergenoemde plan van aanpak *voor de uitvoering van een onderzoek in het geautomatiseerde werk*, dat onderdeel is van het rapport haalbaarheidsonderzoek en dat mede dient voor de aanvraag van een bevel ex art. 126nba/uba/zpa Sv, worden onderscheiden van het hier bedoelde plan van aanpak *voor het binnendringen in het geautomatiseerde werk*, dat door het technische team wordt opgesteld nádat een bevel ex art. 126nba/uba/zpa Sv is afgegeven en dat onderdeel is van de verkennende fase. Alleen het plan van aanpak voor het binnendringen in het geautomatiseerde werk wordt getest in een proefopstelling.
[198] Zie *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 11 en p. 38.
[199] Zie *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 38.

te onderzoeken geautomatiseerd werk, waaronder de nevenschade voor derden.[200] Ook in het geval binnendringsoftware wordt ingekocht wordt het functioneren ervan in een (representatieve) testomgeving gecontroleerd, onder meer op bruikbaarheid en op de vragen of de software niet onrechtmatig data verzamelt en of die software niet heimelijk communiceert met derden.[201] Bij gebruik van een technisch hulpmiddel wordt beoordeeld of dat correct kan worden ingesteld en of de werking geen onbedoelde neveneffecten heeft.[202]

De onderzoeksfase: (1) binnendringen en (2) het verrichten van onderzoekshandelingen

Wanneer tijdens de verkennende fase is bepaald op welk geautomatiseerd werk en op welke gegevens of categorieën van gegevens de bevoegdheidsuitoefening betrekking heeft, dan kan, indien aan de juridische voorwaarden daarvoor is voldaan en de risico's zorgvuldig zijn afgewogen, de officier van justitie een bevel geven overeenkomstig de artikelen 126nba, 126uba en 126zpa Sv (de onderzoeksfase). In navolging van de memorie van toelichting[203] bij het wetsvoorstel worden in de nota van toelichting op het Besluit binnen de onderzoeksfase de eerder genoemde twee (sub)fasen onderscheiden:

1. De eerste sub-fase betreft het (heimelijk en op afstand) binnendringen in een geautomatiseerd werk, kortweg 'binnendringen in een geautomatiseerd werk'. Dit onderdeel omvat veelal het plaatsen en verwijderen van een technisch hulpmiddel.
2. De tweede sub-fase betreft het – al dan niet met een technisch hulpmiddel – verrichten van bepaalde onderzoekshandelingen in het geautomatiseerde werk waarin is binnengedrongen. Daarmee kunnen gegevens worden vastgelegd die kunnen dienen als bewijs in een strafzaak. Als deze tweede sub-fase wordt bedoeld, dan wordt dit omschreven als het 'verrichten van onderzoekshandelingen'.

Wanneer het gaat om beide fasen tezamen (de onderzoeksfase), dan wordt dit in het Besluit aangeduid als: (het uitvoeren van) onderzoek in een geautomatiseerd werk.

Het daadwerkelijke binnendringen in het geautomatiseerde werk vindt plaats overeenkomstig het vooraf opgestelde plan van aanpak voor het binnendringen in het geautomatiseerde werk.[204] Er zijn verschillende technieken beschikbaar die het mogelijk maken in een geautomatiseerd werk binnen te dringen, en daarbij eventuele beveiligingen te omzeilen. Het aantal verschillende technieken is niet limitatief, en de mate van beveiliging van de uiteenlopende soorten van geautomatiseerde werken varieert sterk.

---

[200] Zie bijvoorbeeld *Kamerstukken II* 2018/19, 34 372, nr. 29 (verslag van een schriftelijk overleg), p. 13: "*Het doel van de keuring van technische hulpmiddelen die worden gebruikt voor het verrichten van onderzoekshandelingen is om te borgen dat de werking van een hulpmiddel dusdanig betrouwbaar is dat de hiermee verkregen onderzoeksgegevens, die kunnen dienen als bewijs in een strafzaak, betrouwbaar, integer en herleidbaar zijn. De wijze waarop het binnendringen in een geautomatiseerd werk plaatsvindt is niet van invloed op de betrouwbaarheid van de onderzoeksgegevens en maakt daarom geen onderdeel uit van het keuringsproces. De kwaliteit van het binnendringen in een geautomatiseerd wordt geborgd door dit handelen voor te behouden aan daartoe opgeleide deskundige opsporingsambtenaren van een technisch team. Het functioneren van de binnendringsoftware wordt in een testomgeving gecontroleerd. In de procedure rondom de inzet van de bevoegdheid wordt aandacht besteed aan de risico's voor het te onderzoeken geautomatiseerd werk, waaronder de schade voor derden.*" Ook: *Kamerstukken I* 2018/19, 34 372, L (verslag van een schriftelijk overleg), p. 8-9: "*Een zorgvuldige inschatting en afweging van de mogelijke risico's van onderzoekshandelingen voor derden vormt een expliciet onderdeel van het haalbaarheidsonderzoek, dat voorafgaand aan de inzet van de bevoegdheid wordt verricht. In zoverre wordt materieel tegemoet gekomen aan de opmerking van de Afdeling* [advisering van de Raad van State]*, dat er bij de afweging van de inzet van de bevoegdheid aandacht moet zijn voor eventuele nadelige gevolgen voor derden. Voordat wordt overgegaan tot de inzet van een technisch hulpmiddel wordt de werking hiervan in een testomgeving gecontroleerd. Hierbij wordt aandacht besteed aan de risico's voor het te onderzoeken geautomatiseerd werk, waaronder schade voor derden. Door risico's van het onderzoek en mogelijke schade aan derden mee te wegen in het haalbaarheidsonderzoek en voorafgaand aan de inzet in een testomgeving te controleren wordt het risico op schade voor derden tot een minimum beperkt.*"

[201] Zie de nota van toelichting op het Bogw, onder 3.5, p. 18 en p. 20; *Kamerstukken II* 2017/18, 34 372, nr. 27 (verslag van een schriftelijk overleg), p. 7-8; *Kamerstukken I* 2017/18, 34 372, G (NMvA I), p. 15-16.

[202] *Handelingen I* 2017/18, nr. 34, item 5, p. 19.

[203] *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 7.

[204] Zie de nota van toelichting op het Bogw, p. 16 en 46, en ook *Kamerstukken II* 2017/18, 34 372, nr. 27 (verslag van een schriftelijk overleg), p. 12.

In de eerste plaats kan worden binnengedrongen met behulp van inloggegevens die door middel van *social engineering* of het gebruik van kunstmatige intelligentie zijn verkregen. In de tweede plaats kunnen inloggegevens van een persoon worden bemachtigd door hem te verleiden te reageren op een e-mailbericht of een ander verzoek om contact. Met behulp van deze technieken kan malware worden geplaatst, waardoor toegang tot een geautomatiseerd werk wordt verkregen en een bug of keylogger kan worden aangebracht. In de derde plaats kunnen kwetsbaarheden in een computer worden geëxploiteerd, zoals fouten of lekken (bugs) in software.[205, 206]
Zodra in het geautomatiseerde werk is binnengedrongen kunnen bepaalde onderzoekshandelingen worden verricht, zoals omschreven in artikel 126nba lid 1 Sv. Deze onderzoekshandelingen kunnen handmatig worden verricht, dan wel met behulp van een technisch hulpmiddel in de vorm van een softwareapplicatie die door een opsporingsambtenaar van een technisch team in het geautomatiseerde werk wordt geplaatst (artikel 23 lid 1 Bogw).

De afsluitingsfase

Zodra het doel van het onderzoek in het geautomatiseerde werk is bereikt, of wanneer de geldigheidsduur van het bevel is verlopen, wordt het onderzoek beëindigd. Indien een technisch hulpmiddel is geplaatst dan wordt dit zoveel mogelijk verwijderd[207] en wordt het systeem zo veel mogelijk achtergelaten als ware er niet in het systeem binnengedrongen.[208] In sommige gevallen kan worden afgezien van de verwijdering van geïnstalleerde software of van het ongedaan maken van de wijzigingen die in het geautomatiseerde werk zijn aangebracht.[209] Daarop wordt hieronder teruggekomen.

Thans wordt nader ingegaan op de onderzoeksfase van de inzet van de bevoegdheid.

3.7. Het binnendringen in een geautomatiseerd werk

Het binnendringen

Teneinde het verrichten van onderzoekshandelingen in een geautomatiseerd werk mogelijk te maken, zal het technische team eerst (heimelijk en op afstand) binnendringen in een geautomatiseerd werk. Van 'binnendringen' is in ieder geval sprake wanneer de toegang tot het geautomatiseerde werk wordt verworven door het doorbreken van een beveiliging, door een technische ingreep, met behulp van valse signalen of een valse sleutel, of door het aannemen van een valse hoedanigheid.[210]
Er zijn verschillende technieken beschikbaar die het binnendringen mogelijk maken. Er zijn immers vele verschillende soorten geautomatiseerde werken en de beveiliging daarvan kan nog eens vele verschillende gedaanten aannemen. Concreet kan het daarbij gaan om de toepassing van softwareapplicaties, maar ook om het eenvoudig inloggen op het geautomatiseerde werk

---

205 Om het verwarrend te maken worden dergelijke kwetsbaarheden of lekken in software ook wel een 'bug' genoemd. Kwetsbaarheden in de beveiliging van software die zich lenen voor dit – door de ontwikkelaar niet bedoelde – gebruik worden 'exploits' genoemd. Hierop wordt in de hoofdtekst teruggekomen.

206 Zie *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 9. Zie verder: *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 34-35. Hierover gaat ook het verslag van een deskundigenbijeenkomst met de vaste commissie voor Veiligheid en Justitie van de Eerste Kamer, *Kamerstukken I* 2016/17, 34 372, E.

207 Zie art. 126nba lid 6 Sv, van overeenkomstige toepassing verklaard in de artt. 126uba en 126zpa Sv.

208 *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 76.

209 Zie *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 76, en *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 36-37.

210 Voor de regeling rond het binnendringen van het geautomatiseerde werk is aangesloten bij de regeling van de computervredebreuk in het Wetboek van Strafrecht, art. 138ab lid 1 Sr. Zie *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 15.

met inloggegevens van de gebruiker die voorafgaand aan de toepassing van de bevoegdheid zijn verkregen door middel van bijvoorbeeld *social engineering* (ontfutselen).[211]
Van belang voor de keuze van een methode van binnendringen zijn, naast proportionaliteit en subsidiariteit, aspecten als de effectiviteit van de inzet, de kans op onderkenning van het binnendringen door derden en het risico op gevolgschade (voor het onderzochte geautomatiseerde werk).[212] In het geval (commerciële) binnendringsoftware wordt ingekocht, wordt het functioneren hiervan in een testomgeving gecontroleerd.[213]
Anders dan ten aanzien van het technisch hulpmiddel waarmee onderzoekshandelingen worden verricht, maakt de wijze waarop het binnendringen plaatsvindt, bijvoorbeeld de wijze waarop de beveiliging van een geautomatiseerd werk wordt omzeild, geen deel uit van het keuringsproces dat in paragraaf 3.8 aan bod komt.

Een wettelijke grondslag voor (het faciliteren van) binnendringen

In de wetsgeschiedenis passeren diverse illustraties van methoden voor binnendringen de revue. De bespreking van deze methoden is echter niet limitatief bedoeld en in de wet en wetsgeschiedenis is van deze methoden geen nadere normering gegeven. De vraag rijst dan wat de wettelijke basis is voor deze verrichtingen, bijvoorbeeld indien die in de tijd ruim voorafgaan aan het onderzoek in een geautomatiseerd werk zelf. Datzelfde geldt voor de toepassing van methoden die geen vorm van binnendringen behelzen, maar die ertoe strekken het binnendringen als zodanig te ondersteunen of mogelijk te maken. Indien met dergelijke methoden ter voorbereiding van het onderzoek in een geautomatiseerd werk geen, dan wel een niet meer dan geringe inbreuk wordt gemaakt op de grondrechten en vrijheden van burgers, en deze methoden niet zeer risicovol zijn voor de integriteit en beheersbaarheid van de opsporing, kunnen zij eventueel worden gebaseerd op artikel 3 Politiewet.[214]

---

[211] Zie *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 9. Zie: *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 34: "*Er zijn verschillende technieken beschikbaar die het mogelijk maken in een geautomatiseerd werk binnen te dringen, en daarbij eventuele beveiligingen te omzeilen. Het aantal verschillende technieken is niet limitatief, en de mate van beveiliging van de verschillende soorten van geautomatiseerde werken vertoont grote verschillen. In de eerste plaats kan worden binnengedrongen met behulp van inloggegevens die door middel van «social engineering» of het gebruik van kunstmatige intelligentie zijn verkregen. In de tweede plaats kunnen inloggegevens van een persoon worden verkregen door diegene te verleiden te reageren op een e-mailbericht of een ander verzoek om contact. Met behulp van deze technieken kan malware worden geplaatst, waardoor de toegang tot een geautomatiseerd werk open wordt gezet en een «bug» of «keylogger kan worden geplaatst. In de derde plaats kunnen kwetsbaarheden in een computer worden geëxploiteerd, zoals het gebruik van fouten of lekken in de software. Hierbij worden in beginsel geen nieuwe kwetsbaarheden gecreëerd. Zodra een dergelijke kwetsbaarheid wordt opgemerkt kan deze via het internet worden verspreid. Voordat deze informatie wordt verspreid wordt gesproken van een «zero day exploit». De softwarefabrikanten passen voortdurend de software aan om dergelijke kwetsbaarheden op te lossen. Indien de gebruiker de wijzigingen (zogenaamde patches) niet bijhoudt kan gebruik worden gemaakt van een lek in de gebruikte versie van de software.*" Hierover gaat ook het verslag van een deskundigenbijeenkomst met de vaste commissie voor Veiligheid en Justitie van de Eerste Kamer, *Kamerstukken I* 2016/17, 34 372, E.

[212] *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 38.

[213] Zie de nota van toelichting op het Bogw, onder 3.5, p. 18 en p. 20; *Kamerstukken II* 2017/18, 34 372, nr. 27 (verslag van een schriftelijk overleg), p. 7-8.

[214] Aan het Wetboek van Strafvordering ligt de notie ten grondslag dat opsporingsmethoden een voldoende specifiek omschreven en kenbare wettelijke basis behoeven indien zij inbreuk maken op grondrechten en vrijheden van burgers, dan wel wanneer zij zeer risicovol zijn voor de integriteit en beheersbaarheid van de opsporing. Voor een wijze van opsporing die niet specifiek in de wet geregeld is, geldt dat deze onder omstandigheden kan worden gelegitimeerd door de algemene taakstelling van de Nationale politie zoals omschreven in artikel 3 Politiewet 2012 (en de artikelen 141 en 142 Sv), namelijk zolang die wijze van opsporing slechts een beperkte inbreuk maakt op grondrechten van burgers (zoals de aanspraak op privacy) en niet zeer risicovol is voor de integriteit en beheersbaarheid van de opsporing. Zie HR 20 december 2011:ECLI:NL:HR:2011:BP0070, *NJ* 2012/159; HR 20 december 2011, ECLI:NL:HR:2011:BP0199; HR 1 juli 2014, ECLI:NL:HR:2014:1563; HR 5 maart 2019, ECLI:NL:HR:2019:298; HR 19 januari 2021, ECLI:NL:HR:2021:80. Zie ook G.J.M. Corstens, *Het Nederlands strafprocesrecht*, bewerkt door M.J. Borgers en T. Kooijmans, Deventer: Wolters Kluwer 2021, p. 28-30, en B.F. Keulen & G. Knigge, *Strafprocesrecht (Ons strafrecht deel 2)*, Deventer: Wolters Kluwer 2020, p. 305-308.

Het gebruik van commerciële software en van (onbekende) kwetsbaarheden bij het binnendringen

Voor het binnendringen in een geautomatiseerd werk kan onder omstandigheden gebruik worden gemaakt van kwetsbaarheden (bugs) in software die is geïnstalleerd op het geautomatiseerde werk in kwestie.[215] Dat kan zowel bekende als onbekende kwetsbaarheden betreffen.[216] De minister heeft te kennen gegeven dat het gebruik van commerciële binnendringsoftware van derden waarvan niet duidelijk is of deze van bekende of onbekende kwetsbaarheden gebruikmaakt, tot het uiterste geval beperkt moet blijven.[217] Dergelijke software, ook wel '*intrusion software*' genoemd,[218] mag volgens de minister uitsluitend worden aangewend

---

[215] Zie hierover de brief van de staatssecretaris van Veiligheid en Justitie, de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Defensie aan de voorzitter van de Tweede Kamer der Staten-Generaal, van 8 november 2016, *Kamerstukken II* 2016/17, 26 643, nr. 428, p. 2: "*Kwetsbaarheden ontstaan bij het produceren van hard- en software, bijvoorbeeld door programmeerfouten of door beperkte aandacht voor veiligheid bij het ontwerp. Hard- en software worden vaak vanwege concurrentieoverwegingen snel op de markt gebracht. Bovendien zijn de omvang en complexiteit van software fors toegenomen. Veel gebruikte applicaties hebben tegenwoordig tientallen miljoenen regels broncode. Kwetsbaarheden zijn daarom talloos en wijdverbreid.*"

[216] *Kamerstukken I* 2016/17, 34 372, D (MvA I), p. 19. Een onbekende kwetsbaarheid wordt ook wel een 'zero-day *vulnerability*', of kortweg een 'zero-day' genoemd (omdat de producent van de betreffende software/hardware géén gelegenheid heeft gehad, namelijk: slechts nul dagen, om de kwetsbaarheid te verhelpen). De applicaties waarmee van dergelijke kwetsbaarheden gebruik wordt gemaakt heten: zero-day *exploits*. Volgens lid 4 van art. 126ffa Sv wordt onder 'onbekende kwetsbaarheid' verstaan: een kwetsbaarheid in een geautomatiseerd werk waarvan aannemelijk is dat die niet bekend is of kan worden verondersteld niet bekend te zijn bij de producent van het apparaat of van het programma op basis waarvan automatisch computergegevens worden verwerkt, en die kan worden gebruikt om dat geautomatiseerde werk binnen te dringen.

[217] Nota van toelichting op het Bogw, p. 15; *Kamerstukken II* 2018/19, 34 372, nr. 29 (verslag van een schriftelijk overleg), p. 10: "*Het gebruik van commerciële binnendringsoftware van derden is een uiterste middel binnen deze bevoegdheid.*"
Zie verder: *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 34-35; *Kamerstukken I* 2016/17, 34 372, D (MvA I), p. 18-25, waarin de minister uitgebreid ingaat op dit onderwerp; *Kamerstukken I* 2017/18, 34 372, G (NMvA I), p. 3-12; de brief van de staatssecretaris van Veiligheid en Justitie, de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Defensie aan de voorzitter van de Tweede Kamer der Staten-Generaal, van 8 november 2016, *Kamerstukken II* 2016/17, 26 643, nr. 428.

[218] Ter toelichting (uit openbare bronnen). Voorbeelden van wat wel wordt genoemd *intrusion software, surveillance technology, digital intelligence, cyberespionage* of (gewoon) spyware zijn FinFisher, Exodus (voor zowel iPhones als Androids), Zwangi (Spyware.Screenspy), UFED (van het Israëlische *digital intelligence* bedrijf Cellebrite), RCS (van het Italiaanse cyberbedrijf Hacking Team), Sherlock (van het Israëlische cyberbedrijf Candiru), en Pegasus. Thans meer over FinFisher en Pegasus.
FinFisher, ook wel bekend als FinSpy, betreft een softwarepakket van Lench IT solutions plc./Gamma International dat heimelijk kan worden geïnstalleerd op computers, waarmee computers kunnen worden overgenomen, waarmee daarop aanwezige data kunnen worden geregistreerd en waarmee communicatie kan worden onderschept. Het pakket wordt aangeboden aan met name de politie, justitie en inlichtingendiensten van staten. Ideële organisaties als BoF verwijten de producent (onder meer) dat het softwarepakket ook wordt geleverd aan staten waarin mensenrechten structureel worden geschonden. FinFisher kwam ook ter sprake tijdens een deskundigenbijeenkomst met de vaste commissie voor Veiligheid en Justitie van de Eerste Kamer, zie *Kamerstukken I* 2016/17, 34 372, E, p. 11. Zie tevens de brief van de minister van Veiligheid en Justitie van 7 oktober 2014 in antwoord op Kamervragen van het lid Gesthuizen over het gebruik van omstreden spionagesoftware door de politie, *Aanhangsel Handelingen II* 2013/14, 202, en zie M. Persson, 'Politie gebruikt mogelijk omstreden spionagesoftware', *Volkskrant* 8 augustus 2014.
Over Pegasus is veel te doen sinds onderzoekers van de universiteit van Toronto in 2016 het bestaan ervan hebben achterhaald en wereldkundig gemaakt. Pegasus is het paradepaardje van het Israëlische cyberbedrijf NSO Group. Het maakt gebruik van verscheidene kwetsbaarheden, faciliteert diverse aanvallen, en het kan onder bepaalde condities zonder interventie van de gebruiker ('*zero-click*') worden geïnstalleerd op mobiele telefoons en andere mobiele apparaten die draaien op de besturingssystemen iOS (van Apple) of Android (van Google).
Zie voor een *product description* van Pegasus: https://www.documentcloud.org/documents/4599753-NSO-Pegasus.
Zie voor de onthulling van het bestaan van Pegasus: B. Marczak & J. Scott-Railton, *The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender* (Citizen Lab Research Report No. 78), University of Toronto, 24 augustus 2016.
Zie voor berichtgeving over Pegasus onder (veel) meer: 'Niet alleen Catalaanse politici, ook Spaanse premier slachtoffer spyware', *NOS Nieuws* 2 mei 2022; E. Overbeek, 'Polen heeft zijn eigen Watergate: Pegasus is het topje van de spionage-ijsberg', *Trouw* 3 februari 2022; D. Priest, 'A UAE agency put Pegasus spyware on phone of Jamal Khashoggi's wife months before his murder, new forensics show', *Washington Post* 21 december 2021; M. Hijink & W. van Dijk, 'Pegasus verschaft zichzelf toegang tot alles op je mobiel', *NRC* 19 juli 2021, en M. Srivastava & T. Bradshaw, 'Israeli group's spyware 'offers keys to Big Tech's cloud'', *Financial Times* 19 juli 2019 (https://www.ft.com/content/95b91412-a946-11e9-b6ee-3cdf3174eb89).
Zie kritisch bovendien: Amnesty International, *Forensic Methodology Report. How to Catch NSO Group's Pegasus*, London: Amnesty International 2021.
Het Kamerlid Verhoeven (D66) diende op 19 juli 2019 op dit terrein een initiatiefwetsvoorstel in: Voorstel van wet van het lid Verhoeven houdende een regeling voor een afwegingsproces voor het gebruik van kwetsbaarheden in geautomatiseerde werken door de overheid (Wet Zerodays Afwegingsproces), *Kamerstukken II* 2018/19, 35 257.

wanneer minder ingrijpende middelen, zoals het gebruik van inloggegevens, *social engineering* of bekende kwetsbaarheden, niet toereikend zijn om heimelijk toegang te verkrijgen tot een geautomatiseerd werk.[219] Niettemin is de toepassing van software die mogelijk gebruikmaakt van onbekende kwetsbaarheden volgens de minister soms onvermijdelijk om ernstige criminaliteit te kunnen bestrijden.[220]

De missive om de aanwending van commerciële binnendringsoftware waarvan onduidelijk is of deze onbekende kwetsbaarheden exploiteert tot het uiterste te beperken, strekt tot het zo min mogelijk stimuleren van de markt voor onbekende kwetsbaarheden en de daaraan verbonden negatieve gevolgen voor de veiligheid van het internet.[221] In de nota van toelichting op het Bogw verwijst de minister naar het Regeerakkoord 2017–2021, waarin de coalitiepartijen hebben afgesproken dat de aanschaf van dergelijke binnendringsoftware aan beperkingen zal moeten worden gebonden en dat die software slechts zal worden ingekocht in een specifieke

---

219 Nota van toelichting op het Bogw, onder 3.3, p. 15-17. Vgl. *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 38: "*Het gebruik van een kwetsbaarheid is vaak niet de meest aangewezen methode.*"

220 Nota van toelichting op het Bogw, onder 3.3, p. 15; *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 51; *Kamerstukken I* 2017/18, 34 372, G (NMvA I), p. 11; *Kamerstukken II* 2018/19, 34 372, nr. 29 (verslag van een schriftelijk overleg), p. 9. Zie ook *Kamerstukken I* 2016/17, 34 372, D (MvA I), p. 21: *De politie zal geen informatie over onbekende kwetsbaarheden inkopen ten behoeve van de inzet van de voorstelde bevoegdheid tot het binnendringen in een geautomatiseerd werk. Wel is het mogelijk dat de politie software aanschaft waarmee in bepaalde gevallen het binnendringen in geautomatiseerd werk wordt uitgevoerd. Niet kan worden uitgesloten dat dergelijke software gebruik maakt van onbekende kwetsbaarheden. Leveranciers van dergelijke software geven hun broncode doorgaans niet prijs.*" De Kamerleden Verhoeven, Van Tongeren en Gesthuizen hebben op 12 december 2016 een amendement ingediend dat strekte tot een zodanige wijziging van het voorstel tot de Wet computercriminaliteit III dat het binnendringen als bedoeld in art. 126nba lid 1 Sv alleen plaatsheeft zonder gebruik te maken van kwetsbaarheden in software. In de toelichting op het amendement van de leden Verhoeven, Van Tongeren en Gesthuizen valt te lezen: "*Dit amendement beperkt de bevoegdheid voor de politie om geautomatiseerde werken binnen te dringen, er mag namelijk geen gebruik worden gemaakt van kwetsbaarheden in software. Het binnendringen van geautomatiseerde werken zonder gebruik van kwetsbaarheden in software kan bijvoorbeeld door middel van (spear)phishing technieken, oftewel het sturen van een misleidende email of bericht waarmee een verdachte verleid kan worden om een wachtwoord of logingegevens prijs te geven of om een technisch hulpmiddel zoals een keylogger of andere software te installeren, mits zonder het gebruik van kwetsbaarheden, waarmee vervolgens inloggegevens buitgemaakt kunnen worden. Een andere techniek is social engineering, waarmee door middel van psychologische manipulatie het uitvoeren van handelingen of het openbaar maken van vertrouwelijke informatie, zoals een wachtwoord of inloggegevens, uitgelokt kan worden. Daarnaast zijn technieken mogelijk als brute forcing, dictionary attacks of shoulder surfing.*" Zie *Kamerstukken II* 2016/17, 34 372, nr. 13, p. 1. Het amendement is verworpen.

221 Bij de behandeling van het wetsvoorstel in de Eerste Kamer is tijdens een deskundigenbijeenkomst van 20 juni 2017 met de vaste commissie voor Veiligheid en Justitie gesproken over de wereldwijde aanval met het WannaCry ransomware-virus, dat ertoe leidde dat afdelingen in ziekenhuizen sloten en dat bedrijven ontwricht werden. WannaCry was volgens een deskundige een uitstekend voorbeeld van hoe het niet-rapporteren van kwetsbaarheden juist had geleid tot een mondiale cyberaanval. Zie *Kamerstukken I* 2016/17, 34 372, E, p. 4 en p. 11. Zie bovendien: *Kamerstukken I* 2016/17, 34 372, D (MvA I), p. 18-25, waarin de minister uitgebreid ingaat op dit onderwerp.

zaak.[222, 223] De politie kan dan bijvoorbeeld een softwarepakket aanschaffen en/of op basis van de aanschaf van een (beperkte) licentie of gebruiksrecht de binnendringsoftware uitsluitend voor de desbetreffende zaak inzetten.[224]

Als de officier van justitie bepaalt dat het gebruik van binnendringsoftware van een externe leverancier noodzakelijk is, dient dit centraal binnen het OM te worden getoetst alvorens in die specifieke zaak wordt overgaan tot de aanschaf daarvan.[225] Leveranciers van dergelijke software worden gescreend door de AIVD.[226] Bovendien is vereist dat zij niet leveren aan dubieuze

---

222 VVD, CDA, D66 en ChristenUnie, *Vertrouwen in de toekomst. Regeerakkoord 2017-2021*, van 10 oktober 2017. Op p. 3 staat vermeld: "*Voor de uitvoering van de Wet Computercriminaliteit III komt 10 miljoen euro extra beschikbaar. Daarbij zal slechts in een specifieke zaak hacksoftware worden ingekocht door opsporingsdiensten. Leveranciers van dergelijke software worden gescreend door de AIVD en verkopen niet aan dubieuze regimes. Statistieken over het gebruik van hacksoftware worden jaarlijks openbaar gemaakt. Bij de evaluatie van de wet na twee jaar wordt bezien in hoeverre deze regeling de effectiviteit van de wet ernstig aantast. In dat geval wordt alsnog de aanschaf van hacksoftware voor algemeen gebruik overwogen.*" Zie de nota van toelichting op het Bogw, onder 3.3, p. 15.
Een analoge afspraak ontbreekt overigens in het huidige regeerakkoord: VVD, D66, CDA en ChristenUnie, *Omzien naar elkaar, vooruitkijken naar de toekomst. Coalitieakkoord 2021 – 2025,* van 15 december 2021.

223 *Kamerstukken II* 2017/18, 34 372, nr. 27 (verslag van een schriftelijk overleg), p. 7: "*Conform de afspraken in het Regeerakkoord 2017–2021 zal de politie binnendringsoftware van derden die mogelijk gebruik maakt van onbekende kwetsbaarheden alleen aanschaffen als daar in een specifieke zaak een noodzaak toe bestaat. In de praktijk kan het voorkomen dat er gebruik wordt gemaakt van één softwarepakket dat bestaat uit onderdelen voor het verrichten van onderzoekshandelingen (een technisch hulpmiddel), waaraan het onderhavige besluit eisen stelt, en onderdelen voor het binnendringen van een geautomatiseerd werk. Deze software kan met het oog op de keuring van het technische hulpmiddel worden aangeschaft voordat dit nodig is in een specifieke zaak. Dit is noodzakelijk omdat de keuring enige tijd in beslag kan nemen en na een besluit om dergelijke software te gebruiken om binnen te dringen, deze snel ingezet moet kunnen worden. Het gebruik van software op basis van een licentie biedt de mogelijkheid om een demonstratieversie van de software te keuren voordat de software in een specifieke zaak kan worden ingezet om binnen te dringen. Indien inzet om binnen te dringen aan de orde is, dient alsnog een aparte licentie daarvoor te worden aangeschaft. Het gebruik van commerciële binnendringsoftware van derden is een uiterste middel. De wijze waarop het binnendringen plaatsvindt, bijvoorbeeld de wijze van het omzeilen van de beveiliging van een geautomatiseerd werk, maakt geen deel uit van het keuringsproces. Wel wordt het functioneren van de binnendringsoftware in een testomgeving gecontroleerd. Tevens wordt in de procedure rondom de inzet van de bevoegdheid aandacht besteed aan de risico's voor het te onderzoeken geautomatiseerd werk, waaronder schade aan derden.*" Zie ook: *Kamerstukken I* 2017/18, 34 372, G (NMvA I), p. 7 en p. 10.

224 Nota van toelichting op het Bogw, onder 3.3, p. 16-17: "*Na het onderzoek wordt het softwarepakket verwijderd of is de licentie verbruikt waardoor hergebruik niet meer mogelijk is. Wanneer in een toekomstige zaak het gebruik van binnendringsoftware van derden wederom is aangewezen, zal eerst de bruikbaarheid van de minder ingrijpende middelen worden beoordeeld en het daarvoor benodigde gehele toetsings- en beslissingsmodel doorlopen, voordat kan worden overgegaan tot een (hernieuwde) aanschaf van een softwarepakket of van een nieuwe licentie.*"
Zie ook: *Kamerstukken I* 2017/18, 34 372, G (NMvA I), p. 10-11. En zie: *Kamerstukken II* 2018/19, 34 372, nr. 29 (verslag van een schriftelijk overleg), p. 9: "*Conform de afspraken in het Regeerakkoord 2017–2021 zal het inkopen van binnendringsoftware die mogelijk gebruik maakt van onbekende kwetsbaarheden worden beperkt door dit enkel in specifieke zaken mogelijk te maken. Hierdoor wordt het betreden van de markt van binnendringsoftware die mogelijk gebruik maakt van onbekende kwetsbaarheden tot een minimum beperkt. In plaats daarvan wil de regering meer inzetten op de eigen ontwikkeling van methoden voor het binnendringen, daartoe zal de ontwikkeling van passende producten binnen de politie worden gestimuleerd.*"

225 Nota van toelichting op het Bogw, onder 3.3, p. 15. Zie ook: *Kamerstukken II* 2017/18, 34 372, nr. 27 (verslag van een schriftelijk overleg), met name p. 7-8. Hierbij is vermeldenswaard dat bij de behandeling van het wetsvoorstel in de Eerste Kamer tijdens een deskundigenbijeenkomst met de vaste commissie voor Veiligheid en Justitie is gesproken over de behoefte aan toezicht op beleidsniveau dan wel systematisch integraal toezicht aangaande het gebruik van kwetsbaarheden. Zie *Kamerstukken I* 2016/17, 34 372, E, p. 17.

226 Zie de brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties en de minister van Justitie en Veiligheid d.d. 23 juni 2022 in antwoord op Kamervragen van de leden Omtzigt en Van Dijk over het gebruik van hacksoftware, zoals Pegasus, in Nederland, *Aanhangsel Handelingen II* 2021/22, nr. 3252, p. 6.: "*De procedure zoals genoemd in het regeerakkoord van 2017 - dat leveranciers van hacksoftware die wordt ingekocht door opsporingsdiensten worden gescreend door de AIVD - wordt door de AIVD uitgevoerd als een naslagverzoek conform de F-taak in de Wiv 2017 onder artikel 8 lid 2f. Dit artikel betekent dat de AIVD in de eigen systemen naar een specifieke persoon of instantie een naslag kan doen op verzoek van anderen, conform de Regeling naslag Wiv 2017.*"

regimes.[227] Het gaat dan om landen die zich schuldig maken aan ernstige schendingen van mensenrechten of internationaal humanitair recht.[228] Om deze reden voert de politie een toets uit voordat wordt overgegaan tot de aanschaf van binnendringsoftware. Die toets is tweeledig. In de eerste plaats wordt de leverancier gevraagd of hij niet heeft geleverd aan landen waartegen vanuit de EU of de VN restrictieve sancties bestaan. In de tweede plaats wordt gecontroleerd of in het land waar de leverancier is gevestigd een exportcontroleregime bestaat waarin de inachtneming van mensenrechten onderdeel is van de beoordeling voor het verstrekken van een exportvergunning.[229]

Uitstel van het bekendmaken van een onbekende kwetsbaarheid op de voet van artikel 126ffa Sv

Indien politie of justitie – al dan niet binnen het bestek van de uitoefening van de bevoegdheid ex artikel 126nba Sv – op de hoogte komt van een (tot dan toe onbekende) kwetsbaarheid of lek in de beveiliging van hardware of software, wordt dit gemeld bij de producent van die hardware of software met het oog op het beëindigen of dichten daarvan.[230]

In voorkomende gevallen kan echter toepassing worden gegeven aan de procedure van artikel 126ffa Sv.[231] De officier van justitie kan op grond van een zogeheten 'zwaarwegend opsporingsbelang' uitstel bevelen van het bekendmaken van een onbekende kwetsbaarheid

---

227 *Kamerstukken I* 2017/18, 34 372, G (NMvA I), p. 12; *Kamerstukken II* 2017/18, 34 372, nr. 27 (verslag van een schriftelijk overleg), p. 7-8: "*Als de officier van justitie bepaalt dat gebruik van binnendringsoftware van een externe leverancier noodzakelijk is, zal dit centraal in het OM worden getoetst alvorens in die specifieke zaak wordt overgaan tot aanschaf. Daarnaast worden de leveranciers van dergelijke software gescreend door de AIVD en mogen deze leveranciers de software niet verkopen aan dubieuze regimes.*"

228 *Handelingen I* 2017/18, nr. 34, item 5, p. 29.

229 Zie de brief van de minister van Justitie en Veiligheid van 26 juli 2019 in antwoord op Kamervragen van het lid Verhoeven, *Aanhangsel Handelingen II* 2018/19, nr. 3537. Deze toets is nader toegelicht in de brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties en de minister van Justitie en Veiligheid d.d. 23 juni 2022 in antwoord op Kamervragen van de leden Omtzigt en Van Dijk over het gebruik van hacksoftware, zoals Pegasus, in Nederland, *Aanhangsel Handelingen II* 2021/22, nr. 3252, p. 6: "*In het Regeerakkoord 2017-2021 is vastgelegd dat leveranciers van hacksoftware die wordt ingekocht door opsporingsdiensten niet mogen leveren aan dubieuze regimes. Zoals aangegeven in de beantwoording van Kamervragen gaat het om landen die zich schuldig maken aan ernstige schendingen van mensenrechten of internationaal humanitair recht. Om deze reden voert de politie een toets uit voordat over wordt gegaan tot de aanschaf van binnendringsoftware. In deze toets wordt de leverancier gevraagd niet te hebben geleverd aan landen waartegen vanuit de EU of de VN restrictieve sancties bestaan en wordt gecontroleerd of in het land waar de leverancier is gevestigd een exportcontroleregime bestaat waar mensenrechten een onderdeel is in de beoordeling voor het verstrekken van een exportvergunning. De politie past dit beleid toe en eist van leveranciers een bevestiging dat niet aan zulke dubieuze regimes wordt geleverd. Aanvullend hierop wordt door de politie deze toets periodiek herhaald.*"

230 Nota van toelichting op het Bogw, onder 3.3, p. 15; *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 9: "*Uitgangspunt is dat een kwetsbaarheid of lek in de beveiliging van software, dat door politie en justitie wordt aangetroffen, wordt gemeld bij de leverancier met het oog op het beëindigen of dichten daarvan.*" Zie ook: *Kamerstukken I* 2016/17, 34 372, D (MvA I), p. 18 en zie p. 25: "*Net als in de fysieke wereld hebben politie en justitie tot taak de criminaliteit op het internet zoveel mogelijk te voorkómen en op te sporen. Het laten voortbestaan van een onbekende kwetsbaarheid kan een risico inhouden op (meer) slachtoffers van criminaliteit. Kwetsbaarheden die in het kader van een opsporingsonderzoek aan het licht komen, en waarvan aannemelijk is dat ze nog onbekend zijn, worden in beginsel direct of zo spoedig mogelijk gemeld aan de fabrikant van de desbetreffende hard- of software.*" Bovendien: *Kamerstukken I* 2017/18, 34 372, G (NMvA I), p. 4.

231 Dit artikel is in het wetsvoorstel ingevoegd bij amendement van de Kamerleden Recourt en Tellegen, *Kamerstukken II* 2016/17, 34 372, nr. 14, met als toelichting: "*Dit amendement beoogt om de regel dat kwetsbaarheden in geautomatiseerde werken door de officier van justitie moeten worden gemeld sterker in de wet te verankeren. Het uitgangspunt zijn integere en veilige geautomatiseerde werken. De overheid dient dit te bevorderen. Vanwege de risico's die kwetsbaarheden in een geautomatiseerd werk met zich mee brengen, is de regel dat bekende kwetsbaarheden worden gemeld om de eigenaar van dat werk in staat te stellen die kwetsbaarheid te verhelpen. Het voorliggend wetsvoorstel biedt echter de mogelijkheid om op grond van een zwaarwegend opsporingsbelang een kwetsbaarheid niet te melden. Dit amendement regelt dat de officier van justitie het bevel om een kwetsbaarheid niet te melden pas kan geven na een machtiging hiertoe door de rechter-commissaris. Hiermee wordt een onafhankelijke rechterlijke toets in de wet gebracht waarmee voorkomen kan worden dat de officier van justitie mogelijk te gemakkelijk het opsporingsbelang boven de veiligheid van een geautomatiseerd werk laat prevaleren.*"

voor het binnendringen in een geautomatiseerd werk aan de producent.[232] Het afzien van het melden van een onbekende kwetsbaarheid vereist een machtiging daartoe van de rechter-commissaris.[233]
Een zwaarwegend opsporingsbelang doet zich voor wanneer het opsporingsbelang zwaarder weegt dan het maatschappelijk belang om de producent de mogelijkheid te bieden de kwetsbaarheid te verhelpen. Factoren die bij de afweging betrokken kunnen worden zijn:

- of de melding zou resulteren in het tenietdoen van het heimelijke karakter van het opsporingsonderzoek;[234]
- of het een systeem betreft dat door criminelen is vervaardigd en/of vrijwel alleen voor criminele doeleinden wordt gebruikt. Het melden van een onbekende kwetsbaarheid zou in dergelijke gevallen criminaliteit faciliteren;[235]
- hoe groot de kans is dat de kwetsbaarheid door kwaadwillenden wordt uitgebuit;[236]
- hoe groot het aantal onschuldige personen en organisaties is dat kwetsbaar wordt door het achterwege blijven van de melding en
- in hoeverre de desbetreffende hardware of software wordt gebruikt bij de vitale infrastructuur of regulier en wijdverbreid is in de maatschappij.[237]

De afweging om een dergelijke melding uit te stellen overstijgt het individuele opsporingsonderzoek en wordt daarom binnen het OM centraal gemaakt.[238]

De machtiging is tijdelijk. In artikel 126ffa Sv wordt echter geen termijn gesteld aan het uitstel van de melding van een onbekende kwetsbaarheid. Het wordt aan de interactie tussen officier van justitie en rechter-commissaris gelaten om te komen tot nadere inkadering van de periode van geldigheid van het uitstel. Het ligt echter in de rede om voor de periode van uitstel van de melding aan te sluiten bij de periode van geldigheid van de machtiging voor het onderzoek in het geautomatiseerde werk, waarbij het voornemen bestaat gebruik te maken van de betreffende kwetsbaarheid. De bevoegdheid tot het onderzoek in een geautomatiseerd werk is gekoppeld aan een periode van vier weken, daarna kan het bevel telkens met een periode van vier weken worden verlengd.[239]
Een machtiging kan worden verlengd als de melding zou resulteren in het tenietdoen van het heimelijke karakter van het opsporingsonderzoek. Ook kan de onbekende kwetsbaarheid een systeem of computerprogramma betreffen dat door criminelen is vervaardigd en/of vrijwel alleen voor criminele doeleinden wordt gebruikt. Het melden van een onbekende kwetsbaarheid in dergelijke gevallen zou het effect hebben criminaliteit te faciliteren. In dergelijke gevallen

---

232 *Kamerstukken I* 2016/17, 34 372, D (MvA I), p. 18-25; *Kamerstukken II* 2017/18, 34 372, nr. 27 (verslag van een schriftelijk overleg), p. 13-14; *Kamerstukken II* 2018/19, 34 372, nr. 29 (verslag van een schriftelijk overleg), p. 8-9.

233 Deze bepaling geeft geen antwoord op de vraag welke rechter-commissaris bevoegd is om kennis te nemen van de vordering tot het verkrijgen van een machtiging ex art. 126ffa Sv. Dat kan de rechter-commissaris zijn die reeds is benaderd met het oog op een machtiging als bedoeld in art. 126nba lid 4 Sv, maar niet in alle gevallen waarin een onbekende kwetsbaarheid wordt ontdekt is eerder een rechter-commissaris op die voet betrokken. In de op 12 augustus 2021 gepubliceerde (ongedateerde) beschikking van de rechter-commissaris in de rechtbank Den Haag, ECLI:NL:RBDHA:2013:19764, acht de rechter-commissaris zich bevoegd tot kennisneming van de vordering op de grond dat de afweging van officier van justitie om de vordering te richten tot de rechter-commissaris in die rechtbank niet onredelijk of onbegrijpelijk is. De officier van justitie had toegelicht dat hij de vordering bij de Haagse rechter-commissaris had ingediend, omdat de vordering specifieke kennis en expertise bij de rechter-commissaris vereist en dit bij het kabinet van de rechter-commissaris van de rechtbank Den Haag aanwezig is.

234 *Kamerstukken II* 2017/18, 34 372, nr. 27 (verslag van een schriftelijk overleg), p. 13-14.

235 *Kamerstukken II* 2017/18, 34 372, nr. 27 (verslag van een schriftelijk overleg), p. 13-14; *Kamerstukken I* 2016/17, 34 372, D (MvA I), p. 18-19.

236 *Kamerstukken I* 2016/17, 34 372, D (MvA I), p. 23.

237 Zie *Kamerstukken I* 2017/18, 34 372, G (NMvA I), p. 3-9, met name p. 6.

238 *Kamerstukken I* 2016/17, 34 372, D (MvA I), p. 18 en zie p. 23 (waarin wordt gewezen op de noodzaak van coördinatie van het gebruik van onbekende kwetsbaarheden: "*Bij dat team* [het technisch team] *is het overzicht over het gebruik en melden van onbekende kwetsbaarheden.*"); *Kamerstukken II* 2017/18, 34 372, nr. 27 (verslag van een schriftelijk overleg), p. 13-14.

239 *Kamerstukken I* 2016/17, 34 372, D (MvA I), p. 18.

kan langduriger uitstel van de melding aan de fabrikant aan de orde zijn.[240] Het uitstel wordt dan periodiek door de rechter-commissaris getoetst. Het uitstellen van het delen van informatie over aangetroffen onbekende kwetsbaarheden in wijdverbreide en regulier gebruikte hard- of software ligt uiteraard niet in de rede.[241]

Oneigenlijk gebruik door derden, waaronder de leverancier van hacksoftware

Er is een tweede risicofactor verbonden aan het gebruik van commerciële software, zoals spyware, en van onbekende kwetsbaarheden bij het binnendringen, namelijk dat oneigenlijk gebruik van deze software door derden, waaronder de leverancier ervan, niet valt uit te sluiten. Zodra sprake is van een technische kwetsbaarheid in een geautomatiseerd werk bestaat per definitie de kans dat derden van die kwetsbaarheid gebruikmaken. Voor geen enkel systeem dat met internet is verbonden valt bij voorbaat uit te sluiten dat dit wordt binnengedrongen door derden.

Indien de politie bij de inzet van de bevoegdheid gebruikmaakt van een bepaalde kwetsbaarheid, dan neemt de politie maatregelen om te voorkomen dat anderen daarvan tegelijk gebruikmaken, zoals:

- het vooraf analyseren van het geautomatiseerde werk in kwestie;
- het direct na het binnendringen eerst nader analyseren ten behoeve van een verbeterde risico-inschatting;
- het sterk beperken van de tijd van het contact tussen het te onderzoeken systeem en het systeem van de politie, en
- het monitoren van activiteiten van het betrokken deel van het te onderzoeken systeem.

Dergelijke maatregelen zijn niet alleen van belang voor het beperken van de kans dat derden van dezelfde kwetsbaarheid gebruikmaken, maar ook om het risico op onderkenning van de opsporingsactiviteiten te beperken en de integriteit van het bewijs zeker te stellen.[242]

Met het oog op het voorkomen van misbruik door de leverancier heeft de minister onderstreept dat bij het verrichten van onderzoek in een geautomatiseerd werk noch het geïnfecteerde werk, noch de digitale infrastructuur van het technische team in verbinding staat met een server van de leverancier van de hacksoftware.[243]

In dit verband wijst de minister ook op de hierna te bespreken (voorafgaande) keuring van het technisch hulpmiddel waarmee onderzoekshandelingen worden verricht. Hoewel de keuringseis

---

[240] *Kamerstukken I* 2016/17, 34 372, D (MvA I), p. 19 en zie 21: "*In de beantwoording van een eerdere vraag van de leden van de CDA fractie over het opnemen van een maximale termijn is aangegeven dat juist het melden van een onbekende kwetsbaarheid in gevallen het effect zou hebben criminaliteit ongemoeid te laten omdat de opsporing niet kan worden voortgezet.*" Opmerking onderzoekers: daaraan valt toe te voegen dat een onbedoeld en ongewenst leereffect uitgaat van het melden van een onbekende kwetsbaarheid aan de producent van (bijvoorbeeld) malware of van een communicatiesysteem dat specifiek ter ondersteuning van criminaliteit is ontwikkeld. Dit roept de vraag op of art. 126ffa Sv zijn doel niet voorbijschiet door ook in die gevallen het onvermeld laten van de onbekende kwetsbaarheid aan de producent te limiteren.

[241] *Kamerstukken I* 2016/17, 34 372, D (MvA I), p. 19; *Kamerstukken I* 2017/18, 34 372, G (NMvA I), p. 3-9, met name p. 6.

[242] *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 34-35; *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 67-68, 73-74, 93-94; *Kamerstukken I* 2016/17, 34 372, D (MvA I), p. 18.

[243] *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II),
p. 45: "*In het kader van het onderzoek met behulp van een technisch hulpmiddel, een softwareapplicatie, wordt uitsluitend een verbinding tot stand gebracht tussen het binnengedrongen geautomatiseerd werk en de server van de politie. Er wordt geen verbinding tot stand gebracht met de server van de maker van de softwareapplicatie.*"
p. 51: "*Het gebruik van de software tijdens de onderzoeksfase zal dus plaatsvinden zonder dat de politieserver in contact staat met de leverancier van de software.*"
p. 74: "*Het besluit dat ter uitvoering van het wetsvoorstel wordt opgesteld zal technische eisen stellen aan de softwareapplicaties die voor het onderzoek in een geautomatiseerd werk word*[en] *gebruikt, waaronder de eis* [dat] *uitsluitend gegevens worden opgeslagen op de politieserver. De software zal dus niet in contact staan met de server van de leverancier. De leverancier heeft geen mogelijkheid om zelfstandig updates uit te voeren en zelf de controle over het geautomatiseerde werk over te nemen. Evenmin kunnen andere klanten van de leverancier toegang krijgen tot het geautomatiseerde werk.*"
p. 78: "*De leden van de D66-fractie hebben gevraagd of het klopt dat de geïnfecteerde geautomatiseerde werken tevens in verbinding staan met een server van de leverancier van de hacksoftware. Zoals in de beantwoording van een eerdere, soortgelijke vraag van de leden van deze fractie eerder aan de orde is gekomen, is dit niet het geval.*"

geen betrekking heeft op de applicatie waarmee wordt binnengedrongen, vormt ook de keuring van het technisch hulpmiddel naar het oordeel van de minister een mogelijke maatregel om misbruik tegen te gaan. Met de keuring kan worden voorkomen dat softwareapplicaties worden ingezet die niet voldoen aan de daaraan te stellen eisen, bijvoorbeeld versleuteling.

3.8. Het technisch hulpmiddel en de handmatige inzet van de bevoegdheid

Het begrip 'technisch hulpmiddel'

Het verrichten van onderzoekshandelingen in een geautomatiseerd werk met de onderzoeksdoeleinden die in het bevel van de officier van justitie zijn opgenomen, kan weliswaar ook "*ad hoc en handmatig*" worden uitgevoerd, maar vindt bij voorkeur plaats met behulp van een technisch hulpmiddel dat (conform artikel 21 lid 1 Bogw) door een opsporingsambtenaar van een technisch team in een geautomatiseerd werk wordt geplaatst.[244] Een technisch hulpmiddel betreft volgens artikel 1 onder f Bogw:

> "*softwareapplicatie die gegevens detecteert, registreert en transporteert en waarmee onderzoekshandelingen worden verricht ter uitvoering van een bevel*".

Met gegevens 'detecteren' wordt gedoeld op het waarnemen van gegevens in een te onderzoeken geautomatiseerd werk. Een voorbeeld is het lezen van een bestand op de computer van een verdachte.[245] 'Detecteren' betreft dus het vinden van de gegevens waarnaar wordt gezocht.
Van gegevens 'registreren' is sprake als het technisch hulpmiddel de gedetecteerde gegevens overneemt uit het geautomatiseerde werk. Het gaat hier om de inhoud van de gegevens.[246] 'Registreren' behelst dus het maken van een kopie van de gedetecteerde gegevens teneinde die te kunnen vastleggen in een technische infrastructuur van de politie. In gevallen waarbij technische hulpmiddelen worden gebruikt die gegevens extraheren die in de cloud zijn opgeslagen nadat bijvoorbeeld een gebruikersnaam en wachtwoord zijn verkregen, vinden detectie en registratie pas plaats in het technisch hulpmiddel zelf. Een voorbeeld is een technisch hulpmiddel waarmee een mailbox van een verdachte wordt gelezen. Bij de keuring zal worden nagegaan of het technisch hulpmiddel een voorziening bevat om de inhoud van de geregistreerde gegevens zichtbaar te maken.[247]
Het 'transport' van de geregistreerde gegevens vindt – automatisch – plaats vanaf de locatie waar de registratie plaatsvindt over een beveiligde verbinding naar een 'technische infrastructuur', een beveiligde opslaglocatie in beheer van de politie, waarop de gegevens worden vastgelegd.[248]

In de omschrijving "*waarmee onderzoekshandelingen worden verricht ter uitvoering van een bevel*" ligt besloten dat onder het begrip 'technisch hulpmiddel' *niet* de applicatie

---

[244] *Kamerstukken II* 2015/2016, 34 372, nr. 3 (MvT), p. 14, p. 16. Zie ook: *Kamerstukken I* 2016/17, 34 372, D (MvA I), p. 20.
[245] Nota van toelichting op het Bogw, p. 38.
[246] Nota van toelichting op het Bogw, p. 38-39.
[247] Nota van toelichting op het Bogw, p. 38-39. Niet is van belang op welke wijze de metadata worden geregistreerd. Als de in het geautomatiseerde werk gedetecteerde gegevens door het technische hulpmiddel in een ander format worden geregistreerd (een voorbeeld is een sms-bericht dat op een mobiel apparaat in PDU-format is opgeslagen en dat door een technisch hulpmiddel in ASCII-codes wordt geregistreerd), zal na de vastlegging van de gegevens op de technische infrastructuur de omzetting van het format met een applicatie moeten worden uitgelokt.
[248] Art. 13 lid 1 Bogw stelt de eis dat "*een technisch hulpmiddel [...] de geregistreerde gegevens automatisch naar een technische infrastructuur* [transporteert]." Zie bovendien de nota van toelichting op het Bogw, p. 18, 20 en 40. Op het onderwerp van de beveiligde verbinding wordt hieronder nog teruggekomen.

valt die eventueel wordt gebruikt om het geautomatiseerde werk binnen te dringen.[249] De normen die het gebruik van een technisch hulpmiddel omkleden, en dan met name de keuringseisen die aan het technisch hulpmiddel worden gesteld, zien dus uitsluitend op de softwareapplicatie waarmee de onderzoekshandelingen worden verricht *nadat* eenmaal in het geautomatiseerde werk is binnengedrongen.[250] Deze beperking heeft als reden dat de gegevens waarvan de betrouwbaarheid, integriteit en herleidbaarheid moeten worden gewaarborgd, worden vergaard door middel van de onderzoekshandelingen, terwijl het daaraan voorafgaande binnendringen uitsluitend de weg voor het vergaren van gegevens ontsluit en op zichzelf de betrouwbaarheid van die gegevens niet beïnvloedt.[251]

De softwareapplicatie bevat – samengevat – zodanige functionaliteiten dat daarmee gegevens kunnen worden (1) gedetecteerd, (2) geregistreerd en (3) automatisch getransporteerd en dat daarmee (4) onderzoekshandelingen kunnen worden verricht ter uitvoering van een bevel. Gelet op de gekozen bewoordingen is verdedigbaar dat de vier condities die in de omschrijving van het begrip 'technisch hulpmiddel' zijn opgenomen vier *cumulatieve* voorwaarden betreffen.[252]
Dat het begrip 'technisch hulpmiddel' zich niet eenvoudig laat afbakenen ten opzichte van het 'handmatig' (dat wil zeggen: het *zonder* een technisch hulpmiddel) verrichten van onderzoekshandelingen in een geautomatiseerd werk, volgt onder meer uit een passage in de nota van toelichting op het Besluit. Daarin maakt de minister melding van de mogelijkheid dat het technische team bij het verrichten van onderzoekshandelingen in een geautomatiseerd werk gebruikmaakt van een 'script'[253] dat is geschreven door het technische team zelf en dat "*semi-handmatig*" wordt ingezet.[254] De minister gaat ervan uit dat na afloop van de inzet van het 'script' alsnog een keuring daarvan plaatsvindt (tenzij de aard van het hulpmiddel zich naar het oordeel van de officier hiertegen verzet).

---

249 Zie de nota van toelichting op het Bogw, onder 3.5, p. 18: "*De wijze waarop het binnendringen plaatsvindt, bijvoorbeeld de wijze van het omzeilen van de beveiliging van een geautomatiseerd werk, maakt geen deel uit van het keuringsproces. In het geval binnendringsoftware wordt ingekocht wordt het functioneren hiervan in een testomgeving gecontroleerd.*" Zie ook (identiek) de nota van toelichting op het Bogw, onder 3.5, p. 20. Zie bovendien: *Kamerstukken II* 2017/18, 34 372, nr. 27 (verslag van een schriftelijk overleg), met name p. 7-8.

250 Zie de nota van toelichting op het Bogw, p. 28: "*De adviezen van BoF en KPN om niet alleen technische hulpmiddelen die worden gebruikt voor het doen van onderzoek, maar ook hulpmiddelen die worden gebruikt bij het binnendringen te onderwerpen aan een voorafgaande keuring met het oog op het voorkomen van schade van derden, zijn niet overgenomen.*" Zie ook nota van toelichting op het Bogw, p. 33: "*T-mobile is van mening dat het begrip «technisch hulpmiddel» eng wordt gedefinieerd en wijst erop dat bij hacking niet alleen gebruik wordt* [gemaakt] *van «standaard» software en bijbehorende payloads, maar ook van slimheid/scripts/own codes van hackers. In reactie hierop wordt opgemerkt dat onder technisch hulpmiddel uitsluitend de software wordt verstaan die wordt gebruikt voor het verrichten van onderzoekshandelingen. Voor zover er bij het binnendringen in een geautomatiseerd werk gebruik wordt gemaakt van software, wordt deze software niet gekeurd.*"

251 Zie bijvoorbeeld *Kamerstukken II* 2018/19, 34 372, nr. 29 (verslag van een schriftelijk overleg), p. 13: "*Het doel van de keuring van technische hulpmiddelen die worden gebruikt voor het verrichten van onderzoekshandelingen is om te borgen dat de werking van een hulpmiddel dusdanig betrouwbaar is dat de hiermee verkregen onderzoeksgegevens, die kunnen dienen als bewijs in een strafzaak, betrouwbaar, integer en herleidbaar zijn. De wijze waarop het binnendringen in een geautomatiseerd werk plaatsvindt is niet van invloed op de betrouwbaarheid van de onderzoeksgegevens en maakt daarom geen onderdeel uit van het keuringsproces. De kwaliteit van het binnendringen in een geautomatiseerd wordt geborgd door dit handelen voor te behouden aan daartoe opgeleide deskundige opsporingsambtenaren van een technisch team. Het functioneren van de binnendringsoftware wordt in een testomgeving gecontroleerd. In de procedure rondom de inzet van de bevoegdheid wordt aandacht besteed aan de risico's voor het te onderzoeken geautomatiseerd werk, waaronder de schade voor derden.*"

252 Zie ook de nota van toelichting op het Bogw, p. 32: "*Van het verrichten van onderzoekshandelingen zonder technisch hulpmiddel is sprake als geen gebruik wordt gemaakt van software die gegevens detecteert, registreert en transporteert.*"

253 Een 'script' betreft een betrekkelijk klein programmaatje dat meestal is geschreven om veelvoorkomende taken (bijvoorbeeld systeembeheertaken) pragmatisch te automatiseren, of om een langdurige maar eenmalige taak automatisch te verrichten.

254 Nota van toelichting op het Bogw, p. 21.

De softwareapplicatie die in de onderzoeksfase wordt gebruikt kan zijn uitgerust met verschillende functionaliteiten waarmee de in artikel 126nba lid 1 Sv omschreven doelen kunnen worden bereikt. Het bevel van de officier van justitie dient, zoals gezegd, de functionaliteiten te vermelden die – afhankelijk van het doel van het onderzoek – zullen worden ingeschakeld.[255] Dergelijke functionaliteiten zijn bijvoorbeeld het opnemen van geluid, het maken van screenshots, het vastleggen van toetsaanslagen (keylogging) en het doorzoeken van bepaalde bestandsmappen en het vastleggen van gegevens hieruit.[256] De opsporingsambtenaar van het technische team beperkt bij de plaatsing van het technische hulpmiddel in een geautomatiseerd werk de werking van het hulpmiddel tot de in het bevel vermelde functionaliteit(en).[257]

Op een vrijwel identieke wijze als waarop dat is geregeld in het Besluit technische hulpmiddelen strafvordering,[258] bepaalt artikel 22 Bogw dat de toegang tot technische hulpmiddelen centraal wordt geregistreerd.[259] De korpschef wijst één of meer ambtenaren aan die met de registratie zijn belast (lid 1). Na vertoon van het bevel van de officier van justitie met daarin een aanduiding van de aard en functionaliteit van het technisch hulpmiddel verschaft een met registratie belaste ambtenaar toegang tot een technisch hulpmiddel ten behoeve van de plaatsing ervan (lid 2). De toegang tot een technisch hulpmiddel wordt verleend voor de periode die nodig is voor de uitvoering van het bevel (lid 3). De met registratie belaste ambtenaar registreert de aanduiding van het technisch hulpmiddel, het tijdstip van de toegangverlening, de in het bevel vermelde aanduidingen van de aard en functionaliteit van het technisch hulpmiddel, de in het bevel vermelde periode waarbinnen aan het bevel uitvoering moet worden gegeven en de aanduiding van de opsporingsambtenaar die om toegang tot het technisch hulpmiddel verzoekt.[260]

De technische hulpmiddelen waarmee tijdens de onderzoeksfase onderzoekshandelingen in een geautomatiseerd werk worden verricht, kunnen worden betrokken van verschillende producenten of binnen de politieorganisatie zelf worden ontwikkeld, mits aan de wettelijke vereisten voor keuring wordt voldaan.[261]

De technische eisen die aan het technisch hulpmiddel worden gesteld (hoofdstuk 5 Bogw)

Omdat de gegevens die met een technisch hulpmiddel worden vastgelegd kunnen dienen als bewijs in een strafzaak, is het van essentieel belang dat de betrouwbaarheid en integriteit van de gegevens vaststaan, dat de gegevens herleidbaar zijn en dat het technisch hulpmiddel zelf betrouwbaar en integer functioneert.[262] Daartoe worden in de artikelen 8 tot en met 12 Bogw aan een technisch hulpmiddel de volgende technische eisen gesteld:[263]

- *gerichte werking*: een technisch hulpmiddel is zodanig ingericht dat de werking ervan kan

[255] Zie o.a. *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 50: "*Een belangrijke inrichtingseis zal zijn dat de instelling van de software kan worden gedifferentieerd naar het gebruik van verschillende functionaliteiten.*"

[256] *Kamerstukken II* 2015/2016, 34 372, nr. 3 (MvT), p. 35.

[257] Art. 23 lid 2 jo lid 1 Bogw.

[258] Besluit van 20 oktober 2006 tot vaststelling van het Besluit technische hulpmiddelen strafvordering, *Stb.* 2006, 524. Zie met name art. 6 van dit besluit.

[259] Opmerking onderzoekers: Het valt te betwijfelen of een als technisch hulpmiddel aangemerkte softwareapplicatie in dit opzicht gelijkgesteld kan worden aan de technische hulpmiddelen als bedoeld in het Besluit technische hulpmiddelen strafvordering. Software laat zich immers niet altijd goed vergelijken met, bijvoorbeeld, een handzaam apparaat.

[260] Nota van toelichting op het Bogw, p. 45-46.

[261] *Kamerstukken I* 2016/17, 34 372, D (MvA I), p. 24.

[262] De nota van toelichting op het Bogw, p. 18 en p. 37. Zie ook de nota van toelichting op Regeling eisen keuringsdienst technisch hulpmiddel, waarnaar hierna nog wordt verwezen, *Stcrt.* 2019, 10713, p. 4.

[263] Zie de nota van toelichting op het Bogw, p. 37-40. Zie ook *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 31.

worden beperkt tot de in het bevel vermelde functionaliteit(en);[264]

- *gerichte detectie en registratie*: een technisch hulpmiddel detecteert en registreert uitsluitend gegevens ten behoeve van de in het bevel vermelde functionaliteit(en).[265] Een technisch hulpmiddel dat een functionaliteit of functionaliteiten bevat ten behoeve van het opnemen van telecommunicatie detecteert en registreert uitsluitend de communicatie die plaatsvindt met gebruikmaking van één of meer identificerende kenmerken van het geautomatiseerde werk van de individuele gebruiker of gebruikers op wie het bevel betrekking heeft;[266]
- *betrouwbaarheid en integriteit*: een technisch hulpmiddel registreert gegevens op zodanige wijze dat de inhoud van de geregistreerde gegevens identiek is aan de inhoud van de gedetecteerde gegevens.[267] Een technisch hulpmiddel is beveiligd tegen wijziging van de werking hiervan, tegen wijziging van de geregistreerde gegevens en tegen kennisneming van de geregistreerde gegevens door onbevoegden;[268]
- *herleidbaarheid*: een technisch hulpmiddel voorziet de geregistreerde gegevens van een uniek gegeven. Dit is om te waarborgen dat de gegevens afkomstig zijn van het technisch hulpmiddel. Uit dit unieke gegeven moet de relatie met het geplaatste technisch hulpmiddel blijken. Hierbij kan worden gedacht aan een code die bij de plaatsing aan het technisch hulpmiddel is toegevoegd. De technische infrastructuur moet in staat zijn om bij de vastlegging van de geregistreerde gegevens het unieke gegeven te herkennen. Op deze wijze kan een herleidbaar gegevensspoor worden gecreëerd;[269]
- *datum en tijd*: een technisch hulpmiddel voorziet de geregistreerde gegevens van de datum en tijd waarop de registratie plaatsvindt.[270]

---

[264] Art. 8 Bogw. Zie de nota van toelichting op het Bogw, p. 37: "*Softwareapplicaties met behulp waarvan onderzoekshandelingen in een geautomatiseerd werk worden verricht beschikken naar hun aard vaak over verschillende functionaliteiten. Om te waarborgen dat de onderzoekshandelingen binnen de grenzen van het bevel van de officier van justitie worden verricht, bepaalt artikel 8 van het besluit dat een technisch hulpmiddel zodanig is ingericht dat de werking ervan kan worden beperkt tot de in het bevel vermelde functionaliteit of functionaliteiten. Hierbij kan worden gedacht aan functionaliteiten als het opnemen van geluid, het maken van screenshots, het vastleggen van toetsaanslagen of het doorzoeken van bepaalde bestandsmappen en het vastleggen van gegevens hieruit. Bij de keuring wordt getoetst of een technisch hulpmiddel instellingen bevat waarmee de werking van een technisch hulpmiddel kan worden beperkt tot een bepaalde functionaliteit of tot bepaalde functionaliteiten.*"

[265] Art. 9 lid 1 Bogw. Zie de nota van toelichting op het Bogw, p. 38: "*De in artikel 9, eerste lid, gestelde eis ligt in het verlengde van artikel 8. Een technisch hulpmiddel moet in staat zijn uitsluitend gegevens te detecteren en te registreren ten behoeve van de in het bevel vermelde functionaliteit of functionaliteiten. De NVvR heeft in haar advies opgemerkt dat deze eis in combinatie* [met] *de artikelen 8 en 22* [lees: 23] *overbodig lijkt en kan worden geschrapt dan wel nader toegelicht zou moeten worden. De artikelen 8, 9, eerste lid, en 22* [lees: 23] *zijn complementair. De artikelen 8 en 9 hebben betrekking op de technische eisen voor de keuring van het technische hulpmiddel. Artikel 8 ziet op de inrichting van het technische hulpmiddel, artikel 9 op de werking van het technische hulpmiddel. En in artikel 22* [lees: 23] *worden eisen gesteld aan de plaatsing door een opsporingsambtenaar van een technisch hulpmiddel.*"

[266] Art. 9 lid 2 Bogw. Zie de nota van toelichting op het Bogw, p. 39: "*Een technisch hulpmiddel mag uitsluitend de communicatie die plaatsvindt met gebruikmaking van één of meer identificerende kenmerken van het geautomatiseerde werk van de individuele gebruiker of gebruikers op wie het bevel betrekking heeft registreren.*"

[267] Art. 10 lid 1 Bogw.

[268] Art. 10 lid 2 Bogw. Zie de nota van toelichting op het Bogw, p. 39: "*Hierbij dient te worden opgemerkt dat in de ICT nooit volledige garanties tegen beïnvloeding van buitenaf kunnen worden gegeven. Wel kan die beïnvloeding zo moeilijk mogelijk worden gemaakt. Bij de keuring wordt getoetst of er beveiligingsmaatregelen aanwezig zijn die beïnvloeding van een technisch hulpmiddel van buitenaf naar de stand van de techniek zo goed mogelijk tegengaan. Hierbij kan worden gedacht aan het aanwezig zijn van authenticatiemaatregelen voor de communicatie met het technische hulpmiddel.*"

[269] Art. 11 Bogw. Zie de nota van toelichting op het Bogw, p. 39.

[270] Art. 12 Bogw. Zie de nota van toelichting op het Bogw, p. 39: "*Hierdoor wordt inzichtelijk op welk moment een onderzoekshandeling heeft plaatsgevonden. De eis van datum- en tijdregistratie betekent niet dat er doorlopend datum- en tijdregistratie moet plaatsvinden gedurende de inzet van een technisch hulpmiddel. Artikel 12 staat er niet aan de in de weg dat een technisch hulpmiddel uitsluitend gegevens registreert als er gegevens van het te onderzoeken geautomatiseerde werk worden ontvangen. De strekking van de eis is dat zodra er gegevens worden geregistreerd door een technisch hulpmiddel er zekerheid bestaat over de datum en het tijdstip van de gegevensregistratie door het technische hulpmiddel.*"

Het transport van de geregistreerde gegevens naar de technische infrastructuur

Artikel 13 Bogw schrijft voor (1) dat het technisch hulpmiddel de geregistreerde gegevens automatisch transporteert naar een technische infrastructuur en (2) dat dit technisch hulpmiddel de geregistreerde gegevens tijdens het transport naar een technische infrastructuur beveiligt tegen wijziging van de geregistreerde gegevens en kennisneming van de geregistreerde gegevens door onbevoegden. Aangenomen mag worden dat deze beveiligingseisen ook gelden indien het technische team voor het transport van de geregistreerde gegevens naar de opslaglocatie geen gebruik maakt van een technisch hulpmiddel.[271]

Het transport van de signalen vanuit het geautomatiseerde werk naar de server van de politie vindt plaats over een beveiligde verbinding, waarbij de gegevens worden versleuteld op een wijze die met de thans beschikbare technieken niet of nauwelijks is te kraken.[272] De gegevens worden onverwijld naar de politieserver gezonden en automatisch voorzien van een hashcode,[273] zodat de gegevens daarna niet kunnen worden gewijzigd zonder dat dit zichtbaar is.[274]

De voorafgaande keuring van het technisch hulpmiddel (hoofdstuk 6 Bogw)

Uitgangspunt van het Bogw is dat alleen technische hulpmiddelen worden gebruikt die voorafgaand aan het gebruik ervan zijn goedgekeurd. Daaraan liggen drie redenen ten grondslag:

1. Door goedkeuring van een technisch hulpmiddel staat voorafgaand aan het gebruik ervan vast dat het hulpmiddel voldoet aan de technische eisen van de artikelen 8 tot en met 13 Bogw. Daarmee is geborgd dat de werking van een technisch hulpmiddel dusdanig betrouwbaar is dat de daarmee verkregen gegevens, die kunnen dienen als bewijs in een strafzaak, betrouwbaar, integer en herleidbaar zijn.[275]
2. Ter afscherming van gevoelige opsporingsmethoden hoeven de werking en specificaties van een goedgekeurd technisch hulpmiddel niet te worden prijsgegeven omdat in het proces-verbaal van de inzet kan worden volstaan met een verwijzing naar het referentienummer in het keuringsrapport.
3. Keuring kan bijdragen aan het beperken van misbruik door derden.

---

[271] Zie de nota van toelichting op het Bogw, p. 20: "*De gegevens die bij het verrichten van onderzoekshandelingen, al dan niet met een technisch hulpmiddel worden verkregen dienen automatisch (…) te worden vastgelegd op een technische infrastructuur van een technisch team. (…).*"

[272] Zie *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 109-110; de nota van toelichting op het Bogw, p. 40; *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 50. Daarvoor kan bij de huidige stand van de techniek worden gedacht aan een versleuteling met een cryptografische sterkte van ten minste de *Advanced Encryption Standard* (AES) met een cryptografische sleutel ter grootte van 256 bits, aldus de minister. Zie *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 110.

[273] Een 'hashcode' wordt ook wel genoemd: 'hash' of 'hashwaarde'. De hashcode staat bovendien bekend als '(unieke) digitale vingerafdruk', en is tevens het controlegetal dat onderdeel is van een digitale handtekening ('signing').
De hashcode bestaat uit een reeks van tekens (letters en/of cijfers) die resulteert na de toepassing van een bepaald (cryptografisch) hash-algoritme op een bestand of op een gegevensblok. Voorbeelden zijn het SHA-1-algoritme en een van de SHA-2-algoritmen. Als twee bestanden of gegevensblokken dezelfde hashcode hebben dan zijn die twee bestanden of gegevensblokken hoogstwaarschijnlijk identiek aan elkaar. Elke wijziging in een bestand of gegevensblok zal met een uiterst hoge mate van waarschijnlijkheid een andere hashcode opleveren.
'Hashing' garandeert de integriteit (de ongewijzigde inhoud) van een bepaald bestand of gegevensblok. De toevoeging van een digitale handtekening ('signing') garandeert tevens de authenticiteit (de gepretendeerde herkomst) van een bestand of gegevensblok.

[274] *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 109-110.

[275] Art. 14 lid 1 en lid 2 Bogw en de nota van toelichting op het Bogw, p. 40-41 en op p. 21: "*Ter uitvoering van een bevel van de officier van justitie wordt in beginsel steeds gebruik gemaakt van een vooraf goedgekeurd technisch hulpmiddel.*" Zie ook: *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 14 en p. 110; *Kamerstukken I* 2017/18, 34 372, G (NMvA I), p. 14, p. 15; *Kamerstukken II* 2018/19, 34 372, nr. 29 (verslag van een schriftelijk overleg), p. 17 en p. 13 (citaat): "*Voor de toelating van het bewijs in een strafzaak zijn de betrouwbaarheid, integriteit en herleidbaarheid van met een technisch hulpmiddel vergaarde onderzoeksgegevens cruciaal. In de praktijk zal daarom niet lichtzinnig van het gebruik van een vooraf goedgekeurd hulpmiddel worden afgezien.*" Zie bovendien de nota van toelichting op Regeling eisen keuringsdienst technisch hulpmiddel, *Stcrt.* 2019, 10713, p. 4.

(Ad 1). Een technisch hulpmiddel wordt uitsluitend goedgekeurd als het voldoet aan de eisen van de artikelen 8 tot en met 13 Bogw. De keuring van een technisch hulpmiddel richt zich op (a) de betrouwbaarheid en integriteit van de uitvoering van de met dat middel verrichte onderzoekshandelingen, en (b) de betrouwbaarheid, integriteit en herleidbaarheid van de zodoende verkregen gegevens.[276] Bij goedkeuring mag ervan worden uitgegaan dat aan de wettelijke eisen omtrent de betrouwbaarheid, integriteit en herleidbaarheid van de gegevens is voldaan.[277]
De keuring strekt zich uit tot het transport van de gegevens naar de opslaglocatie. De technische infrastructuur waarop de vastlegging van met een technisch hulpmiddel geregistreerde gegevens plaatsvindt wordt niet gekeurd.[278]
Ingeval het technisch hulpmiddel bij de keuring niet blijkt te voldoen aan alle technische eisen die in het Bogw aan dat hulpmiddel worden gesteld, is het mogelijk om te voldoen aan een of meer technische eisen via 'vervangende (procedurele) waarborgen'. Een voorbeeld betreft het ontbreken van een technisch geborgde datum-tijdfunctie. Dat kan worden opgelost door in een keuringsrapport vervangende procedurele waarborgen verplicht te stellen, waardoor materieel aan de technische eisen kan worden voldaan.[279]

(Ad 2). De keuringsdienst legt ingevolge artikel 18 lid 2 Bogw de resultaten van de keuring vast in een keuringsrapport.[280] Indien een technisch hulpmiddel is goedgekeurd, wordt het voorzien van een keuringsnummer c.q. referentienummer.[281] In dat geval kan in het proces-verbaal van de inzet worden volstaan met een verwijzing naar dit keuringsnummer/referentienummer, waardoor de samenstelling en de werking van het hulpmiddel kunnen worden afgeschermd met het oog op de bescherming van opsporingsbelangen.[282]

(Ad 3). Omtrent het belang van de (voorafgaande) keuring van het technisch hulpmiddel heeft de minister in reactie op het advies van de Raad van State, onder verwijzing naar een advies van de ideële organisatie Bits of Freedom (BoF), opgemerkt dat de ervaringen met bepaalde softwareapplicaties in andere landen het belang van een zorgvuldige keuring onderstrepen. Het gaat hier bijvoorbeeld om ervaringen in Duitsland met *surveillance software* als FinFisher. Zowel in Duitsland als in Frankrijk zou zijn afgezien van de aanwending

---

276 Nota van toelichting op het Bogw, p. 37-40.
277 Nota van toelichting op het Bogw, onder 3.5, p. 18-20.
278 Nota van toelichting op het Bogw, p. 40.
279 Art. 18 lid 3, aanhef en onder e, Bogw: "*Het keuringsrapport van een goedgekeurd technisch hulpmiddel vermeldt ten minste (…) e. relevante verplichte vervangende waarborgen waarmee voldaan kan worden aan één of meer eisen, bedoeld in de artikelen 8 tot en met 13*". Zie tevens de nota van toelichting op het Bogw, p. 43, waar in dit verband wordt gesproken over "*vervangende procedurele waarborgen*".
280 Dit rapport vermeldt volgens artikel 18 lid 3 Bogw ten minste (a) dat het technische hulpmiddel voldoet aan de artikel 8 tot en met 13 Bogw gestelde eisen, (b) een referentienummer, (c) een omschrijving van de werking van het technische hulpmiddel, (d) een aanduiding van de functionaliteit of functionaliteiten van het technische hulpmiddel, (e) relevante verplichte vervangende waarborgen waarmee voldaan kan worden aan één of meer eisen, bedoeld in de artikelen 8 tot en met 13 Bogw, (f) relevante informatie met betrekking tot de werking van een functionaliteit of functionaliteiten van het technische hulpmiddel, en (g) de periode waarvoor de keuring geldt, zolang de werking van het technische hulpmiddel ongewijzigd is.
Na afloop van de in het keuringsrapport genoemde periode kan de keuringsdienst besluiten het technische hulpmiddel opnieuw te keuren of de periode waarvoor de keuring geldt te verlengen. Zie de nota van toelichting op het Bogw, p. 43.
281 Het Bogw spreekt in dit verband van een 'referentienummer' (art. 18 lid 3 onder b Bogw), en zo ook op p. 20 van de nota van toelichting op het Bogw. In de nota van toelichting op het Bogw, p. 22, 28 en 43, wordt het referentienummer vervolgens telkens 'keuringsnummer' genoemd, in een enkel geval onder verwijzing naar art. 18 lid 3 onder b Bogw.
282 Nota van toelichting op het Bogw, p. 20, 22, 28 en 43; *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 110: "*Zodra de keuringsdienst een technisch hulpmiddel heeft goedgekeurd wordt aan de voorziening een referentienummer gekoppeld. Dit referentienummer kan gedurende het verdere verloop van het opsporingsonderzoek worden gebruikt om het desbetreffende hulpmiddel aan te duiden in het proces-verbaal. (…). Zo kan worden gewaarborgd dat de specificaties van technische hulpmiddelen niet worden prijsgegeven. Dit is van groot belang voor de afscherming van gevoelige opsporingsmethoden.*" Zie ook de nota van toelichting op Regeling eisen keuringsdienst technisch hulpmiddel, *Stcrt.* 2019, 10713, p. 4.

van dergelijke spyware, omdat oneigenlijk gebruik door derden, waaronder de leveranciers, en door de politie niet viel uit te sluiten.[283]

De keuring van technische hulpmiddelen wordt volgens artikel 16 lid 1 Bogw opgedragen aan een onderdeel van de landelijke eenheid van de Nationale politie, thans de keuringsdienst van de dienst specialistische operaties (DSO).[284] De keuringsdienst dient een onafhankelijk en objectief oordeel te geven over de ter keuring aangeboden technische hulpmiddelen.
Artikel 16 lid 2 Bogw geeft de minister de mogelijkheid om een andere organisatie aan te wijzen als keuringsdienst. Indien de minister voornemens is om van deze mogelijkheid gebruik te maken worden hierover ingevolge artikel 16 lid 4 Bogw bij ministeriële regeling regels gesteld. Een dergelijke regeling heeft de minister inderdaad opgesteld: de Regeling eisen keuringsdienst technisch hulpmiddel.[285] Daarin zijn de aan een keuringsdienst gestelde eisen neergelegd.[286]
Omdat de landelijke eenheid niet beschikte over voldoende capaciteit en expertise, heeft de minister de Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO) tot 1 maart 2022 aangewezen als keuringsdienst voor het uitvoeren van keuringen van technische hulpmiddelen.[287]
De keuring van technische hulpmiddelen wordt uitgevoerd op basis van een keuringsprotocol waarin wordt vastgelegd op welke wijze de keuring plaatsvindt. Daarnaast kunnen in het keuringsprotocol de criteria worden opgenomen die bij de keuring worden gehanteerd. In het keuringsprotocol van de keuringsinstantie wordt vastgelegd aan welke eisen software moet voldoen om door de keuring te kunnen komen. Een onderdeel daarvan is dat altijd helder moet zijn welke cryptografische algoritmes gebruikt worden, zodat daarop ook getoetst kan worden. In het keuringsprotocol wordt aangegeven dat de leverancier de toegepaste cryptografische algoritmes en sleutels aan de keuringsdienst kenbaar moet maken. Inzicht hierin is van belang om de werking van het technisch hulpmiddel te waarborgen en de betrouwbaarheid, integriteit en herleidbaarheid te garanderen van het bewijsmateriaal dat hiermee wordt verzameld.[288]
Het keuringsprotocol wordt door de keuringsdienst opgesteld in samenspraak met het OM.[289] Een keuringsprotocol behoeft voorafgaande goedkeuring van de minister.[290]

Artikel 14 lid 3 Bogw schrijft de voorafgaande *her*keuring van (een onderdeel van) het technisch hulpmiddel voor ingeval een technisch hulpmiddel (of een onderdeel hiervan) zodanig wijzigt dat redelijkerwijs kan worden aangenomen dat de werking niet langer

---

283 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 34-35.

284 Zie ook de nota van toelichting op het Bogw, onder II, artikelsgewijze toelichting, artt. 16 tot en met 19, p. 42-43. De dienst specialistische operaties (DSO) was voorheen geheten: de dienst landelijke operationele samenwerking (DLOS). In de nota van toelichting op het Bogw wordt nog naar de DLOS verwezen. Overigens is het geldende Besluit beheer politie, *Stb.* 2015, 223, nog niet aan deze en andere naamswijzigingen aangepast.

285 Voluit: Regeling van de Minister van Justitie en Veiligheid van 15 februari 2019, nr. 2433978, houdende regels voor de aanwijzing van een keuringsdienst voor het keuren van technische hulpmiddelen waarmee onderzoekshandelingen worden verricht in een geautomatiseerd werk, *Stcrt.* 2019, 10713, in werking getreden op 1 maart 2019 en vervallen op 1 maart 2022.

286 Een van de eisen die in deze ministeriële regeling aan de keuringsdienst worden gesteld is bijvoorbeeld dat de keuringsdienst in staat is een voorafgaande keuring als bedoeld in art. 14 lid 1 Bogw binnen vier weken na aanbieding van het technische hulpmiddel uit te voeren (art. 6 onder a).

287 Besluit van de Minister van Justitie en Veiligheid van 11 maart 2019, nr. 2504668, houdende aanwijzing van de Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek TNO als keuringsdienst van het Ministerie van Justitie en Veiligheid (Aanwijzingsbesluit TNO als keuringsdienst van het Ministerie van Justitie en Veiligheid), *Stcrt.* 2019, 15022. Dit besluit is op 1 maart 2022 vervallen.

288 *Kamerstukken II* 2018/19, 34 372, nr. 29 (verslag van een schriftelijk overleg), p. 12.

289 Volgens de redactie van art. 17 lid 1 Bogw wordt de wijze van keuring door "*een keuringsdienst*" vastgelegd in een keuringsprotocol. Volgens de artikelsgewijze toelichting op het Bogw, p. 42, echter wordt het keuringsprotocol "*in samenspraak tussen de keuringsdienst en het openbaar ministerie opgesteld*." De hoofdtekst beoogt te laveren tussen deze twee niet geheel overeenstemmende richtsnoeren.

290 Art. 17 Bogw. Meer hierover: nota van toelichting op het Bogw, p. 42-43.

voldoet aan de in de artikelen 8 tot en met 13 Bogw gestelde eisen. Wanneer er een update van de software plaatsvindt, zal bij de keuringsinstantie een inschatting worden gemaakt of redelijkerwijs kan worden aangenomen dat het technisch hulpmiddel nog aan de technische eisen voldoet. Dit gebeurt mede op basis van de notificatie die de update begeleidt waarin de impact van de update wordt vermeld. Dit kan variëren van een toevoeging van een bepaalde taal waarin de software verkrijgbaar is tot een aanpassing van de functionaliteiten. Zo nodig wordt het technische hulpmiddel opnieuw gekeurd.[291]

De onafhankelijke rechterlijke toetsing van de toepassing van het technisch hulpmiddel en het hiermee verkregen bewijsmateriaal biedt voldoende waarborgen voor effectieve controle in een concrete zaak, aldus de minister. Indien er tijdens de behandeling van een strafzaak niettemin twijfel zou rijzen over de betrouwbaarheid en de integriteit van het tijdens het onderzoek vergaarde bewijsmateriaal, kan de zittingsrechter de volledige informatie opvragen of een deskundige raadplegen.[292] Met andere woorden, zo begrijpen de onderzoekers, het is uiteindelijk de rechter (en niet de keuringsinstantie) die oordeelt over de bruikbaarheid van het bewijsmateriaal. Personen die de keuring uitvoeren moeten in staat zijn om ter terechtzitting uitleg te geven over de verrichte werkzaamheden.[293]

Uitzondering op de hoofdregel (1): keuring achteraf

De artikelen 15 lid 1 en 21 lid 2 Bogw voorzien in een grondslag om de vereiste voorafgaande keuring van het technisch hulpmiddel achterwege te laten. De officier van justitie kan toestemming geven de voorafgaande keuring achterwege te laten "*indien het onderzoeksbelang dit dringend vordert.*" In dat geval vermeldt de officier van justitie in het bevel dat toepassing is gegeven aan artikel 21 lid 2 Bogw.
Over deze (eerste) uitzondering op de hoofdregel van voorafgaande keuring vermeldt de nota van toelichting (in een passage waarnaar hierboven al is verwezen) het volgende:

> *"Een uitzondering op deze hoofdregel is mogelijk als het onderzoeksbelang dringend vordert dat gebruik wordt gemaakt van een hulpmiddel dat zich naar zijn aard niet leent voor voorafgaande goedkeuring. Hierbij kan worden gedacht aan op maat gemaakte software, zoals een script dat is geschreven door een technisch team en dat «semi-handmatig» wordt ingezet."*[294]

Ook kan hierbij worden gedacht aan de situatie dat (her)keuring voorafgaand aan de inzet te veel tijd zou vergen.[295]
De officier van justitie zal bij zijn afweging hierover in overleg met de keuringsinstantie nagaan of het technisch hulpmiddel naar verwachting zal voldoen aan de technische eisen die in de artikelen 8 tot en met 13 Bogw worden gesteld.[296]
Na afloop van het gebruik van het technisch hulpmiddel *kan* de (her)keuring alsnog plaatsvinden, aldus bepaalt artikel 15 lid 1 Bogw.[297] Hoewel artikel 15 lid 1 Bogw de (her)

---

[291] Nota van toelichting op het Bogw, p. 43.
[292] Nota van toelichting op het Bogw, p. 28-29.
[293] *Kamerstukken II* 2018/19, 34 372, nr. 29 (verslag van een schriftelijk overleg), p. 12.
[294] Nota van toelichting op het Bogw, p. 21.
[295] Nota van toelichting op het Bogw, p. 44.
[296] Nota van toelichting op het Bogw, p. 42 en p. 44. Zie ook *Kamerstukken II* 2018/19, 34 372, nr. 29 (verslag van een schriftelijk overleg), p. 13: "*Voor de toelating van het bewijs in een strafzaak zijn de betrouwbaarheid, integriteit en herleidbaarheid van met een technisch hulpmiddel vergaarde onderzoeksgegevens cruciaal. In de praktijk zal daarom niet lichtzinnig van het gebruik van een vooraf goedgekeurd hulpmiddel worden afgezien. Bij deze afweging zal de officier van justitie in overleg met de politie nagaan of het beoogde technische hulpmiddel naar verwachting zal voldoen aan de in het besluit gestelde technische eisen. Via de logging wordt controle uitgeoefend op de verrichte onderzoekshandelingen. Indien de situatie zich voor zou doen dat een reeds ingezet hulpmiddel toch achteraf wordt afgekeurd, dan wordt dit voorgelegd aan de rechter in de strafzaak, die beslist over het gebruik van de gegevens als bewijs.*"
[297] Er is in het Bogw overigens geen termijn gesteld waarbinnen het technisch hulpmiddel achteraf aan de keuringsdienst ter keuring moet worden aangeboden.

keuring achteraf in facultatieve termen ('kan') onder woorden heeft gebracht (er staat dus niet dat (her)keuring achteraf 'moet' plaatsvinden), maakt de nota van toelichting op het Bogw duidelijk dat de officier van justitie zonder meer gehouden is het technisch hulpmiddel achteraf ter (her)keuring aan te bieden, behoudens indien zich het geval voordoet van de hieronder te bespreken uitzondering (2).[298]
De officier van justitie vermeldt de uitkomst van de (her)keuring in de processtukken (artikel 21 lid 3 Bogw).
Buiten het geval waarin uitzondering (2) van toepassing is en geheel wordt afgezien van de keuring, schrijft het Bogw niet voor dat (aanvullende) waarborgen worden getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de met het technisch hulpmiddel vastgelegde gegevens te garanderen in de situatie waarin het technisch hulpmiddel achteraf wél ter (her)keuring is aangeboden, maar de keuringsinstantie het technisch hulpmiddel niet (alsnog) heeft goedgekeurd. In dit verband verdient opmerking dat ingeval bij het verrichten van onderzoekshandelingen geen gebruik is gemaakt van een (hetzij vooraf, hetzij achteraf) goedgekeurd technisch hulpmiddel, de keuringsinstantie niet heeft vastgesteld dat het technisch hulpmiddel voldoet aan de technische eisen van de artikelen 8 tot en met 13 Bogw. De ratio van artikel 21 Bogw dicteert dan dat aanvullende waarborgen worden getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de met het technisch hulpmiddel vastgelegde gegevens te garanderen.[299]

Uitzondering op de hoofdregel (2): achterwege laten van keuring

Krachtens de artikelen 15 lid 2 en 21 lid 4 Bogw kan de officier van justitie afwijken van de voorschriften van de artikelen 15 lid 1 en 21 lid 3 Bogw. Indien de officier van justitie heeft bepaald dat "*het onderzoeksbelang dringend vordert*"[300] dat een niet-gekeurd technisch hulpmiddel wordt gebruikt, kan hij bovendien bepalen dat de keuring na afloop van het gebruik van het technisch hulpmiddel, en dus in haar geheel, achterwege blijft "*indien de aard van het technisch hulpmiddel zich naar het oordeel van de officier van justitie* […] *verzet*" tegen keuring (achteraf).[301] De minister merkte hierover op:

> "*Van deze uitzondering zal in de praktijk niet lichtzinnig gebruik worden gemaakt. Hierbij kan worden gedacht aan de situatie van een speciaal op maat gemaakt technisch hulpmiddel. Wanneer het technische hulpmiddel specifiek is aangepast aan de omgeving waarin de inzet heeft plaatsgevonden, kan het problematisch zijn om bij een keuring dezelfde situatie*

---

298 Nota van toelichting op het Bogw, p. 41-42, p. 44-45.

299 Dienovereenkomstig luidt een passage in de nota van toelichting op het Bogw, p. 22 (waarin géén uitzondering wordt gemaakt voor technische hulpmiddelen die achteraf ter keuring zijn aangeboden, maar die niet zijn goedgekeurd): "*Indien de onderzoekshandelingen zonder (goedgekeurd) technisch hulpmiddel zijn verricht, vermeldt de officier van justitie in de processtukken welke procedurele waarborgen zijn getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de vastgelegde gegevens te kunnen garanderen.*"
Zie ook *Kamerstukken I* 2017/18, 34 372, G (NMvA I), p. 15: "*Indien een technisch hulpmiddel na afloop van de inzet ervan ter keuring wordt aangeboden en niet wordt goedgekeurd, dan betekent dit dat niet is voldaan aan de wettelijke eisen omtrent betrouwbaarheid, integriteit en herleidbaarheid van de met het technische hulpmiddel vastgelegde gegevens. Het is dan aan de officier van justitie om te bepalen in hoeverre de gegevens voldoende betrouwbaar, integer en herleidbaar zijn voor het gebruik in een strafzaak. De kans dat de gegevens niet kunnen worden gebruikt als bewijsmateriaal is dan, mede afhankelijk van de reden van afkeuring, reëel. Als de officier besluit om de gegevens toch te gebruiken als bewijs in een strafzaak, dient hij maatregelen te treffen om rechterlijke controle op de rechtmatigheid van de inzet en de betrouwbaarheid, integriteit en herleidbaarheid van de vastgelegde gegevens mogelijk te maken.*"

300 Bij toepassing van art. 21 lid 4 Bogw wordt (alleen) afgeweken van art. 21 lid 3 Bogw en mag keuring of herkeuring na afloop van het gebruik achterwege blijven. Met toepassing van art. 21 lid 4 Bogw wordt echter niet afgeweken van het voorschrift van art. 21 lid 2 Bogw, te weten dat de officier van justitie kan bepalen dat "*indien het onderzoeksbelang dit dringend vordert*" een niet-gekeurd technisch hulpmiddel wordt gebruikt. In dat geval dient de officier van justitie in het bevel dus toch nog wel te vermelden dat toepassing is gegeven aan art. 21 lid 2 Bogw.

301 Bij toepassing van art. 21 lid 4 Bogw zal in het bevel – op grond van art. 21 lid 2 Bogw – (moeten) worden vermeld *dat* voor het onderzoek in een geautomatiseerd werk gebruik wordt gemaakt van een niet-gekeurd technisch hulpmiddel, althans dat toepassing wordt gegeven aan art. 21 lid 2 Bogw. In art. 21 lid 4 Bogw wordt immers uitsluitend afgeweken van het uitgangspunt van keuring na afloop en de vermelding van de uitkomst daarvan in de processtukken.

na te bootsen. Met name bij op maat gemaakte software die tijdens het verrichten van onderzoekshandelingen nog moet worden aangepast aan de omstandigheden, kan het onuitvoerbaar zijn om de omstandigheden waarbinnen de inzet plaats heeft gevonden te reproduceren en het ingezette technische hulpmiddel daarop te keuren."[302]

Doordat de keuring van het technisch hulpmiddel geheel achterwege blijft, wordt de keuringsdienst niet in staat gesteld te onderzoeken of het technisch hulpmiddel voldoet aan de technische eisen van de artikelen 8 tot en met 13 Bogw. Daaruit kan echter niet worden begrepen dat het technisch hulpmiddel niet (meer) aan die technische eisen zou behoeven te voldoen.
Indien de keuring of herkeuring van het technisch hulpmiddel geheel achterwege blijft, vermeldt de officier van justitie in de processtukken dat toepassing is gegeven aan artikel 21 lid 4 Bogw. Tevens vermeldt hij welke 'aanvullende waarborgen' zijn getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de met het technisch hulpmiddel vastgelegde gegevens te garanderen.[303]
Het Bogw schrijft niet voor op welk moment of binnen welke termijn de officier van justitie moet beslissen of de (her)keuring geheel achterwege blijft. Noch is een termijn gesteld waarbinnen de vermelding van die beslissing en van de getroffen aanvullende waarborgen in de processtukken moet worden opgenomen.

De vraag is wat onder 'aanvullende waarborgen' moet worden verstaan. In de toelichting op artikel 21 Bogw, dat zowel betrekking heeft op de inzet van een niet-gekeurd technisch hulpmiddel als op een handmatige inzet, merkt de minister hierover het volgende op:

"Hierbij kan worden gedacht aan een uitgebreide omschrijving van de functionele specificaties van [een] op maat gemaakt technisch hulpmiddel, het voegen van een digitale kopie van de software en de broncode bij het proces-verbaal, het vooraf en achteraf maken van een forensische kopie of het audiovisueel vastleggen van de uitvoering van de onderzoekshandelingen. De aanvullende procedurele eisen van de officier van justitie kunnen de rechtmatigheid van de inzet waarborgen en voorkomen dat er twijfel ontstaat over de betrouwbaarheid, integriteit en herleidbaarheid van de vastgelegde gegevens."[304]

Ook bij een niet-gekeurd technisch hulpmiddel gelden de eisen van logging en van het vastleggen van gegevens op een technische infrastructuur die voldoet aan de in het Bogw gestelde eisen.[305] Via de logging wordt controle uitgeoefend op de verrichte onderzoekshandelingen. Indien de situatie zich zou voordoen dat een reeds ingezet hulpmiddel toch achteraf wordt afgekeurd, dan wordt dit voorgelegd aan de rechter in de strafzaak, die beslist over het gebruik van de gegevens als bewijs.[306]

De verwijdering van het technisch hulpmiddel (artikelen 25 en 26 Bogw)

Hoofdregel is dat een technisch hulpmiddel wordt verwijderd uit het te onderzoeken geautomatiseerde werk nadat het onderzoeksdoel is bereikt of de periode waarvoor het bevel is afgegeven is verstreken.[307] De verwijdering geschiedt door een opsporingsambtenaar van een technisch team. Sommige softwareapplicaties bieden de functionaliteit van een

[302] Nota van toelichting op het Bogw, p. 45.
[303] Art. 21 lid 4 Bogw.
[304] Nota van toelichting op het Bogw, p. 45. Zie ook *Kamerstukken I* 2017/18, 34 372, G (NMvA I), p. 14-15.
[305] Nota van toelichting op het Bogw, p. 21.
[306] *Kamerstukken II* 2018/19, 34 372, nr. 29 (verslag van een schriftelijk overleg), p. 13.
[307] Zie met name art. 126nba lid 6 Sv; *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 36-37; *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 75-80.

zelfstandige vernietiging van de software na verloop van een bepaalde, vooraf ingestelde, periode.[308]
Nadat het technische hulpmiddel is verwijderd zal de server aan de zijde van de politie geen gegevens meer kunnen ontvangen. Er kunnen echter sporen van het middel in het geautomatiseerde werk achterblijven. Deze sporen kunnen het gevolg zijn van de invloed van het geïnstalleerde technische hulpmiddel op het geautomatiseerde werk, of van handelingen die door het technische team zijn uitgevoerd om het technische hulpmiddel te plaatsen of te verwijderen. In alle gevallen zal zoveel mogelijk worden geprobeerd het geautomatiseerde werk in de oorspronkelijke staat achter te laten, dat wil zeggen als ware de bevoegdheid nooit toegepast.[309]
De politie heeft geen belang bij het achterblijven van gegevens, omdat de kans bestaat dat de software wordt ontdekt en de verdachte aldus op de hoogte raakt van het opsporingsonderzoek en vervolgens bewijsmateriaal vernietigt. Bovendien zou de achtergelaten software (of sporen daarvan) de basis kunnen vormen voor onderzoek naar de werking van middelen van de politie, terwijl de politie belang heeft bij de afscherming daarvan.[310] Om ieder risico uit te sluiten zal de politie dus de nodige inspanningen verrichten om te voorkomen dat sporen van de gebruikte software in het geautomatiseerde werk achterblijven.
Indien een technisch hulpmiddel niet of niet volledig kan worden verwijderd uit een geautomatiseerd werk, beëindigt de met verwijdering belaste opsporingsambtenaar van het technische team het transport van de door het technisch hulpmiddel geregistreerde gegevens naar de technische infrastructuur, zodat het technische team geen gegevens meer kan ontvangen van het geautomatiseerde werk.[311] Op basis van de logging kan worden gecontroleerd of de ontvangst van gegevens op de technische infrastructuur daadwerkelijk is beëindigd.[312]
Indien het technische hulpmiddel niet of niet volledig kan worden verwijderd, bijvoorbeeld omdat het geautomatiseerde werk niet meer is verbonden met het internet, bestaat de mogelijkheid dat dit risico's oplevert voor het functioneren van het geautomatiseerde werk waarin het is geplaatst. In dat geval stelt de opsporingsambtenaar van het technische team de officier van justitie hiervan in kennis en stelt hij informatie ter beschikking ten behoeve van de volledige verwijdering. De officier van justitie stelt op zijn beurt de beheerder van het geautomatiseerde werk daarvan in kennis en stelt hem de nodige informatie ter beschikking ten behoeve van de volledige verwijdering.[313]
In uitzonderingsgevallen kan worden afgezien van de verwijdering van geïnstalleerde software of van het ongedaan maken van de in het geautomatiseerde werk aangebrachte wijzigingen. Hierbij moet volgens de minister worden gedacht aan zwaarwegende belangen die zich verzetten tegen het verwijderen, zoals de situatie dat het verwijderen aanzienlijke risico's meebrengt voor het systeem waarin het technisch hulpmiddel is geïnstalleerd. Deze risico's worden voorafgaand aan de inzet – dat wil zeggen: in de verkennende fase – zoveel mogelijk in kaart gebracht en de officier van justitie wordt hierover door het technische team geïnformeerd.[314]

De handmatige inzet (onderzoek zonder het gebruik van een technisch hulpmiddel)

Hoewel het uitgangspunt is dat gebruik wordt gemaakt van een (gekeurd) technisch hulpmiddel is dat niet altijd strikt noodzakelijk: onderzoekshandelingen kunnen ook "*ad hoc*

[308] Art. 25 Bogw, en zie de nota van toelichting op het Bogw, p. 46-47; *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 105.
[309] *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 36; *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 76 en p. 77.
[310] *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 36; *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 77 en p. 80.
[311] Art. 26 lid 1 Bogw. Zie ook *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 78 en p. 80.
[312] De nota van toelichting op het Bogw, p. 47.
[313] Art. 126nba lid 6, tweede volzin, Sv jo art. 26 lid 2 Bogw. Zie ook *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 36-37 en 105. De beheerder is uit hoofde van zijn functie primair verantwoordelijk voor het behoud en het gebruik van de gegevens die zijn opgeslagen in de aan zijn zorg toevertrouwde computers. Zie *Kamerstukken II* 1998/99, 26 671, nr. 3 (MvT), p. 51; *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 78.
[314] *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 36; *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 80.

en handmatig" worden verricht.[315] In sommige gevallen is dat zelfs beter.[316] Bij 'handmatige' inzet kan worden gedacht aan de situatie dat gegevens direct na het binnendringen in een geautomatiseerd werk kunnen worden ingezien of worden overgenomen ten behoeve van het vaststellen van de identiteit van het geautomatiseerde werk.[317] Er wordt dan kort gezegd geen gebruik gemaakt van software die gegevens detecteert, registreert en transporteert. "*De vraag of het gebruik van een technisch hulpmiddel noodzakelijk is, is onder meer afhankelijk van de aard van de inzet, de aard van het geautomatiseerde werk en de vraag of de gegevens zonder gebruik van een technisch hulpmiddel als rechtmatig bewijs kunnen worden aangemerkt*", aldus de minister,[318] die met "*rechtmatig bewijs*", vermoedelijk 'betrouwbaar bewijs' bedoelt.
Indien de officier van justitie beveelt dat het verrichten van onderzoekshandelingen in een geautomatiseerd werk plaatsvindt zonder een technisch hulpmiddel, worden ter uitvoering van het bevel de onderzoekshandelingen verricht die zijn omschreven in het bevel en worden procedurele waarborgen getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de tijdens het onderzoek vast te leggen gegevens te garanderen, aldus bepaalt artikel 21 lid 5 Bogw.[319] Het Bogw schrijft niet voor op welk moment die procedurele waarborgen moeten worden getroffen.
Anders dan in artikel 21 lid 4 Bogw, waarin is voorgeschreven dat de officier van justitie *in de processtukken vermeldt* welke (aanvullende) waarborgen zijn getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de met het technisch hulpmiddel vastgelegde gegevens te garanderen, schrijft artikel 21 lid 5 Bogw (slechts) voor *dat* (procedurele) waarborgen worden getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de tijdens het onderzoek vast te leggen gegevens te garanderen. Deze bepaling schrijft naar de letter genomen dus niet ook voor dat de officier van justitie *in de processtukken vermeldt* welke (procedurele) waarborgen zijn getroffen. Dit verschil in redactie van lid 4 en van lid 5 van artikel 21 Bogw is echter onbedoeld. Ook ingeval de onderzoekshandelingen handmatig zijn verricht stelt de toelichting op het Bogw onomwonden dat "*de officier (...) in de processtukken* [vermeldt] *welke procedurele waarborgen zijn getroffen om de betrouwbaarheid, integriteit en de herleidbaarheid van de vastgelegde gegevens te garanderen.*"[320]

Het begrip 'procedurele waarborgen' en het verschil met het begrip 'aanvullende waarborgen'

Blijkens de nota van toelichting op het Besluit onder 3.6 adviseert het technische team de officier van justitie welke procedurele waarborgen dienen te worden geïmplementeerd. In de algemene toelichting op het Besluit wordt verder niet omschreven waaruit die waarborgen zoal dienen te bestaan. In de artikelsgewijze toelichting op artikel 21, die betrekking heeft op zowel de inzet van een niet-gekeurd technisch hulpmiddel als de handmatige inzet, wordt het volgende opgemerkt:

> "*Als keuring van een hulpmiddel geheel achterwege blijft of als onderzoekshandelingen worden verricht zonder gebruik van een technisch hulpmiddel dan vermeldt de officier in de processtukken welke aanvullende waarborgen zijn getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de vastgelegde gegevens te garanderen (artikel 21,*

---

315 Art. 21 lid 5 Bogw. Nota van toelichting op het Bogw onder 3.3. Vgl. ook *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 14.
316 Nota van toelichting op het Bogw, onder 3.6, p. 21.
317 Vgl. ook *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 70-71.
318 Nota van toelichting op het Bogw, onder 3.6, p. 21.
319 Zie ook de nota van toelichting op het Bogw, onder 3.6, p. 21.
320 Nota van toelichting op het Bogw, onder 3.6, citaat op p. 21, en zie andermaal p. 22 (onderstreping onderzoekers): "*Indien de onderzoekshandelingen zonder (goedgekeurd) technisch hulpmiddel zijn verricht, vermeldt de officier van justitie in de processtukken welke procedurele waarborgen zijn getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de vastgelegde gegevens te kunnen garanderen.*"

vierde en vijfde lid). Hierbij kan worden gedacht aan een uitgebreide omschrijving van de functionele specificaties van [een] op maat gemaakt technisch hulpmiddel, het voegen van een digitale kopie van de software en de broncode bij het proces-verbaal, het vooraf en achteraf maken van een forensische kopie of het audiovisueel vastleggen van de uitvoering van de onderzoekshandelingen. De aanvullende procedurele eisen van de officier van justitie kunnen de rechtmatigheid van de inzet waarborgen en voorkomen dat er twijfel ontstaat over de betrouwbaarheid, integriteit en herleidbaarheid van de vastgelegde gegevens. (…)
T-Mobile heeft in reactie op het ontwerpbesluit vragen gesteld over het de uitwerking in de praktijk van het treffen van de noodzakelijke procedurele maatregelen bij het werken met een ad-hoc script. Verwezen wordt naar de hierboven genoemde (niet limitatieve) voorbeelden van maatregelen die kunnen worden getroffen."[321]

De begrippen 'aanvullende waarborgen' en 'procedurele waarborgen' worden in dit citaat door elkaar gebruikt, terwijl wordt verwezen naar zowel lid 4 als lid 5 van artikel 21 Bogw. Daaruit kan worden afgeleid dat de waarborgen die moeten worden genomen enerzijds bij gebruik van een niet-gekeurd technisch hulpmiddel en anderzijds bij handmatige inzet, ondanks de verschillen in terminologie, in essentie niet van elkaar verschillen.
Als uitgangspunt heeft te gelden dat de te nemen procedurele en aanvullende waarborgen op een vergelijkbaar niveau de betrouwbaarheid, integriteit en herleidbaarheid van de tijdens het onderzoek vast te leggen gegevens dienen te garanderen, zoals de artikelen 8 tot en met 13 Bogw dat doen met betrekking tot de inzet van een technisch hulpmiddel dat (vooraf) is goedgekeurd. Een goedgekeurd technisch hulpmiddel is bijvoorbeeld in staat om gegevens op zodanige wijze te registreren dat de inhoud identiek is aan de gegevens die in een geautomatiseerd werk zijn gedetecteerd. Ook moet een technisch hulpmiddel de geregistreerde gegevens kunnen voorzien van de datum en tijd van de registratie. Verder moet een technisch hulpmiddel de geregistreerde gegevens kunnen voorzien van een uniek kenmerk dat bij de vastlegging van de gegevens op de opslaglocatie wordt herkend, zodat de herkomst van de gegevens te allen tijde kan worden vastgesteld. Aangenomen mag worden dat bij de handmatige inzet (ter vervanging) procedurele waarborgen zullen dienen te worden genomen om een (nagenoeg) vergelijkbaar resultaat te bereiken. Gedacht kan bijvoorbeeld worden aan het (handmatig) toekennen en controleren van de hashcode.[322]
Schematisch kunnen de eisen aan de verschillende wijzen van inzet als volgt worden weergegeven:

Wijze van inzet	Log-ging?	Vastlegging gegevens op technische infra-structuur?	Hoe worden de betrouwbaarheid, integri-teit en herleidbaarheid van de vastgelegde gegevens gegarandeerd?
Gekeurd technisch hulpmiddel	Ja	Ja	Artt. 8 t/m 13 Bogw en keuring
Niet-gekeurd technisch hulpmiddel	Ja	Ja	Aanvullende waarborgen[323]
Handmatig	Ja	Ja	Procedurele waarborgen[324]

[321] Nota van toelichting op het Bogw, p. 45.
[322] Vgl. *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 109-110.
[323] Onder 3.7 in de nota van toelichting op het Bogw wordt echter gesproken van procedurele waarborgen die de officier van justitie moet vermelden indien onderzoekshandelingen worden verricht "*zonder (goedgekeurd) technis*ch hulpmiddel". Aan de woorden 'aanvullende' of 'procedurele' lijkt daarom, zoals gezegd, geen onderscheidende betekenis toe te komen.
[324] Zie de voorgaande voetnoot.

Los van de te creëren waarborgen geldt dat in elk geval ook logging plaatsvindt en dat de vergaarde gegevens worden vastgelegd op een technische infrastructuur die voldoet aan de eisen zoals opgenomen in het Bogw, met name de artikelen 5, 6, 7, 27 en 28.[325]

3.9. De vastlegging van gegevens en de verstrekking daarvan aan het tactische team

De 'technische infrastructuur' (artikelen 27 en 28 Bogw)

Nadat het geautomatiseerde werk is binnengedrongen, kunnen – al dan niet met behulp van een technisch hulpmiddel – onderzoekshandelingen worden verricht. De gegevens die tijdens het verrichten van onderzoekshandelingen worden geregistreerd worden automatisch vastgelegd op een zogeheten 'technische infrastructuur' van het technische team (artikel 27 lid 1 Bogw). Ook als onderzoekshandelingen zonder goedgekeurd hulpmiddel worden verricht, dienen de verkregen gegevens te worden vastgelegd op een technische infrastructuur.[326] Deze gegevens kunnen dienen ter opsporing en zij kunnen eventueel worden gebruikt als bewijs in een strafzaak.

'Technische infrastructuur' is gedefinieerd als "*technische voorziening van een technisch team bedoeld voor de vastlegging van gegevens ter uitvoering van een bevel*".[327] Hiermee wordt gedoeld op de opslaglocatie voor de gegevens die gedurende de uitvoering van een bevel worden vastgelegd en die kunnen dienen als bewijs in een strafzaak. Uit deze definitie, in combinatie met de definitie van het begrip 'technisch team', vloeit voort dat de vastlegging van gegevens dient plaats te vinden op een technische voorziening binnen de politieorganisatie. Deze eis wordt gesteld om de betrouwbaarheid en de integriteit van het verkregen bewijsmateriaal te borgen en onbevoegde wijziging of kennisneming hiervan te voorkomen.[328]

De onderzoeksgegevens moeten worden weggeschreven naar een server van de politie die – ter voorkoming van manipulatie van de gegevens – binnen een beveiligde omgeving is geplaatst en aan bepaalde eisen voldoet.[329] De servers van deze technische infrastructuur bevinden zich op een locatie van de politie in Nederland.[330]

Een technische infrastructuur is zodanig ingericht dat bij de vastlegging van gegevens het door een technisch hulpmiddel geregistreerde unieke gegeven wordt herkend (artikel 27 lid 2 Bogw). Zo kan de herkomst van de vastgelegde gegevens worden vastgesteld. Bij de vastlegging van gegevens op de technische infrastructuur worden de datum en tijd geregistreerd (artikel 27 lid 3 Bogw). Hierdoor bestaat zekerheid over de datum en het

---

[325] Zie o.a. *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 31: "*In de derde plaats dient te allen tijde te kunnen worden gecontroleerd welke handelingen al dan niet met behulp van een technisch hulpmiddel in het desbetreffende geautomatiseerde werk hebben plaatsgevonden, zodat op een later moment geen twijfel kan bestaan over de aard en consequenties van de handelingen die zijn verricht bij de uitvoering van het bevel. Dit betreft de geautomatiseerde vastlegging (logging) van gegevens over de verwerking van gegevens bij het verrichten van handelingen in een geautomatiseerd werk. De eisen die aan de geautomatiseerde vastlegging worden gesteld worden eveneens nader geregeld in* [het] *Besluit technische hulpmiddelen strafvordering.*"

[326] Nota van toelichting op het Bogw, p. 21.

[327] Art. 1 onder g Bogw.

[328] Nota van toelichting op het Bogw, p. 33.

[329] *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 110.

[330] Zie *Kamerstukken II* 2018/19, 34 372, nr. 29 (verslag van een schriftelijk overleg), p. 11 en (citaat) p. 12: "*De technische infrastructuur waarop onderzoeksgegevens worden vastgelegd is in beheer van de politie. De servers van deze technische infrastructuur bevinden zich in Nederland. Indien voor het binnendringen in een geautomatiseerd werk gebruik gemaakt zal worden van commerciële binnendringsoftware, dan worden de onderzoeksgegevens opgeslagen op de technische infrastructuur van de politie. Er wordt geen gebruik gemaakt van een server van de leverancier van de software.*" Ook: *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 74.

tijdstip van de vastlegging.[331] De inhoud van de op een technische infrastructuur vastgelegde gegevens wordt niet gewijzigd.[332]
De vastgelegde gegevens zijn uitsluitend toegankelijk voor de daartoe door de korpschef aangewezen ambtenaren. Opsporingsambtenaren van het tactische team hebben geen toegang tot de technische infrastructuur en de daarin vastgelegde gegevens. De technische infrastructuur is beveiligd tegen een wijziging van de vastgelegde gegevens en tegen de kennisneming van deze gegevens door onbevoegden.[333]
Via de logging kan controle worden uitgeoefend op het functioneren van de technische infrastructuur. Zowel tijdens de uitvoering van een bevel als achteraf moet kunnen worden vastgesteld of wijziging dan wel onbevoegde kennisneming van de op de technische infrastructuur vastgelegde gegevens heeft plaatsgevonden.[334]

Beoogde gegevens en bijkomende gegevens ('bijvangst')

Het Nederlandse strafprocesrecht kent de doctrine van 'de voortgezette toepassing van dwangmiddelen'. Wanneer bij de rechtmatige uitoefening van een bevoegdheid bij toeval wordt kennisgenomen van gegevens die kunnen bijdragen aan het bewijs van andere delicten dan die met het oog waarop de bevoegdheid wordt toegepast ('bijvangst'), dan kunnen in beginsel andere bestaande bevoegdheden worden uitgeoefend indien de wettelijke vereisten daarvoor zijn vervuld en kunnen de aldus verkregen gegevens worden gebruikt voor het bewijs van die andere delicten.[335] Van deze algemene regel wordt binnen het bestek van het onderzoek in een geautomatiseerd werk afgeweken. Als in het kader van het onderzoek in het geautomatiseerde werk gegevens worden aangetroffen omtrent andere strafbare feiten dan het delict dat de aanleiding vormde voor het binnendringen, dan mogen deze gegevens niet zonder meer worden vastgelegd, aldus de minister. Ook de bevoegdheid tot het ontoegankelijk maken van gegevens is volgens de minister beperkt tot de gegevens met betrekking tot welke of met behulp waarvan het strafbare feit is gepleegd. Als het gaat om gegevens die betrekking hebben op een ander strafbaar feit dan zijn (dus) een aanvullend bevel van de officier van justitie en een aanvullende machtiging van de rechter-commissaris noodzakelijk.[336] Voor het op afstand binnendringen is vereist dat het geautomatiseerde werk in gebruik is bij de verdachte (artikel 126nba Sv), dan wel de persoon jegens wie de bevoegdheid wordt toegepast (artikel 126uba en artikel 126zpa Sv). Als de verdenking betreffende het andere strafbare feit is gericht jegens een andere persoon bij wie dat werk in gebruik is, dan moet een nieuw bevel worden afgegeven met een omschrijving van dat andere feit en van de desbetreffende verdachte, aldus de minister.[337]
Datzelfde geldt ingeval pas na de inzet van de bevoegdheid beter inzicht wordt verkregen in het functioneren van het geautomatiseerde werk en de gegevens die daarop zijn opgeslagen. Volgens de minister kan dan in overleg met de rechter-commissaris worden gekozen voor een meer stapsgewijze aanpak, waarbij de onderzoeksbevindingen aanleiding kunnen

---

331 Nota van toelichting op het Bogw, p. 33, en zie ook p. 47: "*Het kan voorkomen dat de datum en tijd in de technische infrastructuur van de politie afwijken van de ingestelde datum en tijd van het te onderzoeken geautomatiseerd werk. Een technisch team heeft geen invloed op de datum en tijd die een verdachte heeft ingesteld in zijn computer of smartphone. Na overlegging van de onderzoeksresultaten door het technische team aan het tactische team kan het tactische team het tijdsverloop reconstrueren.*"

332 Nota van toelichting op het Bogw, p. 33, p. 47-48.

333 Art. 28 lid 2 Bogw. Zie ook de nota van toelichting, onder 3.3, p. 16.

334 Nota van toelichting, p. 48. Art. 28 lid 3 Bogw luidt: "*Bij de vastlegging van gegevens worden maatregelen getroffen om wijziging van de vastgelegde gegevens of kennisneming van de vastgelegde gegevens hiervan door onbevoegden te voorkomen en achteraf te kunnen vaststellen of wijziging of kennisneming hiervan heeft plaatsgevonden.*"

335 Zie bijvoorbeeld het zogeheten 'geweerarrest', HR 2 december 1935, ECLI:NL:HR:1935:146, *NJ* 1936/250 m.nt. Pompe, en HR 7 december 1993, ECLI:NL:HR:1993:AC0100, *NJ* 1994/281. Zie voor een bespreking van de leerstukken van 'de voortgezette toepassing van dwangmiddelen' en 'misbruik van bevoegdheid': B.F. Keulen & G. Knigge, *Strafprocesrecht (Ons strafrecht deel 2)*, Deventer: Wolters Kluwer 2020, p. 331-333, en zie G.J.M. Corstens, *Het Nederlands strafprocesrecht*, bewerkt door M.J. Borgers en T. Kooijmans, Deventer: Wolters Kluwer 2021, p. 309-312.

336 *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 54.

337 *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 54.

geven tot een aanvullend bevel van de officier van justitie en een aanvullende machtiging van de rechter-commissaris voor het verrichten van nadere onderzoekshandelingen in het geautomatiseerde werk.[338]

De verstrekking van gegevens door het technische team aan het tactische team (artikel 29 Bogw)

De gegevens die ter uitvoering van een bevel op een technische infrastructuur zijn vastgelegd worden verstrekt aan een opsporingsambtenaar die is belast met het opsporingsonderzoek, oftewel een lid van het tactische team.[339] Uitsluitend de gegevens die binnen de reikwijdte van het bevel van de officier van justitie vallen worden ter beschikking gesteld van het tactische onderzoeksteam.[340]

Indien het ter uitvoering van het bevel of ten behoeve van het opsporingsonderzoek nodig is om een selectie te maken uit gegevens die op een technische infrastructuur zijn vastgelegd, voert een opsporingsambtenaar van het technische team een bewerking uit met gebruikmaking van een forensische kopie[341] van de gegevens die ter uitvoering van het bevel zijn vastgelegd. De bewerkte gegevens worden verstrekt aan een opsporingsambtenaar van het tactische team.[342]

Bij de selectie van gegevens legt een opsporingsambtenaar van een technisch team de bewerkingen die hebben plaatsgevonden met betrekking tot de kopie van de vastgelegde gegevens vast in een proces-verbaal, dat aan de officier van justitie wordt gezonden.[343]

Indien het ter uitvoering van het bevel of ten behoeve van het opsporingsonderzoek nodig is om de gegevens te filteren, draagt het technische team dus zorg voor de selectie van onderzoeksgegevens, zodat binnen de categorieën van gegevens die in het bevel van de officier zijn opgenomen uitsluitend de gegevens die van belang zijn voor het opsporingsonderzoek ter beschikking komen van het tactische team. Als voorbeeld noemt de minister de inhoud van e-mailverkeer. Wanneer het bevel van de officier van justitie strekt tot het vastleggen van de correspondentie tussen de verdachte en een met name genoemde andere verdachte, zal het tactische team uitsluitend de beschikking krijgen over die correspondentie, en niet over eventuele andere correspondentie vanuit hetzelfde e-mailadres.[344]

---

338 *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 68.

339 Art. 29 lid 1 Bogw; nota van toelichting op het Bogw, p. 21.

340 *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 14, p. 27.

341 Art. 29 lid 2 en lid 3 Bogw maken slechts melding van een 'kopie'. De nota van toelichting op het Bogw, p. 17, 21 en 48, wijst uit dat de minister hierbij een *forensische* kopie voor ogen staat. Een forensische kopie (of: *image*) is iets anders dan een eenvoudige kopie van een gegevensbestand. Forensische kopieën bevatten behalve alle inhoudelijke informatie ook alle metadata en niet-toegewezen data. Het betreft een 'één-op-één kopie', waarbij alle bits op de gegevensdrager worden gekopieerd. Dat forensische kopieën dezelfde informatie bevatten als het origineel, is verifieerbaar door vergelijking van de hashcode van het origineel met die van de kopie.

342 Art. 29 lid 2 Bogw; de nota van toelichting op het Bogw, p. 21.

343 Art. 29 lid 3 Bogw; de nota van toelichting op het Bogw, p. 17.

344 *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 40; *Kamerstukken I* 2016/17, 34 372, D (MvA I), p. 41; Nota van toelichting op het Bogw, onder II, artikelsgewijze toelichting, art. 29, p. 48.

3.10. De logging

Logging in het algemeen

Het Bogw schrijft 'logging' voor, dat wil zeggen: het doorlopend en geautomatiseerd vastleggen in logbestanden van gegevens over de uitvoering van een bevel ex artikel 126nba Sv.[345] Alle handelingen die tijdens het onderzoek in een geautomatiseerd werk plaatsvinden worden gelogd. Dit betreft de handelingen die worden verricht (i) tijdens het binnendringen en (ii) gedurende het onderzoek in een geautomatiseerd werk. Zowel onderzoekshandelingen die met een technisch hulpmiddel plaatsvinden als onderzoekshandelingen waarbij de inzet van een technisch hulpmiddel achterwege blijft worden vastgelegd in logbestanden. De logbestanden worden veilig bewaard op een server van de politie. Door de logging kan worden gecontroleerd welke handelingen al dan niet met gebruik van een technisch hulpmiddel in het geautomatiseerde werk hebben plaatsgehad, zodat op een later moment geen twijfel kan bestaan over de aard en consequenties van de onderzoekshandelingen die zijn verricht bij de uitvoering van het bevel.[346]

Artikel 5 lid 1 Bogw schrijft meer specifiek voor dat gedurende de uitvoering van een bevel doorlopend en automatisch gegevens in logbestanden worden vastgelegd over:[347]

a. de handelingen die worden verricht ter uitvoering van een bevel (inzetlogging). Dit is de logging die wordt uitgevoerd om de tijdens het onderzoek verrichte handelingen vast te leggen. Het betreft handelingen als het (automatisch) vastleggen van het beeldscherm en de toetsaanslagen van de opsporingsambtenaar van een technisch team, maar ook het vastleggen van de communicatie tussen de technische infrastructuur en het geautomatiseerde werk, het vastleggen van gebruikte scripts, softwareversies en het journaal van de opsporingsambtenaar. De inzetlogging zal zoveel mogelijk geautomatiseerd plaatsvinden. Indien automatische logging technisch niet mogelijk is, bijvoorbeeld in gevallen waarin geen technisch hulpmiddel wordt ingezet, legt een opsporingsambtenaar van een technisch team de hiervoor genoemde handelingen handmatig vast, bijvoorbeeld in de vorm van een journaal;[348]
b. de toegang tot een technisch hulpmiddel (authenticatie- en autorisatielogging). Dit betreft een subcategorie van systeemloggingen. Hiermee vindt controle op de toegang tot een technisch hulpmiddel plaats;
c. de gegevens die al dan niet met een technisch hulpmiddel ter uitvoering van een bevel op de technische infrastructuur worden vastgelegd (bewijslogging). Dit betreft een subcategorie van de inzetlogging. Het betreft gegevens over de vastlegging gedurende de onderzoeksfase van al dan niet door een technisch hulpmiddel geregistreerde

---

345 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 14 en p. 31. Zie in het bijzonder artt. 5, 6 en 7 Bogw, en de nota van toelichting op het Bogw, p. 17-18 en p. 36; *Kamerstukken I* 2016/17, 34 372, D (MvA I), p. 6 en p. 20; *Kamerstukken II* 2017/18, 34 372, nr. 27 (verslag van een schriftelijk overleg), p. 8 en p. 11; *Kamerstukken II* 2018/19, 34 372, nr. 29 (verslag van een schriftelijk overleg), p. 13.
De grondslag voor deze regeling in het Bogw ligt in art. 126nba lid 8: "*Bij of krachtens algemene maatregel van bestuur worden regels gesteld omtrent (…) b. de geautomatiseerde vastlegging van gegevens over de uitvoering van het bevel, bedoeld in het eerste lid.*"

346 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 31; *Kamerstukken I* 2016/17, 34 372, D (MvA I), p. 6.

347 Nota van toelichting op het Bogw, p. 17-18.

348 Art. 5 lid 2 Bogw, en zie de nota van toelichting op het Bogw, p. 17: "*De inzetlogging zal zoveel mogelijk geautomatiseerd plaatsvinden. Voor zover dit technisch niet mogelijk is, wordt procedureel binnen de politieorganisatie vastgelegd dat handmatige logging plaatsvindt.*"

gegevens die kunnen dienen als bewijs in een strafzaak;[349]

d. het functioneren van de technische infrastructuur (systeemlogging). Dit betreft de logging die wordt gebruikt voor het signaleren, onderzoeken en verhelpen van problemen met betrekking tot de betrouwbaarheid, integriteit en beschikbaarheid van de technische infrastructuur waarop de tijdens een onderzoek vergaarde gegevens worden vastgelegd. Het betreft logging die automatisch door alle gebruikte systemen wordt gegenereerd en centraal wordt verzameld en vastgelegd.

In artikel 7 worden eisen gesteld ter borging van de betrouwbaarheid en integriteit van de logging.[350] De inhoud van de logbestanden wordt ingevolge artikel 7 lid 1 Bogw niet gewijzigd.
Artikel 7 lid 2 Bogw stelt eisen aan de toegang tot logbestanden om de betrouwbaarheid daarvan te garanderen.[351] De logbestanden zijn uitsluitend toegankelijk voor door de korpschef aangewezen (deskundige) ambtenaren. De opsporingsambtenaren die lid zijn van een technisch team en belast zijn met de plaatsing, inzet en verwijdering van een technisch hulpmiddel hebben geen toegang tot de server waarop de logging plaatsvindt.[352]
Overeenkomstig artikel 7 lid 3 Bogw worden bij de vastlegging van gegevens in logbestanden maatregelen getroffen om wijziging van de logbestanden of kennisneming hiervan door onbevoegden te voorkomen en achteraf te kunnen vaststellen of wijziging of kennisneming heeft plaatsgevonden. Alle loggingsgegevens moeten naar beveiligde omgevingen worden weggeschreven waar manipulatie niet meer mogelijk is.[353]

De minister heeft erkend dat logging vooralsnog niet kan leiden tot het weergeven van alle relevante handelingen. Daarbij geldt dat voor zinvolle logging de exacte werking van de gebruikte software bekend moet zijn, met inbegrip van de broncode. Dit is niet altijd het geval, met name niet wanneer het technisch hulpmiddel (althans een softwareapplicatie) wordt betrokken van een commerciële partij. In een dergelijk geval is goedkeuring van het technisch hulpmiddel door de keuringsdienst een voorwaarde voor de inzet ervan. Bij die keuring wordt onder meer bezien of alle relevante handelingen van de politie tijdens de inzet correct worden gelogd. De controle raakt de integriteit van de informatie die is verzameld, de werking van de software en daarmee ook de onderzoekshandelingen die zijn verricht.[354]

---

[349] Zie ook *Kamerstukken II* 2017/18, 34 372, nr. 27 (verslag van een schriftelijk overleg), p. 8. In de toelichting op het Bogw, p. 18 en (citaat) p. 36, wordt over de bewijslogging opgemerkt: "*Uitsluitend de bewijslogging* [onderzoekers: en dus niet logging van de andere categorieën] *wordt, al dan niet in bewerkte vorm, aan het dossier in een strafzaak toegevoegd. De bewijslogging dient op grond van artikel 26* [onderzoekers: bedoeld wordt artikel 27] *van het besluit plaats te vinden op een technische infrastructuur van een technisch team.*" Art. 27 Bogw heeft betrekking op de in het geautomatiseerde werk geregistreerde gegevens die kunnen dienen als bewijs in een strafzaak. In het Bogw en de gehele wetsgeschiedenis wordt geen separate aandacht besteed aan het verschil tussen enerzijds het vastleggen van de loggingsgegevens (logs) *over* de detectie en registratie van de gegevens die tot bewijs kunnen dienen, en anderzijds de vastlegging van de gegevens die tot bewijs kunnen dienen zelf. De bewijslogging kan wellicht beide betreffen.

[350] Nota van toelichting op het Bogw, p. 37. Aldaar worden de begrippen 'betrouwbaarheid en integriteit' (van de logbestanden) tevens omschreven als 'de kwaliteit' van de logging: "*In artikel 7 worden eisen gesteld ter borging van de kwaliteit van de logging. De gelogde gegevens mogen niet worden bewerkt, zijn uitsluitend toegankelijk voor daartoe door de korpschef geautoriseerde ambtenaren en moeten beveiligd zijn tegen wijziging of onbevoegde kennisneming.*"

[351] Hierover staat in de nota van toelichting op het Bogw, p. 37, nog het volgende: "*In het advies van de NP* [Nationale politie] *is erop gewezen dat de centraal verzamelde systeemlogging logregels bevat van alle systemen binnen de technische infrastructuur van de politie. Veel systemen binnen deze technische infrastructuur worden voor de uitvoering van verschillende bevelen tegelijkertijd gebruikt. Hierdoor kunnen afzonderlijke logregels niet aan een specifiek bevel worden toegewezen. De gegevens worden wel bewaard om aan de eisen van de Wet politiegegevens te kunnen voldoen. Indien tijdens een strafzaak of in het kader van het toezicht van de Inspectie JenV vermoedens rijzen over onregelmatigheden, zoals ongeautoriseerde toegang en/of oneigenlijk gebruik, kunnen de gegevens met betrekking tot de uitvoering van het desbetreffende bevel separaat veiliggesteld worden.*"

[352] *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 52 en 59. Hoewel de wetsgeschiedenis er niet expliciet over rept, mag worden aangenomen dat dit ook het geval is wanneer er geen technisch hulpmiddel wordt gebruikt.

[353] *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 52; *Kamerstukken II* 2018/19, 34 372, nr. 29 (verslag van een schriftelijk overleg), p. 11.

[354] *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 78.

Logging als middel van controle en toezicht

De logging is in het bijzonder bedoeld voor de interne controle van de handelingen die tijdens de uitvoering van het bevel worden verricht en van het functioneren van de technische infrastructuur.[355] In het geval in een strafzaak twijfel ontstaat over de tijdens het onderzoek verrichte handelingen of de betrouwbaarheid van het hiermee vergaarde bewijs, kan bovendien aan de hand van de logging hierover verantwoording worden afgelegd.[356]

De in artikel 5 Bogw bedoelde vastlegging van gegevens in logbestanden vindt ingevolge artikel 6 lid 1 Bogw op zodanige wijze plaats dat – zowel *tijdens* de periode die is vermeld in het bevel en waarbinnen aan het bevel uitvoering moet worden gegeven als *na afloop* daarvan – kan worden vastgesteld of een onregelmatigheid heeft plaatsgevonden die van invloed is op de betrouwbaarheid en integriteit van de gegevens die ter uitvoering van het bevel op een technische infrastructuur zijn vastgelegd. De logging dient dus zodanig te zijn ingericht dat op basis hiervan kan worden vastgesteld of en zo ja wanneer een onregelmatigheid heeft plaatsgevonden die van invloed is op de betrouwbaarheid en integriteit van de ter uitvoering van een bevel vergaarde gegevens, die kunnen dienen als bewijs in een strafzaak.[357] Indien een onregelmatigheid wordt geconstateerd maakt een opsporingsambtenaar van een technisch team daarvan een proces-verbaal op dat aan de officier van justitie wordt gezonden (artikel 6 lid 2 Bogw). De officier van justitie en de rechter beoordelen in hoeverre de geconstateerde onregelmatigheid afbreuk doet aan de bewijskracht van de gegevens.[358]

Wat in dit verband precies onder het begrip 'onregelmatigheid' moet worden verstaan, wordt in de toelichting op het Bogw niet nader uitgelegd.[359] Wel worden in de toelichting op het Bogw en in de wetsgeschiedenis als voorbeelden van onregelmatigheden genoemd: (het bestaan van technische aanwijzingen voor) ongeautoriseerde toegang tot de vastgelegde

---

[355] Nota van toelichting op het Bogw, p. 18, p. 36, p. 46; *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 52: "*Omdat het onderzoek in een geautomatiseerd werk in een volledig digitale omgeving plaatsvindt, kunnen de handelingen die verricht worden ter uitvoering van het bevel van de officier van justitie doorlopend en geautomatiseerd worden vastgelegd op de politieserver. Het logging-proces is zo ingericht dat deze te allen tijde blijft functioneren, waardoor zowel tijdens het onderzoek als achteraf controle kan plaatsvinden. Als er sprake zou zijn van manipulatie kan dit dus altijd worden achterhaald.*" Ook: *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 59, p. 77; *Kamerstukken I* 2016/17, 34 372, D (MvA I), p. 20.

[356] Nota van toelichting op het Bogw, p. 36-37.

[357] Nota van toelichting op het Bogw, met name p. 18

[358] Nota van toelichting op het Bogw, met name p. 18, alsook (de artikelsgewijze toelichting op) p. 36-37, p. 40 en p. 46.

[359] Enige duiding valt wellicht te ontlenen aan het volgende. In de consultatieversie van het ontwerp-Bogw, art. 6 lid 1, werd in plaats van het begrip 'onregelmatigheid' nog melding gemaakt van "*een handeling of bewerking (…) die van invloed is op de betrouwbaarheid en integriteit van de ter uitvoering van het bevel vastgelegde gegevens.*" Lid 2 van art. 6 vervolgde: "*Indien een handeling of bewerking als bedoeld in het eerste lid wordt geconstateerd maakt een opsporingsambtenaar van een technisch team daarvan proces-verbaal op (…).*" De logging strekt ertoe om een dergelijke handeling of bewerking te kunnen vaststellen, aldus de toelichting op de consultatieversie van het ontwerp-Bogw (p. 12). Niet blijkt dat met de vervanging van de begrippen 'handeling of bewerking' (in het ontwerpbesluit) door het begrip 'onregelmatigheid' (in het definitieve besluit) een wezenlijke begripswijziging is beoogd.

gegevens, dan wel een wijziging of oneigenlijk gebruik van die gegevens.[360] De – in artikel 6 lid 1 Bogw opgenomen – verwijzing naar artikel 5 Bogw en de hiervoor bedoelde voorbeelden maken duidelijk dat een onregelmatigheid betrekking kan hebben op zowel de gegevens die met het oog op bewijsgebruik zijn geregistreerd (de bewijslogging), als de overige loggingsgegevens. Het gaat in artikel 6 Bogw echter uitsluitend om (technische aanwijzingen voor) onregelmatigheden die afbreuk (kunnen) doen aan de (in artikel 10 Bogw omschreven) 'betrouwbaarheid en integriteit' van de gegevens die kunnen dienen als bewijs in een strafzaak.[361] Die beperking geldt naar het oordeel van de onderzoekers ook voor het begrip 'onregelmatigheid' dat is opgenomen in de artikelen 23 lid 4 en 24 lid 3 Bogw.[362] Aanwijzingen voor de manipulatie van de inzetlogging of van de authenticatie- en autorisatielogging is daarvan een voorbeeld, omdat door die aanwijzingen vragen (kunnen) rijzen over de wijze waarop en door wie de bewijslogging is verkregen.

De logging staat niet uitsluitend ten dienste van de interne controle. De Inspectie Justitie en Veiligheid kan in het kader van haar toezichthoudende taak op de politie met gebruikmaking van de logging onderzoek doen naar eventuele onregelmatigheden bij de uitvoering van het onderzoek in een geautomatiseerd werk.[363] Ook houdt de Inspectie Justitie en Veiligheid toezicht op de naleving van de regels over de vastlegging in logbestanden zelf.[364] Voor de

---

360 Nota van toelichting op het Bogw, p. 37: "*Indien tijdens een strafzaak of in het kader van het toezicht van de Inspectie JenV vermoedens rijzen over onregelmatigheden, zoals ongeautoriseerde toegang en/of oneigenlijk gebruik, kunnen de gegevens met betrekking tot de uitvoering van het desbetreffende bevel separaat veiliggesteld worden.*"
Kamerstukken II 2016/17, 34 372, nr. 6 (NV II), p. 52: "*Het loggingsproces is zo ingericht dat de loggingsinformatie tijdens de fase van bewijsvergaring te allen tijde blijft functioneren en niet valt te manipuleren, te wijzigen of te verwijderen. De software wordt hierop gecontroleerd alvorens deze kan worden ingezet. Het is praktisch mogelijk de logging uit te schakelen. Echter, dit is altijd zichtbaar in de loggingsgegevens, aangezien er dan een verschil zichtbaar zal zijn in de geregistreerde tijd. Een dergelijke onregelmatigheid zal de integriteit en betrouwbaarheid van het bewijsmateriaal aantasten hetgeen aan de bruikbaarheid van het materiaal in de weg staat.*"
Kamerstukken I 2017/18, 34 372, G (NMvA I), p. 13-14: "*Via de logging van de uitvoering van het bevel vindt controle plaats op het onderzoek met een technisch hulpmiddel en het functioneren van de technische infrastructuur waarop de gegevens worden vastgelegd. Hierdoor kan zowel tijdens de uitvoering van een bevel als achteraf worden vastgesteld of wijziging van vastgelegde gegevens dan wel onbevoegde kennisneming hiervan heeft plaatsgevonden. Indien een onregelmatigheid wordt vastgesteld wordt hiervan proces-verbaal opgemaakt, dat aan de officier van justitie wordt gezonden.*" En:
Kamerstukken I 2017/18, 34 372, G (NMvA I), p. 24: "*Ondanks maatregelen kan het voorkomen dat er technische aanwijzingen zijn dat het bewijs door onbevoegden is geraadpleegd of gewijzigd. In een dergelijk geval dient in het proces-verbaal te worden opgenomen dat deze aanwijzingen er zijn en, indien mogelijk, welk effect deze aanwijzingen hebben op de integriteit van het bewijs.*"

361 Art. 10 Bogw wijst uit dat onder 'betrouwbaarheid en integriteit' van de gegevens die kunnen dienen als bewijs in een strafzaak (dat wil zeggen: de geregistreerde gegevens) niet alleen wordt verstaan dat de geregistreerde gegevens identiek zijn aan de in het geautomatiseerde werk gedetecteerde gegevens, maar ook dat onbevoegden geen kennis (kunnen) nemen van de geregistreerde gegevens (vertrouwelijkheid).

362 Anders dan in art. 6 lid 1 Bogw wordt in de artikelen 23 lid 4 en 24 lid 3 Bogw de reikwijdte van het begrip 'onregelmatigheid' naar de letter genomen niet beperkt tot slechts die onregelmatigheden "*die van invloed zijn op de betrouwbaarheid en integriteit van de ter uitvoering van het bevel vastgelegde gegevens*". Voor een onderscheid tussen een meer beperkt begrip 'onregelmatigheid' in art. 6 Bogw en een ruimer begrip 'onregelmatigheid' in de artikelen 23 en 24 Bogw geeft de totstandkomingsgeschiedenis van het Bogw echter geen reden. Niet eerder dan in de definitieve versie van het Bogw werd (ook) in art. 23 lid 4 en 24 lid 3 op advies van de Raad voor de Rechtspraak een verbaliseringsplicht opgenomen voor (naar de huidige terminologie) 'onregelmatigheden'. De toelichting op het Bogw geeft geen aanleiding om te veronderstellen dat met de in art. 23 lid 4 en art. 24 lid 3 genoemde 'onregelmatigheden' andere (met name: méér) onregelmatigheden worden bedoeld dan die zijn bedoeld in art. 6 lid 1 Bogw. Omdat de plaatsing van een technisch hulpmiddel (zie art. 23 lid 1 Bogw) en het verrichten van onderzoekshandelingen (zie art. 24 lid 1 Bogw) reeds worden bestreken door de loggingsverplichtingen van art. 5 lid 1 Bogw is ook de vraag wat de meerwaarde is van het (alsnog) opnemen van verbaliseringsplichten in art. 23 lid 4 en art. 24 lid 3 Bogw naast de in art. 6 lid 2 Bogw omschreven verbaliseringsplicht. Dat een verbaliseringsplicht van 'onregelmatigheden' niet (ook) is opgenomen in art. 25 Bogw (verwijdering technisch hulpmiddel) laat zich verklaren door de omstandigheid dat de verwijdering van een technisch hulpmiddel niet van invloed is op de betrouwbaarheid en integriteit van de ter uitvoering van het bevel vastgelegde gegevens.

363 Nota van toelichting op het Bogw, p. 17-18; *Kamerstukken I* 2016/17, 34 372, D (MvA I), p. 20.

364 Nota van toelichting op het Bogw, p. 36; *Kamerstukken II* 2018/19, 34 372, nr. 29 (verslag van een schriftelijk overleg), p. 11.

Inspectie Justitie en Veiligheid is deze vastlegging een van de belangrijkste bronnen op basis waarvan zij beoordeelt in hoeverre is gewerkt binnen de grenzen van het wettelijk kader en het bevel.[365]

3.11. De verbaliseringsplicht en het voegen van processen-verbaal bij de processtukken

Interne openbaarheid en rechterlijke controle

De opsporingsambtenaar is ingevolge artikel 152 Sv gehouden ten spoedigste proces-verbaal op te maken van de door hem verrichte handelingen.[366] Overeenkomstig 152 lid 2 Sv kan het opmaken van een proces-verbaal onder verantwoordelijkheid van het OM achterwege worden gelaten.

De officier van justitie is volgens artikel 126aa lid 1 Sv gehouden in de strafzaak verantwoording af te leggen over de inzet van bijzondere opsporingsbevoegdheden genoemd in de artikelen 126g tot en met 126zu Sv, dan wel de toepassing van artikel 126ff Sv. Dat geldt dus ook voor de uitoefening van de bevoegdheden van de artikelen 126nba, 126uba en 126zpa Sv. Daartoe voegt de officier van justitie processen-verbaal en andere voorwerpen waaraan gegevens kunnen worden ontleend die zijn verkregen door de inzet van de genoemde bevoegdheden bij de processtukken, maar alleen voor zover die voor het onderzoek in de zaak van betekenis zijn.[367] Niet slechts de gegevens die zijn verkregen door uitoefening van een bijzondere opsporingsbevoegdheid (dat wil zeggen: de onderzoeksresultaten daarvan), maar ook de wijze waarop die gegevens zijn verkregen moet in een proces-verbaal worden gerelateerd.[368] Op die manier wordt controle op de uitoefening van bevoegdheden mogelijk gemaakt. Uit de processtukken zal dus ook moeten blijken op grond van welke gegevens tot de inzet van een opsporingsbevoegdheid is besloten en of de uitvoering daarvan aan de wettelijke eisen heeft voldaan. Het schriftelijk bevel tot het uitvoeren van onderzoek in een geautomatiseerd werk en de machtiging worden bij de processtukken gevoegd.

Artikel 126aa lid 3 Sv maakt het mogelijk dat de voeging van de hiervoor bedoelde processen-verbaal en andere voorwerpen niet terstond, maar pas op een later moment plaatsvindt, te weten zodra het belang van het onderzoek dit toelaat.[369] Voeging vindt evenwel uiterlijk plaats op het door artikel 33 Sv bepaalde moment, te weten zodra de dagvaarding ter terechtzitting in eerste aanleg aan de verdachte is betekend dan wel aan hem een strafbeschikking is uitgevaardigd, behoudens het bepaalde in artikel 149b Sv (i.e. het op bepaalde gronden achterwege laten van voeging met machtiging van de rechter-commissaris).[370]

De verbaliseringsplicht in het Bogw

Onverminderd de verbaliseringsplicht als hiervoor omschreven, houdt de officier van justitie bij het samenstellen van het strafdossier in zaken waarin de bevoegdheid van artikel 126nba Sv is toegepast rekening met bijzondere belangen zoals de afscherming van opsporingsmethodieken en -middelen. Deze belangen kunnen een minder gedetailleerde verantwoording rechtvaardigen.[371]

---

365 Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2019*, Den Haag: Ministerie van Justitie en Veiligheid 2020, p. 21.

366 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 39. Zie ook art. 24 Bogw.

367 Met de woorden 'voor zover die gegevens voor het onderzoek in de zaak van betekenis zijn', wordt het relevantiecriterium tot uitdrukking gebracht. Vgl. *Kamerstukken II* 1996/97, 25 403, nr. 3 (MvT), p. 16 en p. 83; *Kamerstukken II* 2009/10, 32 468, nr. 3 (MvT), p. 17.

368 Zie bijv. *Kamerstukken II* 1997/98, 25 403, nr. 7 (NV II), p. 85; T. Blom in: *Tekst & Commentaar Strafvordering*, Deventer: Kluwer, art. 126aa, aant. 5 onder c (online, bijgewerkt tot 1 januari 2022).

369 *Kamerstukken II* 1996/97, 25 403, nr. 3 (MvT), p. 84.

370 Zie ook lid 4 van art. 126aa Sv. Verder hierover: G.J.M. Corstens, *Het Nederlands strafprocesrecht*, bewerkt door M.J. Borgers en T. Kooijmans, Deventer: Wolters Kluwer 2021, p. 619-620.

371 Nota van toelichting op het Bogw, p. 22 bovenaan.

Het Bogw en de nota van toelichting op het Bogw vermelden enkele verrichtingen waarover de verbaliseringsplicht zich in elk geval uitstrekt:

- Indien een onregelmatigheid wordt geconstateerd bij de voorgeschreven logging maakt een opsporingsambtenaar van een technisch team daarvan proces-verbaal op dat aan de officier van justitie wordt gezonden (artikel 6 lid 2 Bogw). De officier van justitie en de rechter beoordelen in hoeverre de geconstateerde onregelmatigheid afbreuk doet aan de bewijskracht van de gegevens.[372]
- De opsporingsambtenaar van het technische team maakt een proces-verbaal op van de plaatsing van het technisch hulpmiddel dat aan de officier van justitie wordt gezonden.[373] Indien bij de plaatsing van een technisch hulpmiddel een onregelmatigheid plaatsvindt, maakt de opsporingsambtenaar hiervan melding in het proces-verbaal (artikel 23 lid 3 en 4 Bogw).
- De opsporingsambtenaar maakt een proces-verbaal op van het verrichten van onderzoekshandelingen in het geautomatiseerde werk dat aan de officier van justitie wordt gezonden. Indien bij het verrichten van onderzoekshandelingen een onregelmatigheid plaatsvindt, maakt de opsporingsambtenaar hiervan melding in het proces-verbaal (artikel 24 lid 2 en 3 Bogw).
- De opsporingsambtenaar maakt een proces-verbaal op van de verwijdering van het technisch hulpmiddel dat aan de officier van justitie wordt gezonden (artikel 25 lid 3 Bogw). Indien een technisch hulpmiddel niet of niet volledig kan worden verwijderd uit een geautomatiseerd werk, maakt de opsporingsambtenaar daarvan proces-verbaal op. Dat proces-verbaal wordt aan de officier van justitie gezonden (artikel 26 lid 3 Bogw).
- Indien het nodig is om een selectie te maken uit de gegevens die op de technische infrastructuur zijn vastgelegd en het technische team daartoe een bewerking uitvoert met gebruikmaking van een forensische kopie van de gegevens, legt het technische team vast welke bewerkingen hebben plaatsgevonden in een proces-verbaal dat aan de officier van justitie wordt gezonden (artikel 29 lid 3 Bogw).[374]
- Als bij het verrichten van onderzoekshandelingen in een geautomatiseerd werk gebruik wordt gemaakt van een goedgekeurd technisch hulpmiddel, kan in het proces-verbaal van de inzet worden volstaan met een verwijzing naar het keuringsnummer (referentienummer). Daardoor kan de samenstelling van het hulpmiddel ter bescherming van de opsporingsbelangen worden afgeschermd.[375]
- Indien een niet-gekeurd technisch hulpmiddel wordt gebruikt, vermeldt de officier van justitie in het bevel dat toepassing wordt gegeven aan artikel 21 lid 2 Bogw. De officier van justitie vermeldt de uitkomst van de keuring of herkeuring na afloop van het gebruik in de processtukken (artikel 21 lid 3 Bogw).
- Indien geen (her)keuring plaatsvindt, dient de officier van justitie in de processtukken te vermelden welke aanvullende waarborgen zijn getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de met het technisch hulpmiddel vastgelegde gegevens te garanderen. Ook wordt in de processtukken vermeld dat toepassing is gegeven aan artikel 21 lid 4 Bogw.
- Indien de onderzoekshandelingen handmatig zijn verricht, vermeldt de officier van justitie in de processtukken welke procedurele waarborgen zijn getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de vastgelegde gegevens te kunnen garanderen (artikel 21 lid 5 Bogw).[376]

---

372 Nota van toelichting op het Bogw, p. 18.

373 Nota van toelichting op het Bogw, p. 21, p. 38: "*De keuringsdienst stelt bij de keuring een handleiding op voor het gebruik van een hulpmiddel, waarin wordt aangegeven welke instellingen bij gebruik van een technisch hulpmiddel voor een bepaalde functionaliteit moeten worden aangevinkt. Bij de plaatsing van een technisch hulpmiddel wordt hierover verantwoording afgelegd in een proces-verbaal.*" en p. 46: "*Het tweede lid vereist dat bij de plaatsing van een technisch hulpmiddel uitsluitend de in het bevel van de officier aangeduide functionaliteiten worden ingeschakeld. Hierover wordt verantwoording afgelegd in een proces-verbaal.*"

374 Nota van toelichting op het Bogw, p. 21.

375 Nota van toelichting op het Bogw, p. 22.

376 Vgl. de nota van toelichting op het Bogw, p. 22.

Behalve op de verbaliseringsplicht wordt in de nota van toelichting op het Bogw andermaal gewezen op de voorgeschreven logging, waarbij informatie over de inzet wordt vastgelegd. Bovendien wordt wat betreft het verschaffen van informatie in de nota van toelichting op het Bogw gewezen op de procedure zoals bedoeld in artikel 187d Sv:

> *"Indien tijdens de behandeling van een strafzaak twijfels zouden rijzen over de betrouwbaarheid en de integriteit van het verkregen bewijsmateriaal, kan de rechter de volledige informatie opvragen of een deskundige raadplegen. Hierbij staat de rechter de procedure zoals omschreven in artikel 187d Sv ter beschikking, waarin de rechter-commissaris kan beletten dat antwoorden op vragen ter kennis komen van de verdachte en diens raadsman, indien er een gegrond vermoeden bestaat dat door de openbaarmaking een zwaarwegend opsporingsbelang wordt geschaad."*[377]

3.12. De toepassing van de bevoegdheid op het grondgebied van een andere staat

De normering van internationale inzet van de bevoegdheid

Met behulp van het internet kunnen gegevens eenvoudig over grote afstanden worden getransporteerd en ingezien, ongeacht op welke fysieke locatie zij zich bevinden. Vanwege de afwezigheid van grenzen in cyberspace en het op anonimiteit gerichte internetgedrag van bepaalde personen, komt het zeer geregeld voor dat politie en justitie niet kunnen vaststellen op welke fysieke locatie gegevens zijn opgeslagen, worden verwerkt of overgedragen, terwijl de gegevens als zodanig wel benaderbaar en kenbaar zijn.[378] Het is dan niet uitgesloten dat de gegevens waartoe toegang kan worden verkregen, opgeslagen zijn op een server die zich bevindt in een ander land dan Nederland. Bij onderzoek in een geautomatiseerd werk is in zo'n geval het vraagstuk van de extraterritoriale rechtsmacht aan de orde.[379] De minister merkte hierover het volgende op in de memorie van toelichting:

> *"In reactie op deze adviezen merk ik op dat de rechtsmacht van een staat niet is beperkt tot het eigen grondgebied, de regels over de rechtsmacht in het Nederlandse Wetboek van Strafrecht zijn immers niet beperkt tot het beginsel van territorialiteit. Juist bij computercriminaliteit is het betrekkelijk eenvoudig om strafbare feiten te plegen waarbij vanuit meerdere landen wordt geopereerd. Hierbij is de vraag aan de orde in hoeverre opsporingshandelingen kunnen worden verricht met betrekking tot gegevens die zich in een andere jurisdictie bevinden, terwijl de staat die wenst te handhaven wel over extraterritoriale rechtsmacht beschikt. Op*

---

377 Nota van toelichting op het Bogw, p. 22.

378 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT) p. 42. Meer hierover: *Kamerstukken I* 2016/17, 34 372, D (MvA I), p. 33 en 38-40. Over deze materie gaat o.a.: B.J. Koops & M. Goodwin, *Cyberspace, de cloud, en grensoverschrijdende opsporing: De grenzen en mogelijkheden van internationaal recht*, Tilburg: TILT 2014; B.J. Koops, C. Conings & F. Verbruggen, *Zoeken in computers naar Nederlands en Belgisch recht. Welke plaats hebben de 'digitale plaatsen' in de systematiek van opsporingsbevoegdheden?* (Preadvies voor de jaarvergadering van de NVVS 2016), Oisterwijk: Wolf Legal Publishers 2016, p. 137 e.v.; J.J. Oerlemans, *Investigating cybercrime* (diss. Leiden), z.p., z.u., 2017, p. 416-417; J.J. Oerlemans, 'Jurisdictie en grensoverschrijdende digitale opsporing', in: B.J. Koops & J.J. Oerlemans (red.), *Strafrecht & ICT*, Den Haag: Sdu 2019, p. 209-232; Y. Buruma, 'International Law and Cyberspace - Issues of Sovereignty and the Common Good', in: M. Busstra, W. Theeuwen e.a., *International Law for a Digitalised World* (Preadviezen voor de Koninklijke Nederlandse Vereniging voor Internationaal Recht), Den Haag: Asser Press 2020, m.n. p. 95 e.v.; J.W. van den Hurk & S.J. de Vries, 'Waar worden gegevens in de 'cloud' opgeslagen en welke juridische consequentie heeft het antwoord op die vraag? Een speurtocht langs het traditionele juridisch kader en actuele wetgeving en jurisprudentie leidt tot een opmerkelijke conclusie', *Strafblad* 2019, afl. 4, p. 34-44.

379 Dit geldt volgens de minister overigens ook voor de bestaande bevoegdheden van de doorzoeking ter vastlegging van gegevens en de netwerkzoeking. Met de ontwikkeling van cloudcomputingdiensten is het belang van dit vraagstuk toegenomen. Het begrip rechtsmacht omvat twee componenten: de toepasselijkheid van de Nederlandse wet (wetgevende rechtsmacht) en het verrichten van handelingen door Nederlandse rechtshandhavingsautoriteiten met het oog op opsporing en vervolging in Nederland (uitvoerende rechtsmacht). Deze begrippen hangen met elkaar samen: uitvoerende rechtsmacht veronderstelt wetgevende rechtsmacht. Zie *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 43.

grond van het arrest van het Permanent Hof van Internationale Justitie, de voorloper van het Internationale Gerechtshof, in de zogenaamde Lotus-zaak kan worden aangenomen dat een staat slechts executieve rechtsmacht mag uitoefenen op het grondgebied van een andere staat met toestemming van die staat (Series A Nr 10 Leyden 1927). In casu betrof dit het optreden van opsporingsambtenaren in persoon op het grondgebied van een andere staat. De ontwikkeling van de informatie- en communicatietechnologie maakt het betrekkelijk eenvoudig om strafbare feiten te plegen waarbij de schadelijke gevolgen zich in andere landen manifesteren. Op grond van de wet (artikel 539a Sv) en de jurisprudentie bestaat er voor politie en justitie ruimte om, binnen de kaders van het volkenrecht en het interregionale recht, buiten de grenzen van het Nederlandse grondgebied op te treden. (…). Uit het vorenstaande mag uitdrukkelijk niet worden afgeleid, zoals de NOvA stelt, dat de territorialiteit van andere staten maar moet wijken voor het Nederlandse opsporingsbelang. Het internationaalrechtelijke kader en de bilaterale relaties met andere staten op het gebied van de rechtshulp staan hieraan in de weg, en Nederland hecht juist zeer veel waarde aan een gemeenschappelijk optreden van staten bij de bestrijding van de grensoverschrijdende criminaliteit. Het zelfstandig optreden van de rechtshandhavings-autoriteiten mag geen afbreuk doen aan bestaande afspraken en regels op het gebied van de rechtshulp. Als de locatie van de gegevens bekend is, dienen deze afspraken en regels te worden nageleefd.
(…).
Voor de opsporing van grensoverschrijdende ernstige strafbare feiten, waarbij gebruik wordt gemaakt van geautomatiseerde werken voor de verwerking en de opslag van gegevens, is het van essentieel belang dat gebruik kan worden gemaakt van onderzoeksbevoegdheden, ook wanneer dat betekent dat daarmee toegang wordt verkregen tot geautomatiseerde werken die zich buiten Nederland bevinden. De huidige wetgeving op het gebied van extraterritoriale strafvordering biedt daartoe reeds mogelijkheden binnen de grenzen van het volkenrecht. Daarbij dienen de afspraken en regels over de internationale rechtshulp in acht te worden genomen. Vanwege het grensoverschrijdende karakter van deze vormen van criminaliteit is het niet uitgesloten dat meerdere staten over rechtsmacht beschikken. Als staten dat van elkaar weten dan ligt onderling overleg over de meest geëigende aanpak in de rede. Als bekend is dat gegevens zich in een bepaalde andere rechtsmacht bevinden dan is rechtshulp aangewezen."[380]

De geldende doctrine over de extraterritoriale toepassing van opsporingsbevoegdheden houdt in dat het uitoefenen van strafvorderlijke bevoegdheden op het territorium van een andere staat niet zonder meer is toegestaan.[381] Dat zou in beginsel een inbreuk opleveren op de soevereiniteit van een andere staat.
Dat beginsel heeft ook te gelden voor het onderzoek in een geautomatiseerd werk. In de gevallen waarin kan worden aangenomen dat Nederland op grond van de artikelen 2 tot en met 8 Sr over rechtsmacht[382] beschikt, voorziet artikel 539a Sv in een wettelijke basis om opsporingshandelingen te verrichten buiten Nederland, voor zover het volkenrecht en het interregionale recht dit toelaten.[383] Binnen die kaders bestaat dus voor politie en justitie ruimte om buiten de grenzen van het Nederlandse grondgebied op te treden.[384]
Als de locatie van de gegevens bekend is, dienen de internationale afspraken en regels te worden nageleefd, met inbegrip van de regels die het verzoeken en verlenen van internationale rechtshulp normeren.[385]

---

380 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 49-50.
381 De norm is: soevereiniteit en non-interventie. Zie over deze twee beginselen van internationaal publiekrecht: M.N. Shaw, *International Law*, Cambridge: Cambridge University Press 2021, p. 555-559. Zie ook *Kamerstukken I* 2016/17, 34 372, D (MvA I), p. 33.
382 Op grond van het territorialiteits-, personaliteits- dan wel universaliteitsbeginsel, zie *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 43.
383 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 44.
384 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 49.
385 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 50; *Kamerstukken I* 2016/17, 34 372, D (MvA I), p. 33, 38-40.

De officier van justitie dient, indien daarover wetenschap bestaat, in het bevel te vermelden dat de gegevens niet in Nederland zijn opgeslagen. Dit geldt ook voor het geval dat niet bekend is waar de gegevens zijn opgeslagen. Hiermee wordt verzekerd dat het aspect van de inbreuk op de soevereiniteit van een andere staat onderwerp vormt van een expliciete afweging door de officier van justitie en de rechter-commissaris. Dit moet volgens de minister worden gezien als een extra waarborg voor een zorgvuldige voorbereiding van de inzet van de bevoegdheid.[386]

Als van de aangezochte staat geen toestemming is verkregen dan is het volgens de minister aan de strafrechter om te oordelen over de consequenties daarvan voor de strafzaak. Daarbij verwijst de minister naar jurisprudentie van de Hoge Raad waarin is bepaald dat de vraag of de Nederlandse opsporingsambtenaren het volkenrecht hebben nageleefd in beginsel niet relevant is voor de strafzaak tegen de verdachte, en dit op de grond dat de belangen die het volkenrecht in zoverre beoogt te beschermen niet de belangen van de verdachte betreffen, maar die van de staat op het grondgebied waarvan buitenlandse opsporingsambtenaren als zodanig optreden.[387]

Het Cybercrimeverdrag

Het Cybercrimeverdrag,[388] dat tot stand is gekomen onder de vlag van de Raad van Europa en behalve door de lidstaten van de Raad van Europa ook is ondertekend door onder meer de Verenigde Staten, Canada, Japan en Zuid-Afrika, bevat een specifieke regeling voor de grensoverschrijdende toegang tot computergegevens.[389] In dit verdrag wordt ervan uitgegaan dat in geval van overlappende rechtsmacht de desbetreffende verdragspartijen nader overleg voeren.[390]
In een tweetal gevallen is op basis van het verdrag de grensoverschrijdende toegang tot gegevens zonder de toestemming van een andere verdragspartij toegestaan.[391] Dit betreft in de eerste plaats de toegang tot openbare gegevens (uit open bronnen), ongeacht de locatie van de gegevens (artikel 32, onderdeel a, van het Cybercrimeverdrag). Dit betreft in de tweede plaats de toegang, door middel van een netwerkzoeking, tot gegevens die zijn opgeslagen op media die zich bevinden op het grondgebied van een andere verdragspartij, zulks voor zover dit plaatsheeft met de rechtmatige en vrijwillige instemming van de persoon die gerechtigd is de gegevens via het computersysteem aan de partij te verstrekken (artikel 32, onderdeel b, van het Cybercrimeverdrag).
Bij de onderhandelingen over de totstandkoming van het Cybercrimeverdrag kon echter geen overeenstemming worden bereikt over de voorwaarden waaronder in andere gevallen grensoverschrijdende toegang tot gegevens toegelaten is. In de praktijk blijkt bovendien dat opsporingsdiensten van verscheidene staten zich toegang verschaffen tot gegevens die zijn opgeslagen in geautomatiseerde werken die zich op het grondgebied van andere staten bevinden, zulks ten behoeve van het veiligstellen van elektronisch bewijs, en dit zonder dat het Cybercrimeverdrag daarvoor een grondslag biedt. In internationaal verband is dan ook vastgesteld dat het territorialiteitsbeginsel in cyberspace onder druk staat en

---

386 *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 56. Zie ook *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 44-50, en de nota van toelichting op het Bogw, p. 11.

387 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 47, met verwijzingen naar HR 5 oktober 2010, ECLI:NL:HR:2010:BL5629, en HR 17 april 2012, ECLI:NL:HR:2012:BV9070.

388 Het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, Boedapest, 23 november 2001, *Trb.* 2002, 18, en *Trb.* 2004, 290, kortweg het Cybercrimeverdrag. Zie hierover o.m. B.J. Koops, 'Het Cybercrimeverdrag, de Nederlandse strafwetgeving en de (computer)criminalisering van de maatschappij', *Computerrecht* 2003, afl. 2, p. 115-123.

389 Bepalingen over de wederzijdse bijstand met betrekking tot onderzoeksbevoegdheden zijn opgenomen in de artikelen 31 tot en met 35 van het Cybercrimeverdrag.

390 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 44.

391 Die verdragsbasis voor toegang tot gegevens heeft dus *in principe* (d.w.z. afgezien van de reflexwerking van het verdrag) alleen betrekking op het grondgebied van landen die partij zijn bij dit verdrag.

bovendien dat het beginsel niet kan worden nageleefd als de exacte locatie van gegevens onduidelijk is. In het kader van het multilaterale overleg binnen de Raad van Europa worden de mogelijkheden onderzocht voor het verbeteren van het vergaren van digitaal bewijs in de cloud en voor het versterken van de procedures voor rechtshulp bij digitale onderzoeken. Daarmee wordt dus de verhouding verkend tussen het grensoverschrijdend vastleggen van gegevens en de grenzen van uitvoerende rechtsmacht.[392]

De Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv

In afwachting van de verdere ontwikkeling van het internationaalrechtelijke kader voor de uitoefening van rechtsmacht bij de bestrijding van computercriminaliteit moet naar het oordeel van de minister zelfstandig kunnen worden opgetreden om te voorkomen dat het internet een vrijplaats wordt voor criminaliteit.[393] Dit kan met zich brengen dat opsporingshandelingen (moeten) worden verricht met betrekking tot gegevens die niet in Nederland zijn opgeslagen.
Voor dit handelen heeft het OM zelf toetsingscriteria opgesteld. Deze criteria zijn neergelegd in de Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv, afkomstig van het College van procureurs-generaal.[394] Hierop wordt teruggekomen in hoofdstuk 4.

3.13. De notificatieplicht en het bewaren en vernietigen van gegevens

De notificatieplicht van artikel 126bb Sv

Op grond van artikel 126bb Sv geldt een zogeheten 'notificatieplicht', dat wil zeggen een verplichting tot kennisgeving aan de betrokkene van de uitvoering van onderzoek in een geautomatiseerd werk dat bij hem in gebruik is. Op grond van deze verplichting dient de betrokkene in kennis te worden gesteld (i) van het feit dat op afstand heimelijk is binnengedrongen in een geautomatiseerd werk en (ii) van de daarbij toegepaste bevoegdheid, dat wil zeggen: van de verrichte onderzoekshandeling. Hierdoor kan de betrokkene op de hoogte komen van de toepassing van de bevoegdheid ingeval onderzoek in het geautomatiseerde werk heeft geleid tot de vastlegging of ontoegankelijkmaking van gegevens of tot het opnemen van gegevens. De betrokkene is doorgaans de verdachte; bij de toepassing van artikel 126nba Sv is dat (anders dan bij toepassing van artikel 126uba of artikel 126zpa Sv) ook een noodzakelijke voorwaarde. De mededelingsplicht bestaat ten opzichte van de burger op wiens rechten inbreuk wordt gemaakt.
Niet uitgesloten is dat een geautomatiseerd werk bij meer personen in gebruik is. Als de vastlegging van gegevens betrekking heeft op gegevens van een ander dan dient ook een notificatie uit te gaan aan de verantwoordelijke voor die gegevens.
De mededeling (notificatie) moet schriftelijk geschieden. De mededeling behoeft geen uitputtende opgave te bevatten van alle vastgelegde of ontoegankelijk gemaakte gegevens. Ook de reden van het onderzoek in het geautomatiseerde werk hoeft niet te worden vermeld.[395] Volstaan kan worden met een aanduiding van de aard van de betrokken gegevens, dat wil zeggen met een globale aanduiding die de betrokken persoon in staat stelt zelf te beoordelen of zijn rechten zijn geschonden.[396]

---

392 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 44-45.
393 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 50. Vgl. ook *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 15-16, waarin wordt gesproken over inspanningen in EU-context om tot oplossingen te komen, alsook meer uitgebreid *Kamerstukken I* 2016/17, 34 372, D (MvA I), p. 38-40.
394 *Stcrt.* 2019, 10277.
395 *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 85.
396 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 39-40, met verwijzing naar *Kamerstukken II* 1998/99, 26 671, nr. 3 (MvT), blz. 52.

De officier van justitie is gehouden tot de kennisgeving zodra het belang van het onderzoek dat toelaat. Het onderzoek in een geautomatiseerd werk wordt heimelijk verricht. Het belang van het onderzoek zal er daarom in de praktijk toe nopen dat de mededeling wordt uitgesteld. Uitstel van de mededeling kan ook aan de orde zijn bij een onderzoek in een andere strafzaak of bij een onderzoek tegen meer verdachten dat slechts ten dele afgerond is.[397] Notificatie is niet vereist als het proces-verbaal van de toepassing van een bijzondere opsporingsbevoegdheid bij de processtukken wordt gevoegd.[398] De kennisgeving blijft achterwege indien uitreiking van de mededeling redelijkerwijs niet mogelijk is.[399] Dit kan bijvoorbeeld het geval zijn als het gaat om gegevens in een buitenlands geautomatiseerd werk. Hoewel de notificatieplicht ook dan onverkort geldt, kan het zijn dat de betrokkenen niet getraceerd kunnen worden.[400]

Het bewaren en vernietigen van niet-gevoegde gegevens (artikel 126cc Sv)

Zolang de zaak niet is geëindigd, bewaart de officier van justitie ingevolge artikel 126cc lid 1 Sv de processen-verbaal en andere voorwerpen waaraan gegevens kunnen worden ontleend die zijn verkregen door observatie met behulp van een technisch hulpmiddel dat signalen registreert, het opnemen van vertrouwelijke communicatie, het opnemen van telecommunicatie of het vorderen van gegevens over een gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker, voor zover die niet bij de processtukken zijn gevoegd, en houdt hij deze ter beschikking van het onderzoek. Het verzamelen van informatie met behulp van de hier genoemde technische hulpmiddelen kenmerkt zich door de aselecte wijze waarop een grote hoeveelheid informatie over personen wordt verzameld en vastgelegd. Dat betekent dat niet alleen voor het onderzoek relevante informatie wordt vastgelegd, maar ook niet-relevante informatie, zowel over personen die wel, als over personen die niets van doen hebben met het strafbare feit. Dit is de reden dat artikel 126cc regels stelt omtrent de bewaring en vernietiging van processen-verbaal en andere voorwerpen die informatie behelzen die is vastgelegd met dergelijke technische hulpmiddelen en die niet bij de processtukken zijn gevoegd.[401]
Zodra twee maanden zijn verstreken nadat de zaak is geëindigd en volledig aan de notificatieplicht is voldaan, doet de officier van justitie de processen-verbaal en andere voorwerpen als hiervoor bedoeld vernietigen (lid 2 van artikel 126cc Sv).[402]Van de vernietiging wordt proces-verbaal opgemaakt. Met een zaak die is geëindigd wordt gelijkgesteld een voorbereidend onderzoek dat naar redelijke verwachting niet tot een zaak zal leiden (artikel 126cc lid 3 Sv). Zodra blijkt dat gegevens die zijn vastgelegd tijdens een onderzoek in een geautomatiseerd werk van geen betekenis zijn voor het onderzoek, worden zij vernietigd (artikel 126cc lid 6 Sv).
Van vernietiging kan worden afgezien als de officier van justitie op grond van artikel 126dd Sv bepaalt dat de gegevens dienen te worden bewaard ten behoeve van een ander strafrechtelijk onderzoek dan waartoe de bevoegdheid is uitgeoefend of ten behoeve van het verkrijgen van inzicht in de betrokkenheid van personen bij misdrijven en handelingen als bedoeld in artikel 10 lid 1, onderdelen a en b, van de Wet politiegegevens.[403]

Gegevens waaromtrent een verschoningsrecht kan worden uitgeoefend

Zoals gezegd (zie paragraaf 3.11) voegt de officier van justitie overeenkomstig artikel 126aa lid 1 Sv bij de processtukken de processen-verbaal en andere voorwerpen waaraan gegevens

397 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 40; *Kamerstukken II* 1996/97, 25 403, nr. 3 (MvT), p. 84-85.
398 *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 81.
399 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 104.
400 *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 85.
401 T. Blom in: *Tekst & Commentaar Strafvordering*, Deventer: Kluwer, art. 126cc, aant. 3 (online, bijgewerkt tot 1 januari 2022), en zie ook: *Kamerstukken II* 1996/97, 25 403, nr. 3 (MvT), p. 86.
402 Zie ook art. 3 lid 1 van het Besluit bewaren en vernietigen niet-gevoegde stukken.
403 Zie hierover meer: *Kamerstukken I* 2016/17, 34 372, D (MvA I), p. 41-42.

kunnen worden ontleend die zijn verkregen door de uitoefening van een van de bijzondere opsporingsbevoegdheden genoemd in de artikelen 126g tot en met 126zu Sv, dan wel door de toepassing van artikel 126ff Sv, zulks voor zover die gegevens voor het onderzoek in de zaak van betekenis zijn. Dat geldt dus ook voor de resultaten van het onderzoek in een geautomatiseerd werk.

Artikel 126aa lid 2 Sv formuleert een uitzondering op deze regel. Het artikel voorziet in de verplichting tot vernietiging van processen-verbaal en andere voorwerpen die mededelingen behelzen gedaan door of aan een persoon die zich op grond van artikel 218 of artikel 218a Sv kan verschonen indien hem als getuige naar de inhoud van die mededelingen zou worden gevraagd.[404] Artikel 218 Sv bepaalt dat personen die uit hoofde van hun beroep of ambt tot geheimhouding verplicht zijn, zich kunnen verschonen van de verplichting tot het afleggen van getuigenis omtrent hetgeen hun in die hoedanigheid ("*als zoodanig*") is toevertrouwd. De in artikel 218 Sv bedoelde personen worden doorgaans 'professionele geheimhouders' of 'functioneel verschoningsgerechtigden' genoemd, te weten zij die uit hoofde van hun stand, hun beroep of hun ambt tot geheimhouding verplicht zijn, zoals een arts, een psycholoog, een geestelijk verzorger of een advocaat. Een advocaat komt daarom alleen een verschoningsrecht toe in het kader van zijn juridische dienstverlening aan degene die zich tot hem heeft gewend vanwege zijn hoedanigheid van advocaat. Ook informatie die nog niet aan de advocaat is medegedeeld, kan in uitzonderingsgevallen object uitmaken van het verschoningsrecht van de advocaat. Daarvoor is van belang of op grond van in aanmerking komende feiten of omstandigheden aannemelijk is dat de informatie daadwerkelijk bestemd is om door de cliënt aan de advocaat in de uitoefening van zijn beroep te worden toevertrouwd.[405]
Artikel 218a Sv heeft aan de in artikel 218 Sv bedoelde personen sedert 1 oktober 2018 met het oog op bronbescherming toegevoegd: de journalist of publicist die in het kader van nieuwsgaring beschikt over gegevens van personen die deze gegevens ter openbaarmaking hebben verstrekt.

---

404 Naar de letter genomen schrijft art. 126aa lid 2 Sv de vernietiging voor van 'processen-verbaal en andere voorwerpen' voor zover zij geprivilegieerde mededelingen behelzen. Uit art. 5 leden 1 en 2 van het Besluit bewaren en vernietigen niet-gevoegde stukken volgt dat, als geprivilegieerde gegevens zijn opgeslagen op een (afzonderlijke) gegevensdrager of ander voorwerp, ook van de vernietiging van die gegevens sprake is als die gegevens 'niet meer kenbaar zijn'. Hoewel in die artikelleden wordt gesproken over de bewerking van de 'gegevensdrager' of het 'voorwerp', is gelet op de strekking van deze voorschriften niet uitgesloten dat ook door de bewerking van de digitale voorziening waarmee de gegevens raadpleegbaar zijn, kan worden bereikt dat die gegevens 'niet meer kenbaar zijn' in de zin van die artikelleden, aldus oordeelde de Hoge Raad in HR 20 september 2022, ECLI:NL:HR:2022:1257.
In dat verband kan ook worden gewezen op de redactie van de beoogde opvolger van art. 126aa lid 2 Sv, te weten art. 2.8.3 lid 1 van het Wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering (ambtelijke versie, juli 2020): "*Indien door de uitoefening van een van de in dit hoofdstuk opgenomen bevoegdheden gegevens zijn verkregen die mededelingen behelzen gedaan door of aan een persoon die zich op grond van artikel 1.6.7 of 1.6.8 zou kunnen verschonen indien hem als getuige naar de inhoud van die mededelingen zou worden gevraagd, worden deze gegevens vernietigd.*" Zie hierover tevens de bijbehorende memorie van toelichting (ambtelijke versie, juli 2020), p. 461 en p. 489, waaraan valt te ontlenen dat met de wijziging van de termen 'processen-verbaal en andere voorwerpen' in het begrip 'gegevens' de strekking van deze bepaling niet is veranderd.
Zie voor relativerende opmerkingen over de betekenis van de begrippen 'vernietigen van gegevens' en 'niet-meer-kenbaar zijn van gegevens' eveneens die memorie van toelichting, p. 489-490, waaraan onder meer valt te ontlenen: "*(…). Het voorgaande maakt duidelijk dat aan de ene kant secuur moet worden omgegaan met geheimhoudersinformatie (niet beschikbaar voor de opsporing); aan de andere kant kost daadwerkelijke vernietiging hiervan (indien al mogelijk) enorm veel tijd en kan dit problemen opleveren voor de integriteit en authenticiteit van andere opgeslagen data die nog wel door de opsporing mag worden gebruikt. Met het oog op de uitvoerbaarheid voor de praktijk moet de term "vernietigen" in de zin van het eerste lid functioneel worden uitgelegd; de opsporing moet er alles aan doen om te zorgen dat geheimhoudersinformatie niet meer zichtbaar is voor het opsporingsteam en niet meer gebruikt kan worden. Dit proces moet achteraf altijd goed te reconstrueren zijn. Door middel van loggings moet worden bijgehouden wat er met de gegevens is gebeurd.*" (Citaat p. 490 bovenaan).

405 HR 9 februari 2021, ECLI:NL:HR:2021:193, *NJ* 2021/119; HR 25 november 2016, ECLI:NL:HR:2016:2686; HR 10 november 2015, ECLI:NL:HR:2015:3258, en HR 12 oktober 2010, ECLI:NL:HR:2010:BN0526.

Met het voorschrift van artikel 126aa lid 2 Sv is beoogd het belang te beschermen dat eenieder de mogelijkheid heeft om vrijelijk en zonder vrees voor openbaarmaking van wat aan – onder anderen – de advocaat in diens hoedanigheid wordt toevertrouwd, een advocaat te raadplegen.[406] Het voorschrift strekt ertoe dat gegevens die als gevolg van de toepassing van de bevoegdheden genoemd in artikel 126aa lid 1 Sv zijn verkregen, onmiddellijk worden vernietigd indien zij vallen onder het verschoningsrecht als bedoeld in artikel 218 Sv, zodat is verzekerd dat die gegevens geen deel uitmaken van de processtukken en dat daarop in het verdere verloop van het strafproces geen acht wordt geslagen. Uit artikel 126aa lid 2 Sv vloeit derhalve voort dat gegevens als in die bepaling bedoeld niet in het strafproces kunnen worden gebruikt.[407]

De procedure voor de vernietiging van de vastgelegde gegevens is uitgewerkt in het Besluit bewaren en vernietigen niet-gevoegde stukken, waarvan met name de artikelen 4 en 4a.[408] Deze regeling houdt het volgende in. De opsporingsambtenaar die door de uitoefening van een van de bijzondere opsporingsbevoegdheden van de artikelen 126g tot en met 126zu Sv (met inbegrip dus van de artikelen 126nba, 126uba en 126zpa Sv) kennisneemt van mededelingen waarvan hij weet of redelijkerwijs kan vermoeden dat deze zijn gedaan door of aan een geheimhouder, stelt hiervan de officier van justitie onverwijld in kennis.[409] Indien de officier van justitie (vervolgens) vaststelt dat deze mededelingen onder het verschoningsrecht vallen, beveelt hij terstond de vernietiging van de processen-verbaal en andere voorwerpen, voor zover zij deze mededelingen behelzen.[410] Toegesneden op artikel 126nba Sv geldt dus dat zodra de officier van justitie vaststelt dat bij het onderzoek in een geautomatiseerd werk (al dan niet met behulp van een technisch hulpmiddel) gegevens worden vastgelegd die betrekking hebben op communicatie tussen bijvoorbeeld de verdachte en zijn advocaat of tussen de verdachte en zijn arts, de officier van justitie terstond de vernietiging beveelt van de opgenomen en vastgelegde gegevens voor zover deze onder de geheimhoudingsplicht vallen.[411]
Het bevel tot vernietiging is schriftelijk. Van de vernietiging wordt proces-verbaal opgemaakt, dat wordt gezonden aan de officier van justitie.[412]

---

406 Het functionele verschoningsrecht van art. 218 en 218a Sv vindt volgens de Hoge Raad zijn grondslag in een in Nederland geldend 'algemeen rechtsbeginsel' dat meebrengt dat bij vertrouwenspersonen, zoals advocaten, het maatschappelijk belang dat de waarheid in rechte aan het licht komt, moet wijken voor "*het maatschappelijk belang dat een ieder zich vrijelijk en zonder vrees voor openbaarmaking van het besprokene om bijstand en advies tot hen moet kunnen wenden.*" Zie HR 1 maart 1985, ECLI:NL:HR:1985:AC9066, *NJ* 1986/173 m.nt. Haardt onder *NJ* 1986/176; zie ook: HR 10 april 2018, ECLI:NL:HR:2018:553, *NJ* 2018/453; HR 16 juni 2020, ECLI:NL:HR:2020:1048, *NJ* 2021/117; HR 9 februari 2021, ECLI:NL:HR:2021:193, *NJ* 2021/119, en HR 20 september 2022, ECLI:NL:HR:2022:1257. In de memorie van toelichting bij het Wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering (ambtelijke versie, juli 2020) wordt deze jurisprudentie als volgt samengevat (p. 455-456): "*Het komt, kort samengevat, erop neer dat een hulpzoekende niet moet worden weerhouden van het vragen van advies aan en bijstand door bepaalde hulpverleners – de arts, de advocaat, de notaris en de geestelijke – uit vrees dat wat tussen hem en de hulpverlener wordt besproken op enig moment openbaar zou worden. Dat uitgangspunt zou niet alleen worden ondergraven wanneer de verschoningsgerechtigde over deze communicatie zou moeten verklaren, maar ook wanneer bijvoorbeeld van de correspondentie tussen de verschoningsgerechtigde hulpverlener en zijn cliënt of patiënt zonder nadere waarborgen kennis zou kunnen worden genomen. In het verlengde van het verschoningsrecht van de getuige ligt dus dat ook van datgene wat in het contact tussen de verschoningsgerechtigde hulpverlener en hulpzoekende schriftelijk is vastgelegd, in beginsel geen kennis kan worden genomen door de justitiële autoriteiten.*"

407 Daaraan kan worden toegevoegd dat geprivilegieerde gegevens evenmin mogen worden gebruikt in enig opsporingsonderzoek. Zie ook de hierboven genoemde memorie van toelichting bij het Wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering (ambtelijke versie, juli 2020), p. 489: "*Het gaat erom dat de gegevens (het gesprek) worden vernietigd, omdat die niet in het onderzoek mogen worden gebruikt.*"

408 Volledig: Besluit van 15 december 1999, houdende regels ter uitvoering van de artikelen 126aa, tweede lid, en 126cc, vierde lid, van het Wetboek van Strafvordering (Besluit bewaren en vernietigen niet-gevoegde stukken), *Stb.* 1999, 548.

409 Artikel 4 lid 1 Besluit bewaren en vernietigen niet-gevoegde stukken. Opmerkelijk is dat deze bepaling zich naar de letter genomen niet uitstrekt tot gegevens die zijn verkregen door de toepassing van artikel 126ff Sv (doorlating).

410 Artikel 4 lid 2 Besluit bewaren en vernietigen niet-gevoegde stukken.

411 Zie *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 17-18, en *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 33-34.

412 *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 37.

Voor zover de processen-verbaal of andere voorwerpen mededelingen behelzen die weliswaar zijn gedaan door of aan een geheimhouder, maar die naar het oordeel van de officier van justitie niet onder het verschoningsrecht vallen, dan worden zij ingevolge artikel 126aa lid 2, laatste volzin, Sv niet bij de processtukken gevoegd dan na voorafgaande machtiging door de rechter-commissaris. Voeging bij de processtukken van processen-verbaal of andere voorwerpen die mededelingen behelzen die zijn gedaan door of aan een geheimhouder is dus afhankelijk gesteld van het oordeel van de rechter-commissaris over de vraag of deze mededelingen onder het verschoningsrecht vallen.[413]
In de gevallen waarin de geheimhouder zelf verdachte is, wint de officier van justitie het oordeel in van een gezaghebbend lid van de beroepsgroep waartoe de geheimhouder behoort omtrent de vraag of de mededelingen onder het verschoningsrecht vallen. Indien de officier van justitie besluit af te wijken van het oordeel van het gezaghebbende lid van de beroepsgroep, wordt dit besluit met redenen omkleed.
Het Besluit bewaren en vernietigen niet-gevoegde stukken voorziet eveneens in het afgeven van generieke bevelen (artikel 4 lid 4) en in een regeling van (telefoon)nummerherkenning voor advocaten (artikel 4a). Indien bij het aftappen en opnemen van telecommunicatie een nummer is betrokken dat door de Nederlandse orde van advocaten bij de politie is aangemeld, dan wordt het opnemen van de communicatie onmiddellijk beëindigd. Indien communicatie is opgenomen voordat het nummer is herkend, worden de gegevens van de communicatie onmiddellijk langs geautomatiseerde weg vernietigd.[414] Omtrent andere communicatie dan via een telefoon is het volgens de minister technisch nog niet te realiseren om de logging van de keylogger uit te schakelen zodra de verdachte een bericht verstuurt aan zijn advocaat. Daarvoor is het nodig dat het e-mailadres van de advocaat door de keylogger wordt herkend. Daarna kan het vastleggen van gegevens worden afgebroken.[415]

Op gespannen voet met de hiervoor besproken regeling van artikel 126aa lid 2 Sv en artikel 4 van het Besluit bewaren en vernietigen niet-gevoegde stukken staat het bepaalde in artikel 7 en artikel 28 Bogw. Waar de eerste twee genoemde bepalingen de (nagenoeg onmiddellijke) vernietiging voorschrijven van de bij het onderzoek vastgelegde gegevens waaromtrent een verschoningsrecht kan worden uitgeoefend,[416] stipuleert artikel 7 lid 1 Bogw dat de inhoud van de logging, met inbegrip dus van de bewijslogging, *niet* wordt gewijzigd en dicteert artikel 28 lid 1 Bogw dat er geen wijzigingen worden aangebracht in de inhoud van de gegevens die bij een onderzoek in een geautomatiseerd werk op een technische infrastructuur zijn vastgelegd. Deze bepalingen strekken ertoe de betrouwbaarheid, de integriteit en de herleidbaarheid van de bij dit onderzoek verkregen gegevens te garanderen. Voor gegevens waarover het verschoningsrecht zich uitstrekt is in het Bogw niet voorzien in een uitzondering op de regel dat geen wijzigingen mogen worden aangebracht in de bewijslogging, respectievelijk de gegevens die op een technische infrastructuur zijn vastgelegd.
In het Bogw en de bijbehorende nota van toelichting wordt bij deze ongerijmdheid niet stilgestaan. Op dit onderwerp wordt teruggekomen in paragraaf 4.3.

---

413 Vgl. de rol die de rechter-commissaris bij een doorzoeking ter inbeslagneming is toebedeeld in art. 98 lid 1 Sv.
414 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 17-18, en *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 17.
415 *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 39.
416 In de memorie van toelichting (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 17-18) komt de geheimhoudersproblematiek wel, zij het kort, aan de orde. Nadat daarin is opgemerkt dat de regeling van art. 126aa lid 2 Sv betrekking heeft op gegevens die ter kennis van de opsporingsambtenaren komen in het kader van de uitoefening van bijzondere opsporingsbevoegdheden jegens anderen dan de verschoningsgerechtigden, en dat de regeling ook van toepassing is op het onderzoek in een geautomatiseerd werk, wordt zonder voorbehoud gesteld: "*Dit betekent dat zodra bij het onderzoek in een geautomatiseerd werk met het technische hulpmiddel gegevens worden vastgelegd die betrekking hebben op communicatie tussen de verdachte en zijn raadsman of tussen de verdachte en zijn arts wordt, de opgenomen en vastgelegde gegevens worden vernietigd voor zover deze onder de geheimhoudingsplicht vallen.*" Wat betreft de hiervoor beschreven regeling van nummerherkenning van art. 4a van het Besluit bewaren en vernietigen niet-gevoegde stukken zet de minister in de memorie van toelichting uiteen: "*In reactie op de wens van de NOvA, dat de procedure van nummerherkenning ook wordt gewaarborgd bij het onderzoek in een geautomatiseerd werk, kan worden bevestigd dat dit inderdaad het geval is voor het aftappen en opnemen van telecommunicatie.*"

3.14. Het toezicht op de uitvoering van het bevel

Het toezicht op de politie en het toezicht op het OM

Tijdens de uitvoering van het bevel tot onderzoek in een geautomatiseerd wordt toezicht uitgeoefend door de leidinggevende functionarissen binnen de opsporingsdienst en door de betrokken officier van justitie.[417] Ingevolge de artikelen 132a en 148 Sv en artikel 12 Politiewet 2012 komt het gezag over de verrichtingen van opsporingsambtenaren in dit verband toe aan de officier van justitie. De officier van justitie dient dan ook toezicht te houden op de uitvoering van het bevel.[418]

Het toezicht door de Inspectie Justitie en Veiligheid en het toezicht door de procureur-generaal bij de Hoge Raad

In meer algemene zin is er tegelijkertijd nadrukkelijk ook een rol weggelegd voor de Inspectie Justitie en Veiligheid (hierna ook: de Inspectie) en de procureur-generaal bij de Hoge Raad (opnieuw: PG-HR). De minister heeft toezicht op het gebruik van de voorgestelde bevoegdheid in zijn algemeenheid wenselijk geacht. Daarbij heeft de minister vooral het oog op de Inspectie Justitie en Veiligheid, die als rijksinspectie belast is met het toezicht op de kwaliteit van de taakuitvoering door organisaties werkzaam op het terrein van justitie en veiligheid.[419] Overeenkomstig het bepaalde in de artikelen 65, 66 en 67 van de Politiewet 2012 oefent de Inspectie toezicht uit op de taakuitvoering door de politie, zij het "*onverminderd het gezag van (…) de officier van justitie*". De Inspectie kan dus ook toezicht houden op de uitvoering van het bevel tot onderzoek in een geautomatiseerd werk door de politie.[420] Volgens lid 7 van artikel 126nba Sv oefent de Inspectie tevens toezicht uit op de uitvoering van een dergelijk bevel door andere opsporingsambtenaren dan die van de politie en de Koninklijke marechaussee.[421]

Het door de Inspectie uitgeoefende toezicht heeft betrekking op de naleving van de wettelijke regels en voorschriften rond de toepassing van het onderzoek in een geautomatiseerd werk die zijn neergelegd in het Wetboek van Strafvordering en in het Besluit onderzoek in een geautomatiseerd werk.[422] Het toezicht van de Inspectie is zodoende gericht op het functioneren van het wettelijke systeem rond het onderzoek in een geautomatiseerd werk (systeemtoezicht).

De uitoefening van het toezicht is beperkt tot de uitvoering van de bevoegdheid binnen de grenzen van het bevel van de officier van justitie en de machtiging van de rechter-commissaris. De oordeelsvorming door de officier of de rechter-commissaris, zoals deze tot uitdrukking komt in het bevel respectievelijk de machtiging, valt buiten dit toezichtkader.[423]

Het externe toezicht op de beslissingen en het handelen van de officier van justitie en het OM in het algemeen is voorbehouden aan de PG-HR en, zodra het tot een strafzaak komt, de rechter ter terechtzitting.[424] Mocht de Inspectie bij de uitoefening van het toezicht in aanraking komen met mogelijke schendingen van de wettelijke voorschriften door of in opdracht van een officier van justitie, dan kan het hoofd van de Inspectie de PG-HR hierover informeren. Indien naar het oordeel van de PG-HR het OM bij de uitoefening van zijn taak de wettelijke

---

417 *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 59.
418 *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 84.
419 *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 81-82; *Handelingen I* 2017/18, nr. 34, item 5, p. 19.
420 Zie de nota van toelichting op het Bogw, p. 23-24, en 49.
421 Volledig: de ambtenaren, bedoeld in art. 141, onderdeel d, en de personen, bedoeld in art. 142 lid 1, onderdeel b.
422 *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 82. Het op deze pagina genoemde 'Besluit technische hulpmiddelen Strafvordering' dient te worden gelezen als: Besluit onderzoek in een geautomatiseerd werk, en dit omdat het oorspronkelijke voorstel om eerstgenoemd besluit aan te passen later is gewijzigd in het voorstel tot het invoeren van een geheel nieuw op de bevoegdheid toegesneden Besluit onderzoek in een geautomatiseerd werk.
423 Zo volgt uit de artt. 65-67 Politiewet 2012. Zie ook *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 82; *Kamerstukken I* 2016/17, 34 372, D (MvA I), p. 8, en p. 30-33.
424 *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 82.

voorschriften niet naar behoren handhaaft of uitvoert, kan hij de minister daarvan in kennis stellen (artikel 122 lid 1 RO).[425]

Samenvatting toezicht

Uit bovenstaande volgt dat de Inspectie Justitie en Veiligheid toezicht houdt op de uitvoering van het bevel van de officier van justitie door de politie, waarbij – naast wet- en regelgeving – het bevel van de officier van justitie geldt als normatief kader waaraan het politieoptreden dient te worden getoetst. Het toezicht van de Inspectie ontslaat het OM en de officier van justitie in het concrete geval niet van de plicht om zelf toezicht uit te oefenen op de inzet van de bevoegdheid. Ook de officier van justitie zal ervoor moeten waken dat de uitvoering van het bevel binnen de grenzen van de wet en van dat bevel blijft. Tegelijkertijd zijn de beslissingen die de officier van justitie in dat kader neemt onderhevig aan toezicht door de PG-HR.

3.15. Conclusie over het normatieve kader

Hiervoor is ter beantwoording van de eerste deelvraag een schets gegeven van de regels en waarborgen die de uitvoering van onderzoek in een geautomatiseerd werk omringen. Het betreft uitsluitend een bespreking van het nationaalrechtelijke kader voor zover dat is toegesneden op het hier besproken onderzoek. Deze bespreking verantwoordt tevens de items die in dit toezichtonderzoek (in het bijzonder het dossieronderzoek) worden getoetst.
De normen die zijn neergelegd in het Besluit onderzoek in een geautomatiseerd werk dragen volgens de minister een kaderstellend karakter en laten ruimte voor invulling in de praktijk. Niettemin maakt de hiervoor weergegeven schets van dit regelkader duidelijk dat de bevoegdheid die in de artikelen 126nba lid 1, 126uba lid 1 en 126zpa lid 1 Sv aan de officier van justitie is toegekend (op sommige punten) betrekkelijk minutieus is geregeld. Dat bergt het risico van een zekere starheid in zich, die het OM beperkt in de ruimte om in te spelen op nieuwe ontwikkelingen of om rekening te houden met de omstandigheden van het geval. Het is vervolgens de vraag op welke manier het OM dit regelkader toepast en daaraan nadere invulling geeft. Hierop wordt ingegaan in de volgende hoofdstukken.

[425] *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 83.

4. Het door het OM nader vormgegeven formele beleid

In dit hoofdstuk wordt het door het OM vormgegeven en geïmplementeerde beleidskader voor de toepassing van de bevoegdheid tot onderzoek in een geautomatiseerd werk beschreven, als bedoeld in de artikelen 126nba, 126uba en 126zpa Sv (hierna samengevat als: art. 126nba Sv). Het gaat dus niet om het materieel-wettelijke kader dat is beschreven in hoofdstuk 3, maar om het kader dat het OM voor zichzelf, dat wil zeggen: voor toepassing binnen de eigen organisatie, in het leven heeft geroepen. Daarmee valt de vraag of het door het OM vormgegeven en geïmplementeerde kader verenigbaar is met het in hoofdstuk 3 beschreven wettelijke kader in beginsel binnen het bereik van het toezicht van de PG-HR.

Een belangrijk onderdeel van het beleidskader is thans de op 15 oktober 2021 in werking getreden 'Instructie voor de inzet van de bevoegdheid ex artt. 126nba, 126uba, 126zpa en 126ffa Sv', van het College van procureurs-generaal (hierna ook: de Instructie).[426] Aangezien het toezichtonderzoek zich heeft uitgestrekt over de periode van 2019 tot en met 2021, wordt begonnen met een bespreking van de kaders voor de werkprocessen bij de uitoefening van de bevoegdheid voorafgaand aan de inwerkingtreding van de Instructie.

4.1. Het kader voor de werkprocessen inzake de uitoefening van de bevoegdheid

De werkprocessen in de periode voorafgaand aan de inwerkingtreding van de Instructie

Met ingang van 1 maart 2019, de datum van inwerkingtreding van de Wet computercriminaliteit III, is de officier van justitie bevoegd tot het bevelen van onderzoek in een geautomatiseerd werk. In de eerste zaak waarin deze bevoegdheid is uitgeoefend liep het tactisch politieonderzoek op dat moment meer dan een jaar. De toepassing van de bevoegdheid werd door het OM en de politie in deze zaak voorbereid in een periode die voorafging aan de inwerkingtreding van Wet computercriminaliteit III, zodat de officier van justitie, daartoe gemachtigd door de RC, het bevel binnen een week na de genoemde datum kon afgeven. Op dat moment hadden het OM en de Nationale politie in hun organisaties een werkwijze geïmplementeerd die hieronder ter sprake komt.[427]

De betrokken functionarissen

Voor de leesbaarheid van de hierna volgende teksten wordt eerst een beschrijving gegeven van de functionarissen en organisatieonderdelen die bij de uitoefening van de bevoegdheid betrokken (kunnen) zijn (zoals heeft gegolden in de onderzoeksperiode 2019 tot en met 2021):[428]

- Het technische team (als bedoeld in het Bogw) waarvan de leden uitvoering geven aan een bevel van de officier van justitie op de voet van artikel 126nba, 126uba of 126zpa Sv. Hoewel de regelgeving ruimte laat voor het formeren van meer dan één technisch team, heeft de politie tot nog toe volstaan met het samenstellen van één landelijk technisch team. De leden van dit technische team zijn organisatorisch ondergebracht bij 'Digit', een verkorting van: *digital intrusion team*. Digit betreft een onderdeel van de dienst specialistische operaties (DSO) van de landelijke eenheid van de Nationale

[426] Zie https://www.om.nl/onderwerpen/beleidsregels/aanwijzingen/opsporing---politie/instructie-voor-de-inzet-van-de-bevoegdheid-ex.-artt.-126nba-126uba-126zpa-en-126ffa-sv.

[427] Zie de brief van 29 september 2021 van de voorzitter van het College van procureurs-generaal aan de hoofden van de OM-onderdelen, PaG/B&S/18711, p. 2.

[428] Het OM heeft bij de afronding van het rapport te kennen gegeven dat nadien wijzigingen zijn opgetreden. Zo zijn er per 1 januari 2022 een landelijk officier van justitie hightech cybercrime bij het landelijk parket en per 1 juli 2022 een landelijk officier van justitie cybercrime bij het arrondissementsparket Den Haag aangesteld. Per 1 januari 2022 wordt de digit-parketsecretaris 'senior adviseur' genoemd. Per medio 2022 zijn naast de officier van justitie en de beleidsmedewerker, twee senior adviseurs verbonden aan LP Digit.

politie.[429] Het technische team wordt hieronder voor het leesgemak vereenzelvigd met de organisatorische eenheid Digit.[430]

- De cyberofficier (ook: cyber-OvJ): op elk parket van het OM fungeert een officier van justitie als aanspreekpunt voor kennis op het terrein van computercriminaliteit en digitale opsporingsmethoden.
- Er is één landelijke cyberofficier, een officier van justitie (verbonden aan het landelijk parket) die binnen het OM het landelijke aanspreekpunt is op het terrein van computercriminaliteit en digitale opsporingsmethoden.
- De digit-officier (digit-OvJ): de landelijk officier van justitie voor *digital intrusion* (verbonden aan het landelijk parket) geeft functioneel leiding aan Digit. De digit-officier is eventueel aanwezig bij de uitvoering van het onderzoek in een geautomatiseerd werk en fungeert als rechtstreeks aanspreekpunt binnen het OM voor Digit.[431]
- De digit-parketsecretaris: deze parketsecretaris (werkzaam voor het landelijk parket) staat de digit-officier met raad en daad bij.
- Tezamen met een senior-beleidsadviseur vormen de digit-officier en de digit-parketsecretaris het bureau 'LP Digit' ('LP' staat voor: landelijk parket).
- De zaaksofficier (ook wel: zaaks-OvJ): dit kan iedere officier van justitie betreffen, verbonden aan een parket van het OM, onder wiens gezag door een tactisch politieteam in een strafzaak onderzoek wordt verricht. Het bevel ex art. 126nba, 126uba of 126zpa Sv is afkomstig van de zaaksofficier (zie hieronder).
- De rechercheofficier: aan elk parket van het OM is een (meestal zeer) ervaren senior officier van justitie A verbonden die als rechercheofficier gevraagd en ongevraagd adviezen geeft en inhoudelijk toezicht houdt op de kwaliteit van de operationele rechercheonderzoeken onder het gezag van de officieren van justitie binnen het parket waaraan hij is verbonden.
- Er zijn twee rechercheofficieren, lid van het landelijk parket, die de rol van rechercheofficier vervullen voor zaken die worden behandeld door het landelijk parket.
- De hoofdofficier van justitie: iedere hoofdofficier van justitie van een parket van het OM.

De interne notitie

Op vragen naar beleidskaders omtrent de gangbare werkprocessen binnen het OM heeft de digit-officier bij aanvang van het toezichtonderzoek een notitie overhandigd van 1 maart 2019, afkomstig van de digit-officier zelf. Die notitie gaf volgens hem een adequate beschrijving van het werkproces. Op dat moment was het hierin beschreven werkproces (nog) niet vastgelegd in een (gepubliceerde) aanwijzing dan wel (interne) instructie van het College van procureurs-generaal.[432]

---

[429] Zie over de politieorganisatie: Besluit van 8 juni 2015, houdende regels over het beheer van de politie (Besluit beheer politie), *Stb.* 2015, 223, laatstelijk gewijzigd op 1 november 2017. In dit besluit heet DSO nog: dienst landelijke operationele samenwerking (DLOS). Het Besluit beheer politie is dus (nog) niet in overeenstemming met het organogram van de landelijke eenheid van de Nationale politie, toegankelijk op: https://www.politie.nl/informatie/organisatiestructuur-politie-nationaal.html.

[430] Voor de goede orde: Digit is niet hetzelfde als het team (of: de teams) high tech crime (THTC). Dit betreft een meer omvangrijk (eind 2020: ongeveer 120 fte) en gespecialiseerd rechercheonderdeel van de landelijke eenheid van de Nationale politie, dat met technisch complexe middelen tactisch opsporingsonderzoek verricht naar technisch complexe cybercrime.

[431] In de wetsgeschiedenis wordt naar (het bestaan van) deze functionaris tweemaal verwezen. Zie *Kamerstukken II* 2018/19, 34 372, nr. 29 (verslag van een schriftelijk overleg), p. 10: "*Vervolgens wordt geïnventariseerd welke mogelijke middelen effectief kunnen zijn met het technisch team in gezamenlijkheid met de speciale landelijk officier die is aangewezen voor de gecoördineerde inzet van de bevoegdheid.*" Zie ook *Handelingen I* 2017/18, nr. 34, item 5, p. 19: "*Dan vindt er een afweging plaats van de te bereiken doelen, de beschikbare technieken en middelen en de mogelijke alternatieve middelen en risico's. Daarbij wordt altijd de landelijk officier voor het binnendringen in een geautomatiseerd werk van het landelijk parket betrokken.*"

[432] In het door de PG-HR uitgebrachte tussenrapport van januari 2021 leidde deze constatering tot de aanbeveling om het werkproces vast te leggen in een instructie afkomstig van het College van procureurs-generaal. Aan die aanbeveling is gevolg gegeven met de in de hoofdtekst te bespreken instructie van 15 oktober 2021. Zie de brief van 29 september 2021 van de voorzitter van het College van procureurs-generaal aan de hoofden van de OM-onderdelen, PaG/B&S/18711, met als bijlage de instructie van 15 oktober 2021, p. 2 (van de brief).

In de notitie wordt de interne procedure aangaande de besluitvorming over de toepassing van de bevoegdheid als volgt beschreven:

"1. De cyber OvJ is alert op mogelijke kansen voor de inzet van de hackbevoegdheid door Digit, het landelijk technisch team (Digital Intrusion Team) bij de DLOS.[433] *Hierbij houdt hij/zij ook rekening met de evaluatie na 2 jaar.*
2. De zaaks OvJ legt de mogelijkheid tot de inzet van de hackbevoegdheid voor aan de cyber OvJ.
3. De cyber OvJ vervult de rol van poortwachter en kan de zaaks OvJ wijzen op eventuele andere (digitale) mogelijkheden om bewijs te vergaren.
4. Als de cyber OvJ kansen ziet voor de inzet van de hackbevoegdheid, informeert de cyber OvJ de recherche OvJ en het LP Digit.
5. Het LP Digit geeft zo snel mogelijk aan wat de mogelijkheden zijn om een zaak in behandeling te nemen.
6. Bij positief bericht bepaalt de recherche OvJ of de zaak wordt aangemeld voor intake.
7. Na aanmelding door de recherche OvJ start Digit het haalbaarheidsonderzoek. Het LP Digit informeert de zaaks OvJ, recherche OvJ en de cyber OvJ over de verdere procedure.
8. Indien een intake leidt tot een positief haalbaarheidsadvies vindt een overleg plaats tussen Digit, de Landelijk OvJ Digit, de tactisch teamleider en de zaaks OvJ. Indien wenselijk schuift de cyber OvJ aan.
9. De zaaks OvJ beslist – indien nog steeds noodzakelijk – tot inzet van de hackbevoegdheid. De recherche OvJ dient in te stemmen. De hoofd OvJ dient in te stemmen en legt de zaak via de CTC aan het College voor.
10. In overleg met de recherche OvJ moet een oplegnotitie (ondertekend door de zaaks OvJ), het aanvraag proces-verbaal en de aanbiedingsbrief van de hoofd OvJ aan (het secretariaat van) de CTC te worden ingestuurd.
11. Het LP Digit adviseert de zaaks OvJ over de inhoud van de aanvraag 126nba Sv.
12. Het LP Digit doet (het secretariaat van) de CTC het haalbaarheidsrapport en het plan van aanpak toekomen.
13. Na toestemming van het College vordert de zaaks OvJ een machtiging bij de RC. Het LP Digit adviseert de zaaks OvJ over de inhoud van de vordering 126nba Sv.
14. Indien de RC machtiging verleent voor de inzet, wordt de bevoegdheid ingezet onder verantwoordelijkheid van de zaaks OvJ.
15. Digit geeft uitvoering aan de bevoegdheid en onderhoudt hierover nauw contact met LP Digit. Het LP Digit adviseert Digit en beoordeelt mede of het noodzakelijk is een beslissing voor te leggen aan de zaaks OvJ. Het LP Digit en/of de cyber OvJ kan de zaaks OvJ adviseren bij te nemen beslissingen.
16. De resultaten van de uitvoering van het bevel worden – voor zover relevant in het licht van het bevel – door Digit verstrekt aan het tactisch team, al dan niet via tussenkomst van het TDO.[434] *"*

Binnen het OM is aan het werkproces aangaande de uitoefening van de bevoegdheid van artikel 126nba Sv bekendheid gegeven door middel van publicaties op het kennissysteem van het OM, ZoOM, met verwijzingen naar LP Digit.

[433] Voetnoot onderzoekers: 'DLOS' staat voor dienst landelijke operationele samenwerking, een onderdeel van de landelijke eenheid van de Nationale politie dat thans 'dienst specialistische operaties' (DSO) wordt genoemd.
[434] Voetnoot onderzoekers: 'TDO' staat voor: team digitale opsporing, onderdeel van de recherche binnen de regionale eenheden van de Nationale politie, waarin digitale specialisten werkzaam zijn. Bij tactische onderzoeken met een digitale component nemen doorgaans een of meer TDO'ers deel aan het tactische team.

De Instructie voor de inzet van de bevoegdheid ex artt. 126nba, 126uba, 126zpa en 126ffa Sv

Op 15 oktober 2021 is de 'Instructie voor de inzet van de bevoegdheid ex artt. 126nba, 126uba, 126zpa en 126ffa Sv', nr. 2021l002, afkomstig van het College van procureurs-generaal, in werking getreden.[435] De Instructie geeft regels voor de besluitvorming omtrent de toepassing van de bevoegdheid tot het uitvoeren van onderzoek in een geautomatiseerd werk. De Instructie geeft daarnaast regels voor de toepassing van artikel 126ffa Sv.
Het meest opvallende verschil tussen de Instructie en de hiervoor weergegeven notitie is dat de cyber-officier in het werkproces dat in de Instructie wordt voorgeschreven geen rol van betekenis meer toekomt. Desgevraagd heeft de digit-officier te kennen gegeven dat de beschrijving van het werkproces in de instructie overeenstemt met de praktijk zoals die zich in de loop der tijd heeft ontwikkeld. Zie hierover het volgende hoofdstuk.
Aan deze Instructie wordt het volgende ontleend:

> *"Op grond van het Bogw mag de bevoegdheid ex art. 126nba Sv enkel worden uitgevoerd door een technisch team dat onderdeel uit maakt van de Landelijke Eenheid van Politie. Dit technisch team is een team dat in opsporingsonderzoeken ondersteuning verleent aan de tactische rechercheteams.*
> *Het technisch team bepaalt onafhankelijk van het tactisch team op welke wijze uitvoering wordt gegeven aan een bevel ex art. 126nba Sv. Het tactisch team mag geen invloed uitoefenen op het binnendringen in het geautomatiseerd werk en de plaatsing, inzet en verwijdering van een technisch hulpmiddel. De methodieken die het technisch team gebruikt voor het binnendringen zijn afgeschermd en niet kenbaar voor het tactische team.*
> *De zaaksofficier van justitie heeft de leiding en de eindverantwoordelijkheid over het opsporingsonderzoek waarin de bevoegdheid ex art. 126nba Sv wordt ingezet. De landelijk officier van justitie voor Digital Intrusion heeft de leiding over en is verantwoordelijk voor de uitvoering van het bevel door het technisch team."*

Over de digit-officier bevat de Instructie de volgende bepalingen:

> *"Er is een landelijk officier van justitie voor Digital Intrusion aangesteld. De reden daarvoor is dat de toepassing van de bevoegdheid ex art. 126nba Sv specialistische (technische) kennis vergt. Daarbij is het van belang dat de methodieken van het binnendringen afgeschermd blijven. Verder is het van belang dat het tactische team en de zaaksofficier van justitie geen invloed kunnen uitoefenen op de wijze waarop het technische team het bevel ex art. 126nba Sv uitoefent. Tot slot is het wenselijk dat de prioriteiten bij de uitvoering van de bevoegdheid ex art. 126nba Sv centraal binnen het Openbaar Ministerie worden gesteld.*
> *De DIGIT officier van justitie oefent met inachtneming van het bepaalde bij of krachtens het Wetboek van Strafvordering, de Politiewet 2012 en het Bogw het gezag uit over het technisch team.*
> *De DIGIT officier van justitie bepaalt de kaders waarbinnen het technisch team uitvoering geeft aan de bevoegdheid tot het binnendringen van een geautomatiseerd werk en het verrichten van onderzoekshandelingen. Dit omvat ook de wijze van verbaliseren door het technisch team van de door hen verrichte handelingen.*
> *De DIGIT officier van justitie legt in voorkomende gevallen voorgenomen methodieken of handelingen voor aan de rechercheofficier van justitie van het landelijk parket.*
> *De DIGIT officier van justitie bepaalt in overleg met de teamleiding van het technisch team, aan de hand van de beleidsprioriteiten, de operationele prioriteiten bij de uitvoering van de bevoegdheid ex art. 126nba Sv."*

[435] De Instructie is bij de genoemde brief van de voorzitter van het College van procureurs-generaal van 29 september 2021 bekendgemaakt binnen het OM. Bovendien is deze Instructie openbaargemaakt op de website van het OM (www.OM.nl).

Omtrent de procedure voor de besluitvorming over de bevoegdheid van artikel 126nba Sv schrijft de Instructie voor:

"2.1. INTAKE EN VOORONDERZOEK
Een zaaksofficier van justitie die voornemens is gebruik te maken van de bevoegdheid ex art. 126nba Sv, legt dit voor aan de DIGIT officier van justitie.
De DIGIT officier van justitie maakt een eerste inschatting van de juridische haalbaarheid en inventariseert eventuele gevoeligheden. Hij vraagt het technisch team om een eerste inschatting te maken van de technische haalbaarheid en stemt de haalbaarheid en operationele aspecten van een mogelijke inzet af met de teamleiding van het technisch team.
De DIGIT officier van justitie bespreekt deze eerste beoordeling met de zaaksofficier van justitie. In onderling overleg wordt vervolgens bepaald of inzet van de bevoegdheid ex art. 126nba Sv gewenst is.

2.2. TOESTEMMING COLLEGE

Instemming hoofdofficier van justitie
De zaaksofficier van justitie legt zijn voornemen om de bevoegdheid ex art. 126nba Sv in te zetten vervolgens voor aan de rechercheofficier van justitie en de hoofdofficier van justitie van zijn parket. Als beiden instemmen, wordt de voorgenomen toepassing ter goedkeuring voorgelegd aan het College van procureurs-generaal (het College). Dit gebeurt door tussenkomst van en na advisering door de Centrale Toetsingscommissie (CTC).

Advisering door de CTC
De hoofdofficier van justitie doet een verzoek tot advisering aan de CTC. Daartoe stuurt hij een aanbiedingsbrief waaruit zijn instemming blijkt. Bij het verzoek worden een proces-verbaal van de politie tot aanvraag van de bevoegdheid ex art 126nba Sv en een notitie van de zaaksofficier van justitie met een toelichting van het verzoek en de zaak gevoegd. De zaaksofficier van justitie vraagt de DIGIT officier van justitie om advies over de inhoud van deze stukken.
Indien bij het uitvoeren van onderzoekshandelingen gebruik wordt gemaakt van een niet gekeurd technisch hulpmiddel (ex art. 21 lid 2 Bogw), wordt ook een plan van aanpak voor het treffen van aanvullende waarborgen (als bedoeld in art. 21 lid 4 Bogw) meegezonden.
De DIGIT officier van justitie stuurt de CTC een rapportage van het technisch team, waarin een indicatie is opgenomen van de uitvoerbaarheid en haalbaarheid van de voorgenomen inzet van de bevoegdheid. Daarin wordt een inschatting gegeven van risico's voor het binnen te dringen geautomatiseerd werk en (eventueel) (geautomatiseerde werken van) derden.
De CTC bespreekt deze stukken in een vergadering met de zaaksofficier van justitie. De CTC kan aan de DIGIT officier van justitie een nadere toelichting vragen op het binnendringen en op de voorgenomen wijze van uitvoering van het bevel.
De CTC beoordeelt vervolgens het verzoek aan de hand van (onder meer) de verdenking, proportionaliteit, subsidiariteit, de kans van slagen van de inzet van het middel en eventuele gevoeligheden/risico's en stelt een advies op voor het College.
De adviezen van de CTC en de stukken die aan de CTC ter hand zijn gesteld, zijn geen processtukken. Deze stukken worden niet bij het strafdossier gevoegd.

Besluitvorming door het College
Het College beslist, met inachtneming van het advies van de CTC, of de bevoegdheid ex art. 126nba Sv mag worden ingezet.
Het College stelt de CTC in kennis van zijn beslissing, met de eventueel daarbij gestelde voorwaarden. De CTC stelt vervolgens de hoofdofficier van justitie van het aanvragende parket en de DIGIT officier van justitie op de hoogte van die beslissing, met de eventueel daarbij gestelde voorwaarden. De CTC stuurt hen ook het schriftelijke advies toe.

Vervolgtoetsing
De zaaksofficier van justitie bewaakt de voortgang conform de besluitvorming door het College. De zaaksofficier van justitie informeert de DIGIT officier van justitie hierover.
Indien voortzetting van de inzet van de bevoegdheid na het verstrijken van de door het College gegeven termijn wenselijk is, legt de betrokken hoofdofficier van justitie de zaak opnieuw ter toetsing aan de CTC voor conform bovenstaande procedure.

Afloop
In alle gevallen waarin het College toestemming heeft verleend, informeert de betrokken hoofdofficier van justitie, (uiterlijk) na afloop van de zaak in eerste aanleg, de CTC over het resultaat van de toegepaste opsporingsmethode(n).

Spoedprocedure
In geval van dringende noodzakelijkheid kan de zaaksofficier van justitie zich direct wenden tot het secretariaat van de CTC. Daarvoor is toestemming van de hoofdofficier van justitie en instemming van de DIGIT officier van justitie nodig. De zaaksofficier van justitie motiveert het spoedeisende karakter van de voorgenomen inzet en de termijn waarbinnen een beslissing van het College gewenst is.
Indien de CTC van oordeel is dat sprake is van een dringende noodzakelijkheid, stuurt de zaaksofficier van justitie aan de CTC (minimaal) een beknopte notitie met een toelichting van het verzoek en de zaak.
De CTC beoordeelt het verzoek vervolgens op dezelfde wijze als bij een reguliere toetsing en geeft het College (mondeling) advies. Het College neemt hierop (mondeling) een beslissing en informeert de CTC daarover. De CTC koppelt deze beslissing per ommegaande terug aan de zaaksofficier van justitie.
Alle betrokkenen leggen na toepassing van de spoedprocedure alsnog hun verzoek, advies en beslissing schriftelijk vast.

2.3. HET BEVEL
Als het College toestemming heeft verleend, kan de zaaksofficier van justitie een vordering tot machtiging voor het geven van een bevel ex art. 126nba Sv aan de rechter-commissaris doen. Na machtiging door de rechter-commissaris beveelt de zaaksofficier van justitie de inzet. De zaaksofficier van justitie vraagt de DIGIT officier van justitie om advies over de inhoud van de vordering tot machtiging en het bevel."

De Instructie bevat bovendien voorschriften over de omgang met (inkomende en uitgaande) rechtshulpverzoeken die strekken tot het uitvoeren van onderzoek in een geautomatiseerd werk. Daarop wordt hieronder separaat teruggekomen.
Ten slotte wijst de Instructie de digit-officier aan als de centrale autoriteit binnen het OM die op de voet van artikel 126ffa Sv beslist over het uitstel van het bekendmaken van een onbekende kwetsbaarheid voor het binnendringen in een geautomatiseerd werk. "*De DIGIT officier van justitie informeert de zaaksofficier van justitie over een dergelijk bevel, indien dit relevant is voor enige door de zittingsrechter in de strafzaak te nemen beslissing*", aldus de Instructie.

Analyse en beoordeling van de beleidskaders voor de werkprocessen inzake de uitoefening van de bevoegdheid
De in het voorgaande besproken kaders geven aanleiding tot de volgende opmerkingen.

Bij lezing van beide hiervoor beschreven, successieve beleidskaders van het OM springt in het oog dat het OM binnen zijn organisatie een officier van justitie die is verbonden aan het landelijk parket heeft aangesteld als (landelijk) digit-officier. Met inachtneming van de hiërarchische lijnen binnen het OM is de digit-officier exclusief verantwoordelijk voor de uitvoering door Digit van onderzoek in een geautomatiseerd werk. Uitsluitend aan de digit-officier worden de kennis en besluitvorming toevertrouwd aangaande de daarbij door Digit

toegepaste methodieken. Deze strikte scheiding tussen de werkzaamheden van de digit-officier en de zaaksofficier correspondeert met de in het Bogw voorgeschreven scheiding tussen enerzijds het technische team, dat onder leiding van de digit-officier opereert, en anderzijds het tactische team, dat onder het gezag van de zaaksofficier opsporingsonderzoek uitvoert in de strafzaak waarin de bevoegdheid wordt uitgeoefend.
Anders dan de instelling van een zelfstandig technisch team (Digit) bij de landelijke eenheid van de Nationale politie, is de aanstelling binnen de OM-organisatie van een zogeheten digit-officier niet voorzien bij wet of regelgeving. Noch de wet, noch het Bogw maakt melding van een landelijke officier van justitie voor *digital intrusion*. Alle beslissingen die samenhangen met de inzet van de bevoegdheid worden – volgens de bewoordingen van het Bogw – zonder enige differentiatie genomen door *de* officier van justitie. In de nota van toelichting op het Bogw wordt bijvoorbeeld aan de zaaksofficier met zoveel woorden een 'schakelfunctie' toegekend tussen het technisch team en het tactisch team, zonder dat daarbij melding wordt gemaakt van het bestaan van een landelijk officier voor *digital intrusion*. In de toelichting wordt in dit verband slechts opgemerkt: "*De organisatorische scheiding tussen het technische team en het tactische team behoeft de samenwerking tussen de teams gedurende het opsporingsonderzoek niet te belemmeren. De officier van justitie onder wiens leiding het opsporingsonderzoek plaatsvindt vervult hierbij een schakelfunctie*."
Daarmee is niet gezegd dat de aanstelling binnen de OM-geledingen van een digit-officier onder wiens exclusieve gezag het technische team uitvoering geeft aan een bevel van de zaaksofficier op de voet van artikel 126nba Sv, 'uit de lucht komt vallen' en (om die reden) onverenigbaar zou zijn met het materieel-wettelijke kader dat in hoofdstuk 3 is beschreven.
In de wetsgeschiedenis wordt naar (het bestaan van) de digit-officier tweemaal verwezen. Dat betreft allereerst een opmerking van de minister bij de beraadslagingen van 19 juni 2018 in de Eerste Kamer: "*Dan vindt er een afweging plaats van de te bereiken doelen, de beschikbare technieken en middelen en de mogelijke alternatieve middelen en risico's. Daarbij wordt altijd de landelijk officier voor het binnendringen in een geautomatiseerd werk van het landelijk parket betrokken*."[436] Een vergelijkbare opmerking is opgetekend in een brief d.d. 4 december 2018 van de minister: "*Vervolgens wordt geïnventariseerd welke mogelijke middelen effectief kunnen zijn met het technisch team in gezamenlijkheid met de speciale landelijk officier die is aangewezen voor de gecoördineerde inzet van de bevoegdheid*."[437]

Het komt er dus op neer dat het OM met de aanstelling van een landelijk digit-officier en de toekenning van de bij die functie passende taken en verantwoordelijkheden de door het Bogw voorgeschreven organisatorische scheiding tussen enerzijds het werkproces van het technische team (het uitvoeren van onderzoek in een geautomatiseerd werk) en anderzijds het werkproces van het tactische team (het opsporingsonderzoek) consequent heeft geïmplementeerd binnen de eigen organisatie, en dit met medeweten van de minister. Weliswaar was deze inrichting van het werkproces binnen het OM niet voorgeschreven bij wet of regeling, onverenigbaar hiermee is zij evenmin. De beweegredenen voor deze scheiding van werkprocessen heeft het OM uiteengezet in een hierboven aangehaalde passage uit de Instructie. Die beweegredenen komen plausibel en verdedigbaar voor.

Zoals gezegd is in de nota van toelichting op het Bogw opgemerkt dat de organisatorische scheiding tussen het technische team en het tactische team de samenwerking tussen de teams niet hoeft te belemmeren omdat de officier van justitie onder wiens leiding het opsporingsonderzoek plaatsvindt, de zaaksofficier, hierbij een 'schakelfunctie' vervult. Vanwege de organisatorische scheiding tussen de digit-officier en de zaaksofficier, komt de vraag op welke van deze officieren invulling geeft of geven aan deze schakelfunctie en op

[436] *Handelingen I* 2017/18, nr. 34, item 5, p. 19.
[437] Neergelegd in het verslag van een schriftelijk overleg tussen de vaste commissie voor Justitie en Veiligheid en de minister met als onderwerp het Bogw, *Kamerstukken II* 2018/19, 34 372, nr. 29, p. 10.

welke wijze. Dat betreft de uitvoeringspraktijk, in tegenstelling tot het beleid, waarover dit hoofdstuk gaat. Op deze vraag wordt in het volgende hoofdstuk teruggekomen.
Zowel in de notitie van de digit-officier als in de Instructie zijn de taken van de CTC en het College van procureurs-generaal vermeld. De adviesaanvraag bij de CTC en de beslissing van het College van procureurs-generaal vormen (onmisbare) schakels in de besluitvorming over de toepassing van de bevoegdheid van onderzoek in een geautomatiseerd werk. Dit is in overeenstemming met de procedurele eisen die zijn weergegeven in paragraaf 3.3 hierboven.
In de 'BOB-matrixen', die – naar de mededeling van de liaison bij het Parket-Generaal – ter informatie binnen het OM zijn verspreid, wordt dienovereenkomstig melding gemaakt van de taken van de CTC en het College van procureurs-generaal in dit verband.[438]

Het bestaan van de CTC en haar werkzaamheden zijn gegrond op de Aanwijzing opsporingsbevoegdheden, nr. 2014A009, *Stcrt.* 2014, 24442, afkomstig van het College van procureurs-generaal. Deze aanwijzing voorziet echter niet in een rol van de CTC in het hiervoor beschreven werkproces voor de uitoefening van de bevoegdheid ex artikel 126nba Sv. De Aanwijzing opsporingsbevoegdheden is daarmee al drie jaar niet in overeenstemming met de mededelingen van de minister bij de parlementaire behandeling van de Wet computercriminaliteit III en de nota van toelichting op het Bogw. Bovendien strookt deze aanwijzing evenmin met de uitvoeringspraktijk. Deze discrepantie tussen enerzijds de thans geldende Aanwijzing opsporingsbevoegdheden en anderzijds de Instructie roept bovendien de vraag op wat de rangorde is van deze instrumenten en aan welk instrument (dus) voorrang toekomt.

In de tussenrapportage van de PG-HR van januari 2021 is reeds geconstateerd dat de Aanwijzing opsporingsbevoegdheden (nog) niet was aangepast, zoals wel de bedoeling van de minister was.[439] Uit de brief van 29 september 2021 van de voorzitter van het College van procureurs-generaal aan de hoofden van de OM-onderdelen, PaG/B&S/18711, valt op te maken dat deze aanwijzing om "*capaciteitsredenen*" nog niet is geactualiseerd.

4.2. Internationale aspecten van de inzet van de bevoegdheid ex artikel 126nba Sv

De Aanwijzing internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv
In paragraaf 3.12 is reeds gewezen op de Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv, *Stcrt.* 2019, 10277, afkomstig van het College van procureurs-generaal (hierna in deze paragraaf ook: de Aanwijzing).[440] In de inleiding en in paragraaf 1.1 van die Aanwijzing wordt uiteengezet dat het internet niet gebonden is aan landsgrenzen. Dit brengt mee dat bij de uitvoering van de bevoegdheid van artikel 126nba Sv gegevens en geautomatiseerde werken kunnen worden benaderd die zich in het buitenland

[438] Naar de mededeling van het Parket-Generaal is de BOB-matrix een belangrijk intern hulpmiddel dat periodiek geactualiseerd wordt. Die matrixen geven op een laagdrempelige manier inzicht in de geldende interne procedureafspraken die in diverse stukken zijn vastgelegd. Naast de wettelijke vereisten voor de inzet van (bijzondere) opsporingsbevoegdheden, geldt vaak ook een interne instemmings-/goedkeuringsprocedure. Deze afspraken zijn vastgesteld in de landelijke vergadering van rechercheofficieren en opgenomen in deze matrixen voor de inzet van (bijzondere) opsporingsmiddelen.

[439] Vgl. *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 38: "*Het College zal worden verzocht om de voorgestelde bevoegdheid, zodra deze kracht van wet heeft gekregen, op te nemen in de lijst van bevoegdheden waarvoor geldt dat deze aan de CTC voorgelegd moeten worden. De Aanwijzing opsporingsbevoegdheden zal worden aangepast zodat ook de voorgenomen inzet van het onderzoek in een geautomatiseerd werk aan de CTC zal moeten worden voorgelegd.*"

[440] Blijkens een voetnoot in de Aanwijzing is de Aanwijzing mutatis mutandis van toepassing op de uitvoering van een bevel ex art. 126uba en art. 126zpa Sv. Deze aanwijzing is toegankelijk op: https://zoek.officielebekendmakingen.nl/stcrt-2019-10277.html.

bevinden. De Aanwijzing geeft regels voor het handelen in deze internationale context. De Aanwijzing bestrijkt daarmee alleen gevallen waarin het uitvoeren van onderzoek in een geautomatiseerd werk plaatsvindt door (of op verzoek van) de Nederlandse politie en justitie ten behoeve van een Nederlandse stafzaak. Daarvoor wordt dus zo nodig en indien mogelijk een *uitgaand* rechtshulpverzoek gedaan.

De toetsingscriteria van de Aanwijzing

Net als de memorie van toelichting bij de Wet computercriminaliteit III[441] neemt de Aanwijzing tot uitgangspunt dat voor de inzet van de bevoegdheid op het grondgebied van een andere staat bij de bevoegde autoriteiten van die staat een verzoek tot het verlenen van internationale rechtshulp wordt ingediend (paragraaf 1.3 van de Aanwijzing).[442, 443]

Er zijn in de Aanwijzing echter nadere regels gesteld voor gevallen waarin volgens de minister kan worden afgeweken van het uitgangspunt dat voor de inzet van de bevoegdheid op het grondgebied van een andere staat bij de bevoegde autoriteiten van die staat een verzoek tot het verlenen van internationale rechtshulp wordt ingediend. Dit betreft:

1. het geval waarin niet bekend is waar de gegevens zich bevinden (paragraaf 1.4 en 2.2 onder c van de Aanwijzing) en
2. het geval waarbij – ondanks dat bekend is waar de gegevens zich bevinden – toch geen rechtshulpverzoek hoeft te worden gedaan en/of de toestemming van een andere staat niet hoeft te worden afgewacht (paragraaf 2.2 onder a en b van de Aanwijzing).

Zowel het eerste als het tweede geval werd reeds in de wetsgeschiedenis als uitzondering erkend.[444]

Het in de Aanwijzing gebruikte begrip 'waar de gegevens zich bevinden' mist naar het oordeel van de onderzoekers de nodige precisie. Elektronische gegevens c.q. computergegevens (dat wil zeggen de in artikel 80quinquies Sr bedoelde bits en bytes) zijn immaterieel van aard en hebben dus als zodanig geen locatie. Voor de locatie van elektronische gegevens moet dan ook worden aangeknoopt bij de locatie van het geautomatiseerde werk of van de gegevensdrager waarop de elektronische gegevens zijn opgeslagen.

Uitzondering 1: de locatie van de gegevens is (aanvankelijk) niet bekend

De eerste uitzondering betreft het geval waarin wél bekend is dat een geautomatiseerd werk in gebruik is bij een verdachte of een persoon, maar niet bekend is wat de (geografische) locatie is van de gegevens. Daardoor kan niet worden bepaald welke staat betrokken is bij de opslag of verwerking van de gegevens.[445] In deze situatie is er volgens de Aanwijzing onvoldoende informatie om een rechtshulpverzoek te doen en kan bovendien (zelfs) niet

---

441 Zie o.a. *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 3, 25, 44, 46 en 47.

442 Paragraaf 1.2 van de aanwijzing vermeldt in dat verband onder andere: "*De aangezochte staat wordt verzocht aan dit rechtshulpverzoek uitvoering te geven en vervolgens de gevraagde informatie of gegevens te vorderen, te verkrijgen en te leveren. De aangezochte staat is ook zelf bevoegd om op te treden tegen inbreuken op de rechtsorde die op of vanuit het eigen grondgebied worden beraamd of gepleegd. Een verzoek om rechtshulp kan, afhankelijk van de rechtshulprelatie met het desbetreffende land, mondeling of schriftelijk worden gedaan. Als er meerdere staten rechtsmacht kunnen claimen ligt onderling overleg voor de hand. Zie ook nader in detail paragraaf 1.3.*"

443 Ingevolge art. 35 Cybercrimeverdrag hebben verscheidene landen hebben ten behoeve van de snelle afhandeling van verzoeken om internationale rechtshulp in cybercrimezaken een 24/7-contactpunt ingericht. Met het oog op een spoedige en effectieve samenwerking met derde landen is in Nederland het 24/7-contactpunt voor dringende (aan Nederland gerichte) verzoeken om internationale rechtshulp in cybercrimezaken ondergebracht bij het team high tech crime (THTC) van de landelijke eenheid van de Nationale politie, dat korte lijnen heeft met de afdeling voor *hightech crime* van het landelijk parket van het OM. Zie *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 47.

444 *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 49-50; *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 15-16, 94-96 en 98; vgl. ook p. 31 van de nota van toelichting op het Bogw.

445 Vgl. de nota van toelichting op het Bogw, p. 31.

worden uitgesloten dat de gegevens zich in Nederland bevinden.[446] In een dergelijke situatie wordt eerst onderzocht of met een redelijke mate van inspanning de locatie van de gegevens alsnog kan worden vastgesteld. Als dat niet het geval is wordt gehandeld alsof de gegevens in Nederland zijn opgeslagen en worden de Nederlandse rechtsregels toegepast (paragraaf 1.4 en 2.2 onder c van de Aanwijzing).[447]
De begrenzing van de redelijkheid van de te verrichten inspanning is sterk afhankelijk van het concrete geval. In gevallen waarbij onverwijld optreden noodzakelijk is (bijvoorbeeld bij grootschalige aanvallen op de Nederlandse infrastructuur of bij levensbedreigende situaties) en mede gelet op de concrete omstandigheden (bijvoorbeeld het gebruik van anonimiseringssoftware of opslag in de cloud) kan zich de situatie voordoen dat er redelijkerwijs geen mogelijkheid is om de exacte locatie van de gegevens vast te stellen, aldus de Aanwijzing. Bij een *redelijke* inspanning staan de tijd en moeite voor het vaststellen van een specifieke geografische locatie in een reële verhouding tot de noodzakelijkheid van onverwijld optreden,[448] de tijdsdruk en de doorlooptijd van het onderzoek.[449]
Nadat een geautomatiseerd werk is binnengedrongen ontstaan meer mogelijkheden voor het bepalen van de locatie ervan en van de gegevens die dienen te worden benaderd. Voorbeelden die de minister noemt zijn: het deconstrueren van de gebruikte verhullingstechniek vanaf het geautomatiseerde werk, het verkrijgen van inzicht in het internetgebruik vanuit of via het geautomatiseerde werk, of het ontplooien van activiteiten die erop zijn gericht om het geautomatiseerde werk zichzelf te laten identificeren of lokaliseren. Deze mogelijkheden hangen af van de aard van het geautomatiseerde werk en het risico van ontdekking door de gebruiker.[450]
Wanneer de locatie van de gegevens tijdens de onderzoekshandelingen alsnog bekend wordt, geldt volgens paragraaf 1.5 van de Aanwijzing het volgende. Wanneer de gegevens zich op het territorium van een andere staat bevinden, wordt hetzij zo snel mogelijk alsnog aan die staat verzocht om toestemming tot het verrichten van onderzoekshandelingen en het gebruik van deze gegevens, hetzij wordt besloten de onderzoekshandelingen te beëindigen.[451] Indien wordt besloten tot het doen van een rechtshulpverzoek kan de officier van justitie volgens paragraaf 2.2 onder b van de Aanwijzing daarbij kiezen om de inzet te staken in afwachting van een reactie op het rechtshulpverzoek.

---

[446] De memorie van toelichting bij het wetsvoorstel onderzoek in een geautomatiseerd werk (*Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT)) vermeldt daarover onder meer het volgende (p. 47): "*Dit komt voor wanneer vrijwel alle gegevens op de Cloud worden opgeslagen of bewaard. Dit kan ook verband houden met het op anonimiteit – en daarmee op het niet kunnen achterhalen van een geografische plaats – gerichte internetgedrag van bepaalde personen, zoals bij gegevens die via het Tor-netwerk worden gerouteerd of die door middel van NAT (network address translation; het veranderen van IP-adressen in de IP-header) worden verzonden (waarbij een groot aantal computers gebruik maakt van eenzelfde IP-adres). In deze gevallen is een gegeven niet altijd terug te voeren op een IP-adres en bestaat er niet altijd wetenschap van de locatie van de gegevens, en ook niet van de staat die betrokken is bij de opslag of verwerking van de gegevens. Dit kan betekenen dat op afstand heimelijk wordt binnengedrongen in een geautomatiseerd werk waarvan niet bekend is waar zich dit bevindt, bijvoorbeeld een server, met het oog op het verrichten van bepaalde onderzoekshandelingen.*"

[447] Eenzelfde soort benadering heeft de minister eerder ook met betrekking tot de netwerkdoorzoeking gehanteerd, zie *Kamerstukken II* 2004/05, 26671, nr. 10, p. 23: "*In beginsel dient men in een rechtshulpverzoek aan het desbetreffende land om de gegevens te vragen. Men kan echter niet altijd van te voren weten of een netwerkzoeking leidt tot een zoeking in een computer in het buitenland. In dat geval zijn de gegevens te gebruiken voor het onderzoek. Als men dit echter wel weet, ontdekt of zou behoren te weten, is internationale rechtshulp noodzakelijk.*"

[448] In de Aanwijzing wordt daarbij in een voetnoot opgemerkt: "*In de Memorie van Toelichting bij de wet Computercriminaliteit III wordt het concrete voorbeeld gegeven van een DDoS-aanval op een overheidsdienst of een financiële instelling in Nederland waardoor de online dienstverlening gedurende langere tijd wordt onderbroken (Kamerstukken II 2015/16, 34 327, 3, p. 47.)*"

[449] In de Aanwijzing wordt daarbij in een voetnoot opgemerkt: "*Bij concrete inspanningen kan bijvoorbeeld worden gedacht aan het raadplegen van de WHOIS informatie van ICANN, het zo mogelijk vorderen van gegevens bij Nederlandse internetdienstaanbieders waar de verdachte mogelijk gebruik van maakt of het analyseren van in het onderzoek beschikbaar internetverkeer (netflow en/of traceroutes).*"

[450] *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 33.

[451] Vgl. *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 47, waarin in dat geval het rechtshulpverzoek als uitgangspunt wordt genomen.

Volgens de memorie van toelichting bij het wetsvoorstel en de nota van toelichting op het Besluit dient in dit soort gevallen het optreden zeer zorgvuldig te worden ingekaderd en hanteert de officier van justitie zoveel mogelijk een stapsgewijze aanpak.[452] In beginsel zal worden aangevangen met een beperkt eerste bevel met als onderzoeksdoel het vaststellen van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker ervan. Als verdergaande onderzoekshandelingen nodig zijn zal waar mogelijk worden volstaan met het overnemen van de opgeslagen gegevens, zodat de beschikkingsmacht van de rechthebbende niet wordt beperkt. Als bekend is, of in de loop van het onderzoek bekend wordt, dat de gegevens zich in een andere dan de Nederlandse rechtsmacht bevinden, dan ligt een verzoek om internationale rechtshulp voor de hand. Daarbij kan aan de bevoegde buitenlandse autoriteiten verantwoording worden afgelegd over de handelingen die (reeds) zijn verricht en de afwegingen die daarbij zijn gemaakt.

Uitzondering 2: locatie gegevens bekend, maar geen (voorafgaande) toestemming nodig

Volgens paragraaf 2.2 onder a en b van de Aanwijzing zijn er twee gevallen waarin zonder een instemmende reactie op een rechtshulpverzoek kan worden opgetreden. Dat betreft in eerste instantie het geval onder a, waarin de locatie van de gegevens bekend is, de officier van justitie conform het uitgangspunt een rechtshulpverzoek heeft gedaan, maar niet (langer) kan worden gewacht op een reactie van de aangezochte staat dan wel geen reactie van de aangezochte staat valt te verwachten.
Het tweede geval, onder b, betreft het geval waarin de locatie van de gegevens tijdens de onderzoekshandelingen alsnog bekend wordt, maar – anders dan in de hiervoor genoemde uitzondering – het onderzoek *niet* wordt gestaakt in afwachting van de reactie op het rechtshulpverzoek. De officier van justitie kan namelijk volgens de Aanwijzing onder omstandigheden bepalen dat de inzet van de bevoegdheid (alvast) wordt voltooid in afwachting van een reactie op het rechtshulpverzoek.
Volgens paragraaf 2.4 van de Aanwijzing gelden voor deze uitzondering de volgende afwegingscriteria:

- de ernst of onmiddellijkheid van de gevolgen van de aanval of dreiging,
- de aard en ernst van het strafbare feit,
- de vluchtigheid van de gegevens die worden gezocht, en de vraag of die moeten worden veiliggesteld, dan wel ontoegankelijk moeten worden gemaakt,
- de mate van betrokkenheid van de Nederlandse rechtsorde en de gevolgen daarvoor (inclusief slachtofferbelangen),
- de aard van de te verrichten opsporingshandelingen, afhankelijk van:
  - de mate van ingrijpendheid,
  - de mate van inbreuk op de privacy van de verdachte,
  - de mate van inbreuk op privacy van slachtoffers die door middel van het geautomatiseerde werk wordt gemaakt,
- de risico's voor het geautomatiseerde werk:
  - de technische risico's,
  - de inschatting van de mogelijke schade voor derden.

Tot slot dient volgens paragraaf 2.3 van de Aanwijzing de zaaksofficier de context van de aanvaarde soevereiniteitsschending te bespreken met de digit-officier. De zaaksofficier legt vervolgens een met redenen omkleed besluit ter instemming voor aan de rechercheofficier van het parket waaraan hij verbonden is.

[452] *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 48, en de nota van toelichting op het Bogw, p. 31.

Nogmaals de Instructie voor de inzet van de bevoegdheid ex artt. 126nba, 126uba, 126zpa en 126ffa Sv

In aanvulling op de geldende beleidsregels met betrekking tot internationale samenwerking en internationale rechtshulp schrijft de Instructie voor dat de zaaksofficier voor het geven van een bevel ex artikel 126nba Sv in het kader van inkomende of uitgaande rechtshulp toestemming nodig heeft van het College van procureurs-generaal, zulks voordat hij van de rechter-commissaris een machtiging vordert. Het College beslist hierop volgens de in de Instructie voorgeschreven (en hierboven weergegeven) procedure.
De ontvanger van een inkomend rechtshulpverzoek, dat naar Nederlands recht toepassing van de bevoegdheid ex artikel 126nba Sv inhoudt, meldt dit bij de digit-officier. Deze beoordeelt (mede) de wijze van uitvoering van het rechtshulpverzoek. Ook de zaaksofficier die een uitgaand rechtshulpverzoek wil doen dat naar Nederlands recht toepassing van de bevoegdheid ex artikel 126nba Sv inhoudt, meldt dit bij de digit-officier. De digit-officier beoordeelt (mede) het verzoek om inzet van deze bevoegdheid aan/in het andere land.

Analyse en beoordeling van de beleidskaders voor internationale aspecten van de uitoefening van de bevoegdheid

De in het voorgaande besproken kaders geven aanleiding tot de volgende opmerkingen.

De Aanwijzing is gestoeld op het uitgangspunt dat voor de inzet van de bevoegdheid van artikel 126nba Sv op het grondgebied van een andere staat bij de bevoegde autoriteiten van die staat een verzoek tot het verlenen van internationale rechtshulp wordt ingediend. Dit uitgangspunt strookt met het internationale recht en met het materieel-wettelijke kader dat hierboven in paragraaf 3.12 is weergegeven. De wijze van regulering van de in de Aanwijzing omschreven uitzonderingen vinden steun in de wetsgeschiedenis van de Wet computercriminaliteit III. Met name met betrekking tot uitzondering 2, het geval waarbij – ondanks dat bekend is waar de gegevens zich bevinden – toch geen rechtshulpverzoek hoeft te worden gedaan en/of de toestemming van een andere staat niet hoeft te worden afgewacht, komt evenwel de vraag op hoe de inhoud van de Aanwijzing zich verhoudt tot het internationale recht.
Doordat computercriminaliteit en gedigitaliseerde criminaliteit niet aan landsgrenzen is gebonden, valt niet uit te sluiten dat justitiële autoriteiten handhavend optreden buiten de grenzen van het territorium van de staat. Op het terrein van de uitoefening van rechtsmacht is het internationale recht in beweging. Vanwege uiteenlopende opvattingen die in internationaal verband om voorrang strijden valt niet te verwachten dat het juridisch debat binnen afzienbare termijn wordt beslecht. Zoals gezegd staat het territorialiteitsbeginsel in cyberspace onder druk. Naar het oordeel van de minister moet in afwachting van de verdere ontwikkeling van het internationaalrechtelijke kader voor de uitoefening van rechtsmacht bij de bestrijding van computercriminaliteit zelfstandig kunnen worden opgetreden om te voorkomen dat het internet een vrijplaats wordt voor criminaliteit.[453] Dit kan met zich brengen dat opsporingshandelingen (moeten) worden verricht met betrekking tot gegevens die niet in Nederland zijn opgeslagen, aldus de minister.
Thans kan worden geconstateerd dat de Aanwijzing correspondeert met dit door de minister verwoorde uitgangspunt, zonder dat op voorhand moet worden geoordeeld dat de inhoud van de Aanwijzing zich naar de huidige stand van zaken niet verdraagt met het internationale recht.
Voor verdergaande toetsing bestaat thans geen aanleiding. Wel is bij het toezichtonderzoek beoordeeld of bij de uitvoering van het bevel ex artikel 126nba Sv is gehandeld in overeenstemming met – onder meer – de Aanwijzing. Daarop wordt in het volgende hoofdstuk ingegaan.

[453] *Kamerstukken II* 2015/16, 34 372, nr. 3 (MvT), p. 50. Vgl. ook *Kamerstukken II* 2016/17, 34 372, nr. 6 (NV II), p. 15-16, waarin wordt gesproken over inspanningen in EU-context om tot oplossingen te komen, alsook meer uitgebreid *Kamerstukken I* 2016/17, 34 372, D (MvA I), p. 38-40.

4.3. Geheimhoudersgegevens en het verschoningsrecht

Het OM-beleid inzake de geheimhoudersproblematiek

In paragraaf 3.13 is onder het kopje 'Gegevens waaromtrent het verschoningsrecht kan worden uitgeoefend' stilgestaan bij de regeling van artikel 126aa Sv en het Besluit bewaren en vernietigen niet-gevoegde stukken. Deze regeling verplicht onverkort tot het vernietigen van gegevens die binnen het bereik van een functioneel verschoningsrecht vallen.[454]
Hierboven is ook gewezen op de ongerijmdheid van die regeling met voorschriften in het Bogw, in het bijzonder artikel 7 lid 1 en artikel 28 lid 1 Bogw. Uit deze bepalingen van het Bogw vloeit namelijk voort dat geen wijzigingen mogen worden aangebracht in de bewijslogging, respectievelijk in de gegevens die op een technische infrastructuur zijn vastgelegd. In deze bepalingen wordt geen acht geslagen op de vraag of deze gegevens binnen het bereik van een verschoningsrecht vallen.

Volgens een door het OM op 18 december 2020 vastgestelde interne notitie[455] heeft de digit-officier beslist dat – vanwege de specifieke toepasselijkheid van het Bogw op de uitoefening van de bevoegdheid van de artikelen 126nba, 126uba en 126zpa Sv – de bepalingen van het Bogw voorrang hebben op de bepalingen in het Besluit bewaren en vernietigen niet-gevoegde stukken.
In de semigestructureerde interviews met de digit-officier en de digit-parketsecretaris is meermalen aandacht besteed aan de problematiek van geheimhouders. De nadere regeling waaraan LP Digit en Digit volgens de notitie uitvoering geven houdt kort gezegd in dat Digit in overeenstemming met de genoemde bepalingen van het Bogw géén wijzigingen aanbrengt in de bewijslogging, noch in de bij het onderzoek geregistreerde gegevens die op de technische infrastructuur zijn vastgelegd. Digit neemt in de regel geen kennis van de inhoud van de gegevens die bij het onderzoek in een geautomatiseerd werk worden geregistreerd, en Digit controleert in principe niet of het gegevens betreft waaromtrent een verschoningsrecht kan worden uitgeoefend. Tactisch opsporingsambtenaren hebben geen toegang tot de bewijslogging en de gegevens die op de technische infrastructuur zijn vastgelegd; zij kunnen dus niet kennisnemen van die gegevens en daarin evenmin wijzigingen aanbrengen.
Na afronding van het onderzoek in een geautomatiseerd werk worden de geregistreerde gegevens in overeenstemming met artikel 29 Bogw (zie paragraaf 3.9 hierboven) door

[454] In voetnoot 404 in paragraaf 3.13 is ter relativering van het begrip 'vernietigen (van digitale gegevens)' gewezen op art. 5 lid 1 en lid 2 van het Besluit bewaren en vernietigen niet-gevoegde stukken. Daarin is bepaald dat met de vernietiging van een proces-verbaal c.q. ander voorwerp gelijkstaat het op zodanige wijze bewerken van de gegevensdrager waarop dat proces-verbaal is opgeslagen c.q. het op zodanige wijze bewerken van het bedoelde voorwerp dat de gegevens die daaraan vóór die bewerking konden worden ontleend, "*niet meer kenbaar zijn.*"
[455] Voluit: 20201218 Vernietiging van geheimhoudersgegevens bij de inzet van 126nba Sv.

tussenkomst van het TDO[456] en een 'medewerker geheimhouders'[457] overgedragen aan het tactisch team. Het is dan aan de zaaksofficier en het tactisch team om te handelen overeenkomstig de regeling van artikel 126aa Sv, het Besluit bewaren en vernietigen niet-gevoegde stukken, en de op 1 november 2014 in het leven geroepen Instructie vernietiging van geïntercepteerde gesprekken met geheimhouders (2014l001) van het College van procureurs-generaal. De zaaksofficier en het tactisch team worden over deze werkwijze en de daarin besloten liggende toedeling van verantwoordelijkheid door LP Digit vooraf geïnstrueerd. Voordat het tactisch team kennisneemt van de bij uitvoering van het bevel ex artikel 126nba Sv vastgelegde gegevens onderzoekt de medewerker geheimhouders of zich onder de door Digit overgedragen dataset geheimhoudersgegevens bevinden. Zo ja, dan stelt hij de zaaksofficier hiervan op de hoogte. Vervolgens is het aan de zaaksofficier om hierover te beslissen en zo nodig de vernietiging van die gegevens te gelasten. Indien daarvoor vereist is dat de geheimhoudersgegevens worden uitgewerkt en ingezien, wordt de inzage en besluitvorming overgelaten aan een andere officier dan de zaaksofficier; dat kan de rechercheofficier betreffen. Mededelingen die zijn gedaan door of aan een geheimhouder zullen niet dan met machtiging van de rechter-commissaris worden gevoegd bij de processtukken. Niet eerder dan nadat de voorgaande beleidsregels in acht zijn genomen, zal het tactische team kennisnemen van de inhoud van (het restant van) de door Digit overgedragen dataset.

In die gevallen waarin Digit tijdens de uitvoering van het bevel ex artikel 126nba Sv niettemin bekend raakt met de mogelijkheid dat gegevens worden geregistreerd of ingezien waarover het verschoningsrecht zich uitstrekt, wordt de kennisneming van de gegevens door Digit onmiddellijk beëindigd en wordt de digit-officier hiervan terstond op de hoogte gesteld. Registratie kan niet in alle gevallen worden voorkomen, kennisneming wel. Op dat laatste ziet de instructie van de digit-officier.

In die gevallen waarin Digit na afloop van de uitvoering van het bevel ex artikel 126nba Sv bekend wordt met de mogelijkheid dat gegevens zijn geregistreerd waarover het verschoningsrecht zich uitstrekt, wordt de digit-officier hiervan terstond op de hoogte gesteld. Indien de digit-officier oordeelt dat het hier (inderdaad) gegevens betreft waaromtrent het verschoningsrecht kan worden uitgeoefend, stelt hij de zaaksofficier daarvan op de hoogte.

---

[456] Mededeling LP Digit: 'TDO' staat voor: team digitale opsporing, onderdeel van de recherche binnen de regionale eenheden van de Nationale politie, waarin digitale specialisten werkzaam zijn. Bij tactische onderzoeken met een digitale component zijn doorgaans een of meer medewerkers TDO betrokken. De medewerker TDO is degene die op de voet van art. 29 Bogw van Digit de dataset ontvangt met de gegevens die bij de uitvoering van het onderzoek in een geautomatiseerd werk zijn vastgelegd. De medewerker TDO controleert de integriteit van de gegevens door daarover een hashwaarde te berekenen. Daarna maakt de medewerker TDO het bestand leesbaar voor de medewerker geheimhouders. Zie daarover de volgende voetnoot.

[457] Over de procedure met tussenkomst van een 'medewerker geheimhouders' het volgende. Voor de omgang met mogelijke geheimhoudersstukken die zijn verkregen door de toepassing van bijzondere opsporingsbevoegdheden, heeft het OM een werkwijze ontwikkeld die is vastgelegd in de Handleiding verwerking geheimhouderinformatie aangetroffen in inbeslaggenomen voorwerpen en in digitale bestanden, van de landelijke vergadering van rechercheofficieren. Deze regeling stamt uit 2014 en heeft niet specifiek betrekking op de bevoegdheid van art. 126nba/uba/zpa Sv. Samengevat komt deze regeling erop neer dat opsporingsambtenaren die in hun onderzoek worden geconfronteerd met gegevens waarover het verschoningsrecht zich vermoedelijk uitstrekt deze gegevens eerst aan een 'medewerker geheimhouders' voorleggen. Deze medewerker geheimhouders betreft geen afzonderlijke functie binnen de opsporing maar een rol die wordt uitgeoefend door een opsporingsambtenaar die niet bij het opsporingsonderzoek in de concrete zaak betrokken is. Deze functionaris maakt een eerste inschatting of de gegevens onder het verschoningsrecht vallen. Tevens beoordeelt hij globaal of de gegevens mogelijk relevant zijn voor het opsporingsonderzoek. Al dan niet via een 'geheimhouder-officier van justitie' dan wel de zaaksofficier van justitie worden de gegevens die relevant zijn en mogelijk onder het verschoningsrecht vallen aan de rechter-commissaris voorgelegd. De rechter-commissaris beoordeelt vervolgens de gegevens die na de voorselectie door de officier van justitie aan hem worden voorgelegd. In dit verband kan tevens worden gewezen op een uitspraak in kort geding van 22 maart 2022 van de rechtbank Oost-Brabant (ECLI:NL:RBOBR:2022:1035). Het OM heeft op deze uitspraak in kort geding gereageerd met een publicatie op de website van het OM van 'voorlopig beleid' (in afwachting van een aanwijzing van het College van procureurs-generaal en van de uitkomst van het hoger beroep).

Analyse en beoordeling van het beleidskader omtrent geheimhoudersgegevens

Met het oog op het waarborgen van de betrouwbaarheid, integriteit en herleidbaarheid van de gegevens die zijn verkregen bij het onderzoek in een geautomatiseerd werk, stelt het OM zich in de interne notitie op het standpunt dat de bepalingen in het Bogw prevaleren boven de bepalingen in het Besluit bewaren en vernietigen niet-gevoegde stukken. Dit standpunt wordt gebaseerd op de grond dat het Bogw een meer specifieke regeling betreft dan het Besluit bewaren en vernietigen niet-gevoegde stukken. Problematisch aan dit standpunt is volgens de onderzoekers dat het hier niet (uitsluitend) gaat om conflicterende rechtsregels van gelijke rangorde.[458] De vernietiging van gegevens die onder een verschoningsrecht vallen wordt voorgeschreven door een bepaling uit het Wetboek van Strafvordering, te weten artikel 126aa lid 2, dat van hogere rangorde is dan het Bogw. De artikelen 4 en 4a van het Besluit bewaren en vernietigen niet-gevoegde stukken werken dit voorschrift slechts nader uit. Het staat de digit-officier alleen al om die reden niet vrij om vast te stellen dat het Bogw, als de meer specifieke regeling, prevaleert boven de bepalingen van het Besluit bewaren en vernietigen niet-gevoegde stukken.

Het in de interne notitie en door de digit-officier omschreven beleid voorziet op zichzelf in de filtering van geheimhoudersgegevens uit de gegevens die bij de procestukken worden gevoegd. Als gevolg daarvan nemen de leden van het tactische team die uitvoering geven aan het opsporingsonderzoek, geen kennis van de ongefilterde gegevens en kan het tactisch team alleen al om die reden geen gebruik maken van geheimhoudersgegevens. Dit beleid voorziet echter niet in de filtering van dergelijke gegevens uit de technische infrastructuur van Digit en uit de forensische kopieën die worden vervaardigd van de gegevensdragers waartoe Digit zich bij het onderzoek in een geautomatiseerd werk toegang heeft verschaft. Die werkwijze staat op gespannen voet met artikel 126aa lid 2 Sv en het Besluit bewaren en vernietigen niet-gevoegde stukken. Tegelijkertijd verhoudt het bewerken, vernietigen of wijzigen van de vastgelegde gegevens zich niet met artikel 7 en artikel 28 Bogw, die de betrouwbaarheid, integriteit en herleidbaarheid van de gegevens die zijn verkregen bij het onderzoek in een geautomatiseerd werk beogen te waarborgen. De digit-officier heeft laten weten dat het bewerken, wijzigen of vernietigen van door Digit vastgelegde gegevens de integriteit en betrouwbaarheid van de gehele bewijslogging raakt.

Het komt de onderzoekers voor dat de hiervoor beschreven ongerijmdheid in de regelgeving de aandacht behoeft van de minister en dat daarin niet, althans niet op langere termijn, kan worden voorzien door uitsluitend beleidsregels van het OM. De onderzoekers achten het raadzaam om in dit verband een (wettelijke) grondslag te geven aan een regisserende rol voor de rechter-commissaris. In afwachting van nieuwe regelgeving zou (ook) het OM erop kunnen aansturen de rechter-commissaris een regisserende rol toe te kennen.
De kwestie zou bovendien onderdeel moeten zijn van het bredere debat over de wijze waarop het verschoningsrecht bij de uitoefening van bijzondere opsporingsbevoegdheden in acht wordt genomen en over de methode van het (selectief) bewaren c.q. vernietigen van digitale gegevens waarop het verschoningsrecht (mogelijk) van toepassing is.

[458] Ingeval twee onverenigbare rechtsregels tegelijkertijd van toepassing zijn, wijzen conflictregels uit welke van de twee rechtsregels voorrang heeft. Conflictregels zijn zelf niet in de wet vastgelegd. Zij vloeien voort uit de systematiek (en hiërarchie) van regelgeving en uit de interpretatie van conflicterende bepalingen. De drie conflictregels zijn: (1) de hogere rechtsregel gaat voor een lagere rechtsregel (bijvoorbeeld: de wet in formele zin prevaleert boven een uitvoeringsbesluit), (2) de bijzondere rechtsregel gaat voor een algemene rechtsregel (de rechtsregel die specifiek is toegesneden op de geregelde materie prevaleert boven rechtsregels die een breder bereik hebben), (3) de nieuwere rechtsregel gaat voor een oudere rechtsregel. Indien deze conflictregels onderling tot verschillende uitkomsten leiden, gaat de eerste conflictregel voor de tweede, en de tweede conflictregel voor de derde. Een nieuwere rechtsregel van lagere rangorde zet de oudere rechtsregel van hogere rangorde dus niet opzij. Net zomin zet een speciale rechtsregel van lagere rangorde de meer algemene rechtsregel van hogere rangorde opzij, behoudens indien – zoals veelvuldig het geval is – de algemene rechtsregel van hogere rangorde voorziet in delegatie van regelgeving naar speciale uitvoeringsregelingen die onder bepaalde condities een afwijking van de algemene rechtsregel toelaat (maar dan is er geen conflict van rechtsregels als hier bedoeld).

5. De bespreking van de uitvoeringspraktijk

Tegen de achtergrond van de vastgestelde kaders die in de hoofdstukken 3 en 4 zijn verkend, worden in dit hoofdstuk de tijdens het onderzoek verkregen resultaten besproken in deelonderwerpen of thema's. Deze deelonderwerpen betreffen een of meer fasen van de inzet van de bevoegdheid van artikel 126nba Sv.[459] Dat zijn de besluitvormingsfase, de uitvoeringsfase en de fase van de beëindiging van de bevoegdheid.

5.1. De organisatie van het werkproces

Algemeen

In het vorige hoofdstuk is melding gemaakt van het bestaan van de Instructie voor de inzet van de bevoegdheid ex artt. 126nba, 126uba, 126zpa en 126ffa Sv, van 15 oktober 2021 (hierna opnieuw: de Instructie). Bij het toezichtonderzoek is geconstateerd dat de besluitvorming aangaande de toepassing van artikel 126nba Sv in de praktijk overeenkomt met de door de Instructie voorgeschreven organisatie van het werkproces. Deze constatering betreft niet alleen de uitvoeringspraktijk van ná de inwerkingtreding van de Instructie, maar ook die van daarvoor. In zoverre vormt de Instructie dus niet alleen een normerend instrument, maar tevens een later opgemaakte, adequate beschrijving van de organisatie van het werkproces in de reeds langer bestaande praktijk.

De rol van LP Digit en de uitvoering daarvan

Zoals hiervoor beschreven heeft de invoering van de Wet computercriminaliteit III binnen de organisatie van het OM geleid tot de aanstelling van een digit-officier die in samenwerking met de digit-parketsecretaris en met inachtneming van de hiërarchie binnen het OM exclusief verantwoordelijk is voor en toezicht houdt op de uitvoering door Digit van de bevelen die op de voet van artikel 126nba Sv door zaaksofficieren zijn afgegeven. In het voorafgaande overleg met de zaaksofficier (zie de Instructie, onder het kopje 'Intake en vooronderzoek') fungeert de digit-officier als poortwachter voor de inzet van de bevoegdheid. Hij beoordeelt zelfstandig de rechtmatigheid, de haalbaarheid, de risico's en de prioriteiten. Bij een onoplosbaar verschil van inzicht tussen de digit-officier en de zaaksofficier zal de besluitvorming op een hoger niveau binnen de hiërarchie van het OM plaatsvinden. Die situatie heeft zich naar zeggen van de digit-officier (nog) niet voorgedaan.

LP Digit vormt een gespecialiseerd onderdeel van het OM, waaraan dienovereenkomstige, hoge eisen worden gesteld. De personele invulling van de functies van de digit-officier en digit-parketsecretaris is wat dit betreft geheel op orde.
Mede doordat over de wijze waarop het onderzoek in een geautomatiseerd werk wordt uitgevoerd – ook binnen het OM – strikte geheimhouding wordt betracht, bestaat het gevaar dat veel informatie vrijwel uitsluitend is belegd bij LP Digit en Digit. Die stand van zaken bergt organisatorische risico's in zich, zoals het verlies van essentiële kennis bij het onverhoopte uitvallen van de digit-officier en de digit-parketsecretaris, alsmede het gevaar van onvoldoende gecontroleerd, solistisch optreden. Hieraan is in het toezichtonderzoek aandacht besteed.

Zaaksofficieren zijn in sterke mate afhankelijk van de (kennis van de) digit-officier en -parketsecretaris en zij laten zich door hen adviseren. Deze adviezen zijn in alle onderzochte zaken opgevolgd. Ook rechercheofficieren en de CTC zijn tot op zekere hoogte afhankelijk van de (kennis van de) digit-officier en -parketsecretaris en vertrouwen op hun professionaliteit, met dien verstande dat de rechercheofficieren die zijn verbonden aan het landelijk parket en de CTC meer in detail op de hoogte plegen te worden gesteld van de werkwijze bij de

[459] Evenals in het voorgaande hoofdstuk zal niet steeds separaat (tevens) worden verwezen naar de artikelen 126uba en 126zpa Sv en zal worden volstaan met een verwijzing naar art. 126nba Sv waar ook de artikelen 126uba en 126zpa Sv worden bedoeld.

uitvoering van onderzoek in een geautomatiseerd werk, zodat ook zij de rechtmatigheid, haalbaarheid en de risico's van de inzet van de bevoegdheid kunnen inschatten. Mede daardoor opereert LP Digit niet in een vacuüm: meer algemene notities, handreikingen en een vastgelegde manier van werken worden keer op keer voor akkoord voorgelegd aan een bredere kring van betrokkenen: de landelijk rechercheofficier of de vergadering van rechercheofficieren. Ook de CTC stelt zich kritisch op en doet suggesties. Daarnaast zijn er zogeheten 'reflectiekamers'[460] georganiseerd voor het bespreken van juridische probleempunten die zich in de praktijk van LP Digit gaandeweg voordeden.
Als gevolg daarvan is van een organisatorische kwetsbaarheid geen sprake. Van solistisch optreden van de digit-officier en de digit-parketsecretaris blijkt niet.

De schakelfunctie van de officier van justitie

De schakelfunctie tussen het technische team en het tactische team wordt volgens de Instructie vervuld in het overleg tussen de digit-officier (aanspreekpunt Digit) en de zaaksofficier (aanspreekpunt van het tactische team). Zowel uit de Instructie als uit de praktijk blijkt dat de schakelfunctie over twee schakels loopt. De zaaksofficier en de digit-officier informeren elkaar over en weer en beleggen de informatie bij hun eigen teams. In dit verband is overigens niet uitgesloten dat er ook overleg plaatsvindt tussen Digit, de digit-officier, de leider van het tactische team en de zaaksofficier gezamenlijk.[461]
De zaaksofficieren met wie semigestructureerde interviews hebben plaatsgehad konden niet uitsluiten dat er sporadisch, informatief contact plaatsvond rechtstreeks tussen het tactische team en Digit, zonder betrokkenheid van de zaaksofficier. Dat vonden de zaaksofficieren niet problematisch.
Rechtstreeks contact tussen het technische en het tactische team komt in de praktijk (inderdaad) voor, zonder tussenkomst van de zaaksofficier, doorgaans als het technische team tijdens de daadwerkelijke uitvoering van onderzoek in een geautomatiseerd werk (hierna ook: een 'actie' of een 'inzet') over bepaalde informatie moet beschikken. De digit-officier heeft in die gevallen meer betrokkenheid omdat het gebruikelijk is dat hij op cruciale momenten tijdens een actie van Digit op locatie aanwezig is. De zaaksofficier heeft daarentegen niet noodzakelijkerwijze steeds diezelfde mate van betrokkenheid bij een actie zodat het praktisch minder goed uitvoerbaar is om het contact tussen technisch en tactisch team telkens (tevens) via de zaaksofficier te laten verlopen.

Het voorgaande wijst uit dat de schakelfunctie tussen het technische team (Digit) en het tactische team in de uitvoeringspraktijk een enigszins andere invulling heeft gekregen dan de minister aanvankelijk voor ogen stond. De minister ging ervan uit dat de contacten tussen het tactische team en het technische team plaatshebben door tussenkomst van 'de' officier van justitie, waarbij de minister toentertijd het oog had op de zaaksofficier. Bij deze constatering moet evenwel in aanmerking worden genomen dat de wetsgeschiedenis die blijk geeft van de opvattingen van de minister omtrent de schakelfunctie van 'de' officier van justitie tot stand is gekomen op een moment dat de minister nog niet bekend kon zijn met het bestaan van een digit-officier aan wie de schakelfunctie als zodanig eveneens kan worden toevertrouwd.

Dat de regie van overleg tussen het tactische team en Digit in de praktijk meer bij de digit-officier is komen te liggen, komt de onderzoekers niet problematisch voor. Door de nauwe betrokkenheid van de digit-officier en digit-parketsecretaris is de schakelfunctie voldoende geborgd. Van de zijde van het OM bestaat voldoende controle op hetgeen met de schakelfunctie wordt beoogd, namelijk vermijden dat het tactische team (op oneigenlijke

[460] De 'reflectiekamer' vormt een op ad-hocbasis samengesteld gremium binnen het OM, waaraan zeer ervaren OM'ers deelnemen, met het oog op de beantwoording van specifieke juridische probleempunten.
[461] In paragraaf 3.3 hierboven werd dit overleg 'het juridisch-operationeel overleg' genoemd. In de informele notitie is dit overleg vermeld onder punt 8 (zie paragraaf 4.1 hierboven).

gronden) invloed kan uitoefenen op het binnendringen in het geautomatiseerde werk en de plaatsing, inzet en verwijdering van een technisch hulpmiddel.

Hiermee niet in strijd is een bevinding van de Inspectie Justitie en Veiligheid, namelijk de vaststelling dat tijdens acties in 2019 en 2021 enkele malen direct (telefonisch) contact heeft plaatsgevonden tussen Digit en leden van het tactisch team. Overigens heeft ook de Inspectie geen aanwijzing dat het tactische team tijdens de inzet van de bevoegdheid invloed heeft uitgeoefend op het binnendringen in het geautomatiseerde werk en op de plaatsing, inzet en verwijdering van een technisch hulpmiddel.[462]

5.2. De besluitvorming omtrent de inzet van de bevoegdheid ex artikel 126nba Sv

Algemeen

In de onderzochte periode (maart 2019 tot en met december 2021) hebben zich 43 zaken aangediend waarin de bevoegdheid van artikel 126nba Sv (eenmaal of meermalen) is uitgeoefend. Dit aantal over deze periode duidt niet op een grootschalige, ongecontroleerde en ongebreidelde toepassing van de bevoegdheid.[463] De frequentie neemt in de loop van de onderzochte periode overigens wel duidelijk toe.[464]
Bij de bestudering van de nba-dossiers[465] in het kader van het toezichtonderzoek kan uiteraard geen volledig zicht worden verkregen op alle overlegstructuren binnen het werkproces. Niettemin zijn bij de bestudering van de geselecteerde nba-dossiers (vooralsnog) geen aanwijzingen gevonden dat de procedure die strekt tot besluitvorming over de toepassing van de bevoegdheid in de praktijk noemenswaardig afwijkt van de procedure die in het toepasselijke materieelrechtelijke kader is voorzien (zie hoofdstuk 3) of van het beleidskader dat is uiteengezet in de hiervoor genoemde notitie van de digit-officier en in de Instructie (zie hoofdstuk 4).

De verschillende stappen in de besluitvorming

De verschillende stappen in het besluitvormingsproces bleken in alle onderzochte zaken telkens vastgelegd in het nba-dossier. Daarin bevonden zich standaard:

- een (uitgebreid) proces-verbaal aanvraag toepassing van artikel 126nba Sv, afkomstig van het tactische team (het projectvoorstel), eventueel met bijlagen bevattende bevindingen van het tot dan toe uitgevoerde opsporingsonderzoek;
- een rapport haalbaarheidsonderzoek afkomstig van Digit;
- een adviesaanvraag aan de CTC, afkomstig van de zaaksofficier, door tussenkomst van de (plaatsvervangend) hoofdofficier van justitie toegezonden aan de CTC, met als bijlagen de hiervoor genoemde stukken;
- een uitgebreid (telkens positief) advies van de CTC, waaruit tevens blijkt dat het verzoek voorafgaande aan de advisering mondeling aan de CTC is toegelicht door de zaaksofficier en een of meer leden van het tactische team, en dat vervolgens de digit-officier en leden van het technische team – buiten aanwezigheid van de zaaksofficier en leden van het tactische team – de haalbaarheid van het onderzoek en de risico's ervan aan de CTC hebben uiteengezet;
- een document c.q. aantekening waaruit blijkt dat het College van procureurs-generaal

[462] Zie Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2019*, Den Haag: Ministerie van Justitie en Veiligheid 2020, p. 25 en Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2021*, Den Haag: Ministerie van Justitie en Veiligheid 2022, p. 25.
[463] Zo ook het oordeel van de Inspectie Justitie en Veiligheid over het jaar 2020, zie Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2020*, Den Haag: Inspectie Justitie en Veiligheid 2021, p. 3.
[464] Hieronder zal dieper worden ingegaan op de aantallen zaken en zal worden stilgestaan bij de wijze van telling.
[465] Zie voor toelichting op het hier gehanteerde begrip 'nba-dossier' paragraaf 2.3 hierboven.

heeft ingestemd met de toepassing van de bevoegdheid;
- de vordering van de zaaksofficier aan de rechter-commissaris tot het verlenen van machtiging voor het bevel als bedoeld in artikel 126nba Sv, met als bijlagen het projectvoorstel en de daarbij gevoegde bijlagen;
- de machtiging van de rechter-commissaris;
- het bevel van de zaaksofficier tot toepassing van artikel 126nba Sv.

Bij de aanvraag tot verlenging of bij de aanvraag tot uitbreiding van de toepassing van artikel 126nba Sv werd telkens mutatis mutandis dezelfde procedure gevolgd, zij het ten dele onder verwijzing naar eerder opgemaakte documenten.

De materiële eisen voor de inzet van de bevoegdheid

Aan de hand van dossieronderzoek is in de onderzochte zaken nagegaan of:
1. de gerezen verdenking voldoende is geconcretiseerd en onderbouwd,
2. de bevoegdheid is ingezet in gevallen waarin de wet die bevoegdheid openstelt,
3. het delict gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert,
4. is voldaan aan beginselen van proportionaliteit en subsidiariteit.

Het gaat hier telkens om de eisen die in paragraaf 3.1 zijn voorzien van een toelichting.

Vastgesteld is dat in geen van de onderzochte zaken enige twijfel bestaat over het bevestigende antwoord op de hiervoor opgesomde vragen. In alle gevallen is de gerezen verdenking voldoende geconcretiseerd in het projectvoorstel (i.e. het proces-verbaal van aanvraag (met bijlagen)), alsook in de adviesaanvraag aan de CTC en in het advies van de CTC zelf. Bovendien is in die documenten telkens uitvoerig stilgestaan bij de vraag of er alternatieven voorhanden zijn die minder ingrijpen in de persoonlijke levenssfeer van de betrokkene(n). De vragen naar de noodzaak, het verwachte resultaat en het afbreukrisico, alsook het risico voor het geautomatiseerde werk zijn nadrukkelijk (en telkens uitvoerig) onder ogen gezien. De daaraan gewijde passages betreffen geen routinematige 'standaardbeschouwingen'.

De bevelen tot toepassing van de bevoegdheid en de verlenging daarvan

Bovendien is in het toezichtonderzoek nagegaan of de vorderingen aan de rechter-commissaris tot het verlenen van een machtiging voor het bevel ex artikel 126nba Sv, alsmede dat bevel zelf, ook overigens voldeden aan de eisen die de wet daaraan stelt (zie paragraaf 3.4 hierboven). Datzelfde geldt voor de verlenging, wijziging of aanpassing van een en ander, indien van toepassing. Over het algemeen is vastgesteld dat de vorderingen en de bevelen met elkaar en met de machtigingen correspondeerden en dat de vorderingen en bevelen voldeden aan de wettelijke voorschriften. Wel zijn een aantal onvolkomenheden en bijzonderheden geconstateerd die hierna worden besproken. Daaraan voorafgaand verdient de volgende kwestie enige aandacht.

Niet-functionele eis die in de wet, het Bogw of de wetsgeschiedenis aan het bevel wordt gesteld

In de memorie van toelichting is opgenomen dat de reden waarom niet met de toepassing van een andere wettelijke bevoegdheid (dan die van artikel 126nba Sv) kan worden volstaan, in het bevel dient te worden vermeld, zulks opdat de rechter-commissaris in staat wordt gesteld om deze voorwaarde (de subsidiariteitseis) te toetsen, aldus de minister.[466] Een dergelijke eis wordt echter in de wet zelf, bijvoorbeeld artikel 126nba lid 2 Sv, aan het bevel niet gesteld. Het ligt op zichzelf ook niet voor de hand dat de reden van de keuze voor de toepassing van artikel 126nba Sv (en niet voor eventuele alternatieven) wordt opgenomen in het bevel, aangezien die reden de opsporingsambtenaren van het technische team tot

[466] Hierboven besproken in paragraaf 3.1 onder 'Beginselen van proportionaliteit en subsidiariteit'.

wie het bevel zich richt in principe niet aangaat. Indien die reden wordt weergegeven in het proces-verbaal (van de zaaksofficier) dat als bijlage gaat bij de vordering tot het verlenen van een machtiging voor een bevel als hier bedoeld, wordt tegemoetgekomen aan de ratio van de toevoeging van dergelijke informatie, namelijk dat de rechter-commissaris in staat wordt gesteld om te toetsen of aan het subsidiariteitsbeginsel is voldaan.
In de nba-dossiers die zijn onderzocht was de reden waarom niet met een andere wettelijke opsporingsbevoegdheid (dan die van artikel 126nba Sv) kon worden volstaan *niet* opgenomen in de onderscheidene bevelen van de zaaksofficier, maar wel uitdrukkelijk aan de orde gesteld in de processen-verbaal die als bijlage(n) bij de vordering tot het verlenen van een machtiging zijn toegezonden aan de rechter-commissaris.

Constateringen
Dan wordt nu toegekomen aan het uitlichten van enkele (overige) onvolkomenheden en bijzonderheden in de onderzochte zaken.

Aanduiding van het geautomatiseerd werk
Tijdens het onderzoek is in één zaak de vraag opgekomen of in het bevel ex artikel 126nba Sv de specificatie van een van de geautomatiseerde werken toereikend was. Het ging hier om een onbekende smartphone waarvan de specificatie werd beperkt tot de vermelding van een telefoonnummer en de naam van de verdachte. Dit betreffen echter geen specifieke – (nagenoeg) onoverdraagbare – eigenschappen van het geautomatiseerd werk zelf, zoals een IMEI-nummer.

Aanduiding van de aard en functionaliteit van het technisch hulpmiddel
Het bevel dient volgens artikel 126nba lid 2 onder d Sv een aanduiding te bevatten van de aard en functionaliteit van het technisch hulpmiddel dat wordt gebruikt voor de uitvoering van het bevel. Die aanduiding betrof in een enkel geval slechts een abstracte omschrijving, waarbij de functionaliteiten van het technisch hulpmiddel niet concreet werden genoemd: "*een softwareapplicatie waarmee bovenbedoelde gegevens kunnen worden vastgelegd.*"
In een later bevel in dezelfde zaak (maar ook in de bevelen in andere zaken) hebben de onderzoekers geconstateerd dat de functionaliteiten wel (meer) concreet en specifiek zijn omschreven. Zo bevat het tweede bevel in de eerdergenoemde zaak als aanduiding van het technisch hulpmiddel:

> "*softwareapplicatie waarmee gegevens kunnen worden vastgelegd met de volgende functionaliteiten:*
> *a Vastleggen van gegevens*
> *b Opnemen beeld en geluid, waaronder communicatie*
> *c Bepalen plaats*"

Dit kan als een voldoende specifieke aanduiding van de aard en functionaliteit van het technisch hulpmiddel worden beschouwd, te meer als daarbij de vermelding van de categorie van gegevens waarop het bevel betrekking heeft, in aanmerking wordt genomen. De categorieën van deze gegevens stonden afzonderlijk in het bevel vermeld en betreffen e-mailberichten, foto's of belgegevens.
Op dit punt heeft LP Digit de werkwijze al doende verder ontwikkeld en verbeterd. Een concrete en specifieke omschrijving van de functionaliteiten is nu het uitgangspunt.

Omschrijving onderzoekshandelingen
De omschrijving van de onderzoekshandelingen als bedoeld in artikel 126nba lid 1 onder a, d of e Sv in het bevel was in een tweetal zaken betrekkelijk abstract en summier. Die omschrijving luidde in één zaak bijvoorbeeld:

> "*het binnentreden van het geautomatiseerd werk en vervolgens zonder gebruik te maken van een technisch hulpmiddel, in het geautomatiseerde werk zoeken naar identificerende en/of*

locatiegegevens als genoemd in artikel 126nba lid 1 onder a en het zoeken naar, historische en toekomstige, systeem gegevens als genoemd in artikel 126nba lid 1 onder d Sv."

De digit-officier en de digit-parketsecretaris hebben in dit verband te kennen gegeven dat per onderzoek verschillende gegevens worden opgehaald en dat gedurende de onderzoeksperiode (2019-2021) LP Digit van koers is gewijzigd over de vraag hoe concreet de onderzoekshandelingen in het bevel worden omschreven. In zaken waarin sprake is van maatwerk zal sneller worden besloten tot het meer concreet omschrijven van onderzoekshandelingen dan in zaken waarin sprake is van een meer gestandaardiseerde werkwijze. Dat betreft vooral zaken waarin wordt binnengedrongen op een geautomatiseerd werk door middel van het technisch hulpmiddel dat in dit rapport de codenaam 'TH Brons' heeft gekregen (waarover hieronder meer).
Wat betreft de onderzoeksdoelen van artikel 126nba Sv lid 1 onder a en d Sv heeft LP Digit het standpunt ingenomen dat de onderzoekshandelingen niet méér concreet kunnen worden omschreven dan dat "*gegevens worden overgenomen*". Indien ook wordt omschreven op welke wijze dat overnemen plaatsvindt, zal de toegepaste methode (mogelijk) worden prijsgegeven. LP Digit verwijst daarbij naar wetsgeschiedenis waaruit naar voren komt dat niet is vereist dat het bevel de methode vermeldt waarmee in een geautomatiseerd werk wordt binnengedrongen.[467] Afhankelijk van het type zaak en de wensen van het onderzoeksteam wordt volgens LP Digit gekozen voor hetzij een ruim bereik van de omschrijving van de onderzoekshandelingen, hetzij voor het gericht noemen van bepaalde gegevens waartoe het onderzoek zich beperkt. Volgens de digit-officier is in veel zaken op voorhand echter niet precies bekend welke gegevens zullen worden aangetroffen zodat in principe alle informatie relevant kan zijn.

De onderzoekers achten dit standpunt verdedigbaar. Tegelijkertijd zal erop toegezien moeten worden dat het onderzoek zo gericht mogelijk wordt verricht om een zogenoemde *'fishing expedition'* te voorkomen. De omschrijving van de onderzoekshandelingen behelst immers – tevens – een beperking van de gegevens die bij het onderzoek in een geautomatiseerd werk mogen worden geregistreerd.[468] Een nauwkeurige omschrijving van de onderzoekshandelingen in het bevel vormt daarmee een door de minister voorziene waarborg waarmee de bevoegdheid tot het verrichten van onderzoek in een geautomatiseerd werk is omgeven. Om die reden blijft een zo concreet mogelijke omschrijving van de onderzoekshandelingen een punt van aandacht. Aanwijzingen voor dergelijke '*fishing expeditions*' zijn in het toezichtonderzoek overigens niet aangetroffen.

Opnemen vertrouwelijke communicatie (OVC)

Als het bevel betrekking heeft op het opnemen van vertrouwelijke communicatie (OVC) op de voet van artikel 126l Sv of de stelselmatige observatie op de voet van artikel 126g Sv, kunnen in het bevel ex artikel 126nba Sv tevens de gegevens worden vermeld die in een bevel tot toepassing van artikel 126l Sv of artikel 126g Sv moeten worden opgenomen. Er is dan slechts één bevel nodig voor de toepassing van samenhangende bevoegdheden waarbij een geautomatiseerd werk op afstand heimelijk wordt binnengedrongen.[469] Uit de onderzochte zaken blijkt dat dit inmiddels praktijk is geworden. Er wordt dan een zogenaamd 'combi-bevel' afgegeven. Dit was echter niet van meet af aan de toegepaste werkwijze.
In een tweetal zaken is geconstateerd dat er nog sprake is van separate vorderingen, machtigingen en bevelen. Het ging hierbij om een afzonderlijk bevel op basis van artikel 126l Sv dat reeds was gegeven voor een 'reguliere' OVC, dat wil zeggen: zonder daarbij een geautomatiseerd werk op afstand heimelijk binnen te dringen. Nadien is een bevel op basis

[467] Zie daarover paragraaf 3.4 hierboven.
[468] Zie bijvoorbeeld paragraaf 3.9, onder het kopje 'Beoogde gegevens en bijkomende gegevens ('bijvangst').
[469] *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 30. In principe is voor de onderzoeksdoelen van art. 126nba lid 1 onder b en c namelijk een afzonderlijk bevel vereist, zie p. 100 en 102.

van artikel 126nba Sv afgegeven voor toepassing van OVC waarbij een geautomatiseerd werk op afstand heimelijk wordt binnengedrongen. In het bevel werd voor de locaties van OVC verwezen naar de eerdere vorderingen, machtigingen en/of bevelen van de reguliere toepassing van artikel 126l Sv.
Dat is volgens de onderzoekers in het algemeen een niet aan te raden werkwijze, alleen al omdat in de reguliere bevelen ex artikel 126l Sv is opgenomen dat de toepassing van OVC conform het Besluit technische hulpmiddelen zal plaatsvinden terwijl bij een inzet op basis van artikel 126nba Sv het Bogw leidend is. Zoals gezegd, is deze werkwijze gedurende de onderzoeksperiode gewijzigd en worden er thans combi-bevelen afgegeven.

5.3. De uitvoering van het bevel

Algemeen
De Inspectie heeft onderzocht in hoeverre de politie heeft gehandeld binnen de reikwijdte van de door de officier van justitie afgegeven bevelen. In dit verband heeft de Inspectie onder meer opgemerkt:

> *"De Inspectie heeft geen aanwijzingen dat de politie in 2020 de hackbevoegdheid heeft ingezet buiten de in de bevelen aangegeven periodes en onderzoeksdoelen. Tevens heeft de Inspectie geen aanwijzingen dat het technisch team van de politie in 2020 onderzoekshandelingen heeft verricht in een geautomatiseerd werk van een verdachte, zonder dat de officier van justitie een bevel voor toepassing van de hackbevoegdheid had afgegeven voor de betreffende verdachte."*[470]

> *"De Inspectie heeft geen aanwijzingen dat de politie in 2021 de hackbevoegdheid heeft ingezet buiten de in de bevelen aangegeven systemen."*[471]

Wel constateerde de Inspectie dat in 2020 Digit vier keer is binnengedrongen in een geautomatiseerd werk waarvan het unieke kenmerk niet correspondeerde met het kenmerk dat was opgenomen in het bevel. Hoewel het betreffende geautomatiseerde werk wel degelijk in gebruik was bij de verdachte wiens naam in het bevel was vermeld, is daardoor buiten de reikwijdte van het gegeven bevel gehandeld. Digit heeft twee van deze vier afwijkingen direct gesignaleerd en als onregelmatigheid gemeld aan de digit-officier. De Inspectie heeft vastgesteld dat Digit in deze twee gevallen geen onderzoekshandelingen heeft verricht. De andere twee gevallen betreffen twee zaken die ook in dit toezichtonderzoek zijn onderzocht. De Inspectie schrijft daarover in haar verslag van 2020:

> *"In de twee andere situaties heeft de Inspectie na afronding van de inzet door de politie geconstateerd dat de politie op een verkeerd geautomatiseerd werk is binnengedrongen. In deze situaties heeft de politie onderzoekshandelingen verricht en gegevens vastgelegd. De Inspectie heeft de politie hiervan op de hoogte gebracht. Door het hanteren van het verkeerde kenmerk van het geautomatiseerde werk heeft de politie in deze situaties ten aanzien van dit aspect buiten de reikwijdte van het afgegeven bevel gehandeld, waardoor de verkregen gegevens mogelijk niet gebruikt kunnen worden in de betreffende strafzaak. De Inspectie merkt hierbij op dat uit de vastgelegde gegevens is gebleken dat beide geautomatiseerde werken wel in gebruik waren bij de desbetreffende verdachten."*[472]

---

[470] Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2020*, Den Haag: Inspectie Justitie en Veiligheid 2021, p. 10.
[471] Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2021*, Den Haag: Inspectie Justitie en Veiligheid 2022, p. 10
[472] Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2020*, Den Haag: Inspectie Justitie en Veiligheid 2021, p. 10.

De zaaksofficier van justitie heeft in één van twee zaken waarin dit onderzoek tot de verkrijging van gegevens heeft geleid, besloten de aldus verkregen gegevens in de strafzaak niet te gebruiken en te vernietigen. De onderzoekers hebben geconstateerd dat de feitelijke vernietiging niet spoedig plaatsvond na de afgifte van het bevel.
In de andere zaak waarin dit onderzoek tot de verkrijging van gegevens heeft geleid, heeft de zaaksofficier van justitie aan de rechter-commissaris verzocht om zich uit te laten over de onrechtmatigheid. De rechter-commissaris heeft laten weten dat hij de machtiging ook had verstrekt indien in de vordering melding was gemaakt van het juiste unieke kenmerk van het geautomatiseerde werk. De verkregen gegevens in dit onderzoek heeft LP Digit vervolgens niet vernietigd, maar bewaard, teneinde die te kunnen gebruiken in de strafzaak (waarin de zittingsrechter zich ook over de rechtmatigheid van de verkregen gegevens kan uitlaten). Op vragen van de onderzoekers waarom in deze zaak wel om een oordeel van de rechter-commissaris is gevraagd terwijl in de andere zaak de gegevens zijn vernietigd, gaf de digit-officier te kennen dat in deze zaak relevante en bruikbare gegevens waren vergaard, terwijl dat in de andere zaak niet het geval was.

Tot slot signaleert de Inspectie over 2021 dat niet alle door Digit uitgevoerde opsporingshandelingen vallen binnen de reikwijdte van de door de officier van justitie afgegeven bevelen. In enkele situaties is op de volgende onderdelen (mogelijk) afgeweken:

> *"- in één zaak is een technisch hulpmiddel ingezet dat mogelijk standaard locatiegegevens vastlegt bij bepaalde handelingen door de gebruiker van het onderzochte geautomatiseerd werk. De Inspectie signaleert dat deze vastlegging van locatiegegevens mogelijk kenmerken heeft van stelselmatige observatie. In de zaak waarin dit hulpmiddel is ingezet, is echter geen bevel afgegeven voor het middels de hackbevoegdheid stelselmatig observeren van de betreffende verdachte;*
> - *in één zaak is eenmalig als test een geluidsopname gestart op het geautomatiseerde werk van een verdachte, zonder dat daarvoor op dat moment een bevel aan ten grondslag lag. Dat bevel is overigens naderhand op dezelfde dag wel verstrekt;*
> - *in één zaak heeft DIGIT een beëindigingsbevel ontvangen waarmee de looptijd van een eerder gegeven bevel werd verkort. DIGIT was hiervan niet op de hoogte gesteld en ontving dit bevel pas toen het aangegeven beëindigingsmoment reeds was verstreken. In de tussentijd hebben wel onderzoekshandelingen plaatsgevonden. DIGIT heeft hier proces-verbaal voor opgesteld en de betreffende gegevens weggelaten uit de finale overdracht van verzamelde gegevens aan het tactisch team. In een tussentijdse overdracht waren deze gegevens echter reeds overgedragen."*[473]

In zijn commentaar op het concept van dit rapport heeft het OM over deze bevindingen van de Inspectie het volgende laten weten.

In de zaak die onder het eerste gedachtestreepje wordt genoemd ging het om de vastlegging van locatiegegevens die reeds op het geautomatiseerde werk waren opgeslagen. Dit betrof locatiegegevens die door de gebruiker of het geautomatiseerde werk zelf waren gegenereerd, bijvoorbeeld door het gebruik van een specifieke applicatie of instelling. De digit-officier is – in zijn algemeenheid – van oordeel dat het vastleggen van dergelijke gegevens valt onder het bereik van het onderzoeksdoel van artikel 126nba lid 1 sub d Sv.
De onderzoekers achten dit een verdedigbaar standpunt.

In de zaak die de Inspectie vermoedelijk onder het tweede gedachtestreepje bedoelt, gaat het om een geluidsopname die is gestart, terwijl in het (gecombineerde) bevel ex artikel

[473] Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2021*, Den Haag: Inspectie Justitie en Veiligheid 2022, p. 18. De betreffende zaken vallen buiten door de PG-HR geselecteerde en onderzochte zaken voor de dossierstudie.

126nba Sv jo artikel 126l Sv de besloten locatie waar het geautomatiseerd werk zich op dat moment bevond, niet was benoemd. Voor die besloten locatie was echter wel een regulier bevel ex artikel 126l Sv afgegeven. Toen dit duidelijk werd, heeft de digit-officier de betrokken medewerkers van Digit direct geïnstrueerd te stoppen met het maken van geluidsopnames en de reeds gemaakte opname (nog) niet te verstrekken aan het tactisch team. De digit-officier heeft daarna contact gehad met de zaaksofficier van justitie. De zaaksofficier van justitie heeft hierop een mondelinge machtiging van de rechter-commissaris gekregen om te mogen bevelen dat ex artikel 126nba Sv jo artikel 126l Sv ook op de betreffende besloten plaats vertrouwelijke communicatie mocht worden opgenomen (nadat was binnengedrongen in het geautomatiseerd werk). De rechter-commissaris is daarbij geïnformeerd over de reeds gemaakte opname. Hierna heeft de zaaksofficier van justitie het (gecombineerde) bevel ex artikel 126nba Sv jo artikel 126l Sv (mondeling) uitgebreid. Na deze uitbreiding van het bevel is de geluidsopname in opdracht van de digit-officier overgedragen aan het tactisch team, aldus de mededelingen van het OM.
Naar het oordeel van de onderzoekers heeft het OM aldus voldoende adequaat gehandeld.

De situatie die door de Inspectie onder het derde gedachtestreepje wordt beschreven, lijkt betrekking te hebben op een zaak waarin door de zaaksofficier van justitie een beëindigingsbevel was afgegeven die op diezelfde dag in ging (dag 1). Dit bevel is (uiteindelijk) na twee dagen door de zaaksofficier van justitie, via het tactisch team aan Digit verstrekt. Op de dag na de bevolen beëindigingsdatum (dag 2) heeft Digit nog data veiliggesteld en overgedragen aan het tactisch team. De hierop volgende dag (dag 3) is het beëindigingsbevel door Digit ontvangen. Dit bevel ging uit van beëindiging per dag 1. Na constatering van een en ander is door LP Digit overleg gevoerd met de zaaksofficier van justitie. De slotsom van dat overleg was dat het beëindigingsbevel niet werd aangepast, dat Digit een nieuwe dataset aan het tactisch team zou overdragen van de data tot en met dag 1 en dat de data die op dag 2 was vastgelegd enkel bij Digit opgeslagen zouden blijven. Hierbij verdient nog opmerking dat de op dag 2 vastgelegde gegevens binnen het bestek vielen van de door de rechter-commissaris verstrekte machtiging en het initieel afgegeven bevel, aldus de mededelingen van het OM.
Naar het oordeel van de onderzoekers heeft de zaaksofficier er onvoldoende op toegezien dat aan het beëindigingsbevel tijdig uitvoering kon worden gegeven. Als gevolg daarvan heeft Digit data aan het tactische team overgedragen zonder dat Digit ervan op de hoogte kon zijn dat daaraan geen (op dat moment nog) geldend bevel ten grondslag lag.

Uitvoering in combinatie met OVC

Ten aanzien van het opnemen van vertrouwelijke communicatie (OVC) in combinatie met het onderzoek in een geautomatiseerd werk nog het volgende. LP Digit heeft te kennen gegeven dat OVC alleen op bepaalde momenten wordt ingezet, bijvoorbeeld op het moment dat de verdachte met zijn telefoon op een locatie aanwezig is waar hij heeft afgesproken met andere verdachten, terwijl op basis van andere opsporingsinformatie valt te verwachten dat op die plek en dat tijdstip voor het onderzoek relevante onderwerpen worden besproken.
Uit het dossieronderzoek is gebleken dat de CTC in de adviesaanvragen veelvuldig aandacht besteedt aan dit aspect van OVC. Anders dan bij reguliere OVC ex artikel 126l Sv, waarbij een microfoon (een 'bug') wordt geplaatst op een vaste plek (een woning bijvoorbeeld), kan OVC in het kader van artikel 126nba Sv worden ingezet op bijvoorbeeld een mobiele telefoon. In dat geval bevindt de OVC zich niet op een gefixeerde locatie. De OVC-functie wordt daarom alleen geactiveerd wanneer het geautomatiseerd werk zich op een specifieke plaats bevindt. In dit soort gevallen raadt de CTC aan zoveel mogelijk zicht te houden op de verdachte(n), zodat wordt gewaarborgd dat vertrouwelijke communicatie alleen wordt opgenomen op die plekken die zijn ondervangen in het bevel.
In een bepaalde zaak adviseerde de CTC om met de rechter-commissaris een procedure af te spreken waarin de rechter-commissaris benaderd kan worden zodra uit observaties of datagegevens blijkt dat de verdachten een andere woning (dan die is genoemd in het bevel) betreden en waarbij het noodzakelijk is dat OVC ingeschakeld wordt.

Als de keuze wordt gemaakt om alleen bepaalde gesprekken op te nemen, raadt de CTC doorgaans aan om dit vooraf te ondervangen in het bevel. Er kan hierbij worden gekozen voor het afgeven van een bevel voor meer kortdurende periodes; deze periodes betreffen momenten waarop de verdachten blijkens observaties of datagegevens een ontmoeting hebben. Het onderbreken van de inzet zal in dat geval moeten blijken uit het dossier. De CTC is in dit soort zaken van oordeel dat het van belang is om goed te verantwoorden wanneer en bij welke ontmoetingen OVC op de mobiele telefoon wel en niet ingeschakeld wordt, zulks om willekeur te voorkomen. De CTC overwoog in verscheidene adviezen dat zij zich realiseert dat het verantwoorden lastig kan zijn als daarmee de methode prijsgegeven moet worden. Het onderzoeksteam zal zich volgens de CTC hierover met LP Digit moeten verstaan en de verantwoording geldt voor zover de afscherming van het middel dat toelaat, aldus de CTC.
In de onderzochte zaken waarbij sprake was van OVC hebben de onderzoekers geen stukken aangetroffen waaruit de verantwoording (achteraf) expliciet blijkt. Wel volgt uit de stukken duidelijk op welke plekken en waarom op die plekken gesprekken (zullen) worden opgenomen. De digit-officier heeft te kennen gegeven dat het technisch niet altijd mogelijk is om OVC op mobiele apparaten voortdurend te laten doorlopen. Daarom kiest LP Digit ervoor OVC over de band van artikel 126nba Sv gericht aan en uit te zetten.

De onderzoekers achten dit laatste niet problematisch en zelfs aan te bevelen. Op die manier wordt immers voorkomen dat wordt opgenomen op andere plekken dan in het bevel voorzien. LP Digit heeft te kennen gegeven dat het tactische team bijvoorbeeld de verdachte en/of het geautomatiseerd werk waarop de OVC-functie is geïnstalleerd, observeert zodat dit op het juiste moment kan laten weten wanneer de mobiele telefoon zich op een locatie bevindt die is ondervangen in het bevel. Wel dient – om willekeur te voorkomen en disproportioneel optreden tegen te gaan – te worden verantwoord waarom op bepaalde plekken en tijden wel wordt opgenomen en wanneer niet. Bij reguliere OVC op de voet van artikel 126l Sv is het namelijk gemeengoed om *alle* onderschepte communicatie, dat wil zeggen: zonder onderbreking, op te nemen zodat geen discussie kan ontstaan over het ontbreken van communicatie die (eventueel) ontlastend is voor de verdachte.[474] In de strafzaak zouden hierover vragen kunnen rijzen.

Constateringen bij het toezichtonderzoek

Zoals onder paragraaf 5.2 reeds is besproken, is op voorhand niet altijd duidelijk welke gegevens in het geautomatiseerd werk moeten worden gezocht en/of zullen worden gevonden. In het ene onderzoek zal in een geautomatiseerd werk meer gericht kunnen worden gezocht terwijl in het andere onderzoek een ruimere strekking van de in het bevel opgenomen onderzoekshandelingen nodig is, zonder dat het bevel ex artikel 126nba Sv als disproportioneel kan worden aangemerkt.
In één zaak bleek uit de stukken dat het doel van de inzet met name het meekijken met het videobellen van de verdachte betrof. Tijdens de inzet zijn echter voornamelijk andere gegevens, waaronder e-mails, veiliggesteld. Het onderscheppen van de videobelgesprekken bleek (kennelijk) complexer. Dit kan op het eerste gezicht vragen oproepen over de proportionaliteit van de inzet. Tegelijkertijd blijkt uit het dossier dat de uitgevoerde onderzoekshandelingen zowel door de machtiging van de rechter-commissaris als het bevel van de officier van justitie waren gedekt. Met andere woorden: de reikwijdte van de in de machtiging en het bevel opgenomen onderzoekshandelingen was ruimer dan die waartoe de motivering c.q. het doel van de inzet aanleiding gaf. Op grond hiervan kan dus niet worden vastgesteld dat de inzet daarmee een onnodig breed bereik had. Tegelijkertijd blijkt uit de CTC-stukken dat het technisch niet mogelijk was te differentiëren tussen bijvoorbeeld

[474] In de toelichting op de Regeling opnemen vertrouwelijke communicatie politie, *Stcrt.* 2000, 7, p. 10, is hierover opgemerkt: "*Dit betekent dat de grootst mogelijke zorgvuldigheid bij de inzet van dit middel zal moeten worden betracht, hetgeen onder andere tot uitdrukking komt in de verplichting alle te onderscheppen communicatie vast te leggen.*"

gegevens uit Whatsapp, videobellen en e-mail. De CTC achtte deze 'bijvangst', hoewel het onderzoek primair gericht was op het videobellen, in haar advies gelegitimeerd.
Een andere zaak met een groot bereik van het onderzoek in een geautomatiseerd werk betrof de onschadelijkmaking van een internationaal botnet (onderzoeksdoel e van artikel 126nba lid 1 Sv). Gelet op het feit dat het betreffende botnet zich over de hele wereld uitstrekte, had ook de inzet van de bevoegdheid een (potentieel) grote reikwijdte, omdat de onschadelijkmaking uiteindelijk effect had op een zeer groot aantal geautomatiseerde werken. Dat dit effect slechts de onschadelijkmaking betrof van het botnet in de betreffende geautomatiseerde werken (en dus niet het overnemen van gegevens daaruit) maakt dit niet anders. Op basis van bovenstaande vaststellingen kan evenwel niet worden geconcludeerd tot schending van rechtsregels op dit punt. Wel toont het aan dat de impact en reikwijdte van een inzet naar gelang van de aard van de zaak en de doelstelling van de inzet sterk kunnen verschillen.

Binnendringen in een geautomatiseerd werk vergt doorgaans voorbereiding en eventueel de toepassing van methoden die het binnendringen mogelijk maken of faciliteren, bijvoorbeeld doordat op een of andere wijze inloggegevens worden achterhaald waarmee vervolgens in een geautomatiseerd werk kan worden binnengedrongen of doordat een bug wordt geplaatst in een geautomatiseerd werk met behulp waarvan op een later moment (andermaal) wordt binnengedrongen. Er zijn aanzienlijk meer van dergelijke gevallen denkbaar, maar die worden omwille van de afscherming van methodieken hier niet uiteengezet.
In het toezichtonderzoek is meermalen aandacht besteed aan de vraag wat de wettelijke grondslag kan zijn voor het toepassen van dergelijke voorbereidende c.q. faciliterende methoden door de politie. Is dat bijvoorbeeld artikel 3 Politiewet, een andere bijzondere opsporingsbevoegdheid (BOB) dan die van artikel 126nba/uba/zpa Sv, dan wel uitsluitend artikel 126nba/uba/zpa Sv?
De digit-officier heeft in dit verband meegedeeld dat hij het uitgangspunt hanteert dat de politie in het kader van het binnendringen handelingen mag verrichten die een geringe inbreuk op de privacy met zich brengen en/of niet zeer risicovol zijn voor de beheersbaarheid en de integriteit van de opsporing. Het gehanteerde kader is weliswaar vergelijkbaar met de heersende leer omtrent artikel 3 Politiewet, maar vormt naar oordeel van de digit-officier niet de grondslag voor het binnendringen. Die grondslag is het bevel ex artikel 126nba Sv. Indien binnendringhandelingen een meer dan geringe inbreuk op de privacy met zich brengen of zeer risicovol zijn voor de beheersbaarheid en integriteit van de opsporing, is een (aanvullend) bevel of vordering nodig die die handeling mede dekt. De grondslagen voor het binnendringen zijn dan het bevel ex artikel 126nba Sv gecombineerd met de aanvullende BOB-bevoegdheid. Tegelijkertijd heeft LP Digit in gesprek met de onderzoekers uiteengezet dat (aanvankelijk) is gekeken naar voorbereidende methodieken die kunnen worden gebaseerd op artikel 3 Politiewet en niet noodzakelijkerwijs worden gedekt door een bevel ex artikel 126nba Sv. Het is echter inmiddels huidige praktijk dat ook die methoden worden gedekt door een bevel ex artikel 126nba Sv.
De Inspectie heeft geconstateerd dat Digit methodieken waarvan de vraag is of zij zijn voorzien van een wettelijke basis, voorafgaand aan de toepassing ervan overeenkomstig de richtsnoeren van LP Digit voor instemming en ter toetsing voorlegt aan de digit-officier.
Bij het toezichtonderzoek is geconstateerd dat in bepaalde gevallen voorbereidende c.q. faciliterende methodieken, als hier bedoeld, zijn toegepast die louter waren gegrond op artikel 3 Politiewet. Het toezichtonderzoek wijst uit dat toetsing door de digit-officier plaatsvindt aan de hand van criteria die in overeenstemming zijn met de wet en de heersende jurisprudentie van de Hoge Raad dienaangaande. Binnen het bestek van het uitgevoerde dossieronderzoek geeft de uitkomst van deze toetsingen de onderzoekers geen reden voor commentaar.

5.4. Het technisch hulpmiddel en de keuring ervan

Uitgangspunt

In het normatieve kader dat in hoofdstuk 3 is omschreven wordt primair tot uitgangspunt genomen dat het door de officier van justitie bevolen onderzoek in een geautomatiseerd werk op een zodanige wijze wordt uitgevoerd en/of zodanig is omgeven met waarborgen dat de betrouwbaarheid, de integriteit en de herleidbaarheid van de bij dit onderzoek verkregen gegevens is gegarandeerd. Die gegevens kunnen immers dienen tot het bewijs van het strafbare feit ter zake waarvan een verdenking is gerezen. Daarnaast had de minister oog voor het belang van afscherming van gevoelige methodieken en geavanceerde technologieën die bij het binnendringen en/of het verrichten van onderzoekshandelingen worden toegepast.

Het verrichten van onderzoekshandelingen in een geautomatiseerd werk met de onderzoeksdoeleinden die in het bevel van de officier van justitie zijn opgenomen, kan weliswaar ook ad hoc en handmatig worden uitgevoerd, maar vindt bij voorkeur plaats met behulp van een technisch hulpmiddel dat voldoet aan de eisen van artikel 8 tot en met 13 Bogw. Uitgangspunt is dat dit technisch hulpmiddel voorafgaand aan het gebruik ervan wordt goedgekeurd. Bij de keuring gaat de aangewezen keuringsinstantie na of het technisch hulpmiddel voldoet aan de eisen van artikel 8 tot en met 13 Bogw, zodat – onder meer – kan worden uitgegaan van de betrouwbaarheid, integriteit en herleidbaarheid van de daarmee veiliggestelde gegevens. Bij goedkeuring wordt in het proces-verbaal van de inzet verwezen naar het keuringsnummer, waardoor de samenstelling van het hulpmiddel kan worden afgeschermd met het oog op de bescherming van opsporingsbelangen.
Indien het technisch hulpmiddel vooraf noch achteraf is goedgekeurd,[475] of indien voor het verrichten van onderzoekshandelingen geen gebruik wordt gemaakt van een technisch hulpmiddel, zullen maatregelen moeten worden getroffen die de betrouwbaarheid, de integriteit en de herleidbaarheid van de bij het onderzoek verkregen gegevens garanderen.

De uitvoeringspraktijk

De uitvoeringspraktijk van artikel 126nba Sv staat op gespannen voet met het hiervoor beschreven uitgangspunt dat bij het verrichten van onderzoekshandelingen in beginsel gebruik wordt gemaakt van een vooraf goedgekeurd technisch hulpmiddel. In haar verslag van juli 2020 stelde de Inspectie om die reden vast dat "*in 2019 niet is tegemoetgekomen aan het uitgangspunt dat in diverse parlementaire stukken is beschreven.*"[476] De Inspectie

[475] Art. 21 Bogw brengt de in de hoofdtekst weergeven uitgangspunten niet altijd even gelukkig onder woorden. Lid 3 daarvan luidt als volgt: "*Indien ter uitvoering van een bevel gebruik wordt gemaakt van een niet gekeurd technisch hulpmiddel vermeldt de officier van justitie de uitkomst van de keuring of herkeuring na afloop van het gebruik in de processtukken.*" In aanvulling hierop kan uit art. 15 lid 1 Bogw worden afgeleid dat indien ter uitvoering van een bevel gebruik wordt gemaakt van een niet-vooraf-goedgekeurd technisch hulpmiddel de officier van justitie gehouden is het technisch hulpmiddel na afloop van het gebruik ter keuring of herkeuring aan te bieden, behoudens indien de aard van het technische hulpmiddel zich naar het oordeel van de officier van justitie daartegen verzet. Zie over deze verplichting paragraaf 3.8 hierboven, onder het kopje 'Uitzondering op de hoofdregel (1): keuring achteraf'. Zoals aldaar opgemerkt bepaalt art. 21 Bogw echter *niet* met zoveel woorden dat indien het technisch hulpmiddel na afloop wordt *af*gekeurd, (alsnog) waarborgen worden getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de met het technisch hulpmiddel vastgelegde gegevens te garanderen. Dat komt voor als een leemte in de regeling. Ook na afloop van de toepassing van een technisch hulpmiddel bestaat immers nog de mogelijkheid om dergelijke waarborgen te treffen. Aangezien de eis om dergelijke waarborgen te treffen onmiskenbaar onderdeel is van het beschermingsbelang van art. 21 Bogw, is er in dit rapport voor gekozen om in de hoofdtekst tot uitdrukking te brengen dat dergelijke waarborgen moeten worden getroffen in alle gevallen waarin geen gebruik wordt gemaakt van een goedgekeurd technisch hulpmiddel of waarin het verrichten van onderzoekshandelingen in een geautomatiseerd werk plaatsvindt zonder een technisch hulpmiddel (d.w.z. handmatig). Er zijn in het toezichtonderzoek overigens geen aanwijzingen gevonden dat het OM van deze leemte in art. 21 Bogw gebruikmaakt om het treffen van waarborgen te omzeilen. In twee zaken is het technisch hulpmiddel na gebruik afgekeurd, maar die zaken hebben niet tot een vervolging geleid.

[476] Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2019*, Den Haag: Ministerie van Justitie en Veiligheid 2020, p. 8-9.

heeft de PG-HR hiervan op de hoogte gesteld. De Inspectie schetst in haar verslagen over 2020 en 2021 een vergelijkbaar beeld.[477]

In de semigestructureerde interviews met de digit-officier en de digit-parketsecretaris is meermalen op dit onderwerp ingegaan. De digit-officier bracht daarin kort gezegd het volgende naar voren:

- Zonder voorbehoud onderschrijft de digit-officier het primaire uitgangspunt dat de betrouwbaarheid, integriteit en herleidbaarheid van de gegevens die zijn verkregen bij het onderzoek in een geautomatiseerd werk worden gewaarborgd.
- In die gevallen waarin het bevel inhield dat de onderzoekshandelingen in het geautomatiseerde werk handmatig worden verricht, is geen gebruik gemaakt van een technisch hulpmiddel. Het voor één geval door Digit geschreven script voldeed niet aan de definitie van 'technisch hulpmiddel'.
- De digit-officier beklemtoont dat in alle gevallen is voldaan aan de voorschriften van artikel 21 Bogw.
- In die gevallen waarin het toegepaste technisch hulpmiddel niet ter keuring is aangeboden heeft de digit-officier geoordeeld dat de aard van het technisch hulpmiddel zich tegen keuring verzet.
- De digit-officier heeft erop toegezien dat in (vrijwel) alle gevallen voor zover nodig procedurele c.q. aanvullende waarborgen werden gesteld.

Hieronder zal separaat bij verschillende uitgangspunten worden stilgestaan en zal worden beoordeeld hoe de uitvoeringspraktijk zich verhoudt tot de uitgangspunten.

Technisch hulpmiddel versus handmatig onderzoek

In paragraaf 3.8 hierboven is stilgestaan bij de definitie van het begrip 'technisch hulpmiddel'. Dat betreft volgens artikel 1 onder f Bogw een "*softwareapplicatie die gegevens detecteert, registreert en transporteert en waarmee onderzoekshandelingen worden verricht ter uitvoering van een bevel.*"
Deze definitie van 'technisch hulpmiddel' laat ruimte voor verschillende interpretaties.[478] De eerste en de opvolgende digit-officieren hebben in dit verband melding gemaakt van het door hen gehanteerde criterium van de 'directe betrokkenheid' van een lid van het technische team (Digit) bij het verrichten van onderzoekshandelingen in een geautomatiseerd werk. 'Directe betrokkenheid', als door hen bedoeld, doet zich voor wanneer de (handmatige) verrichtingen van de technische opsporingsambtenaar in de plaats komen van één of meer van de drie kenmerken van een technisch hulpmiddel, te weten dat het functionaliteiten bevat voor het *automatisch* (1) detecteren, (2) registreren en (3) transporteren van gegevens. Indien in een van die fasen directe betrokkenheid van Digit is vereist en het proces (dus) niet volledig automatisch kan plaatsvinden door een functionaliteit van de applicatie, beschouwt de digit-officier het onderzoek in een geautomatiseerd werk als handmatig verricht.

Niettemin wijst de uitvoeringspraktijk uit dat de veelvuldig door Digit gebruikte applicatie die in dit rapport de codenaam 'TH Brons' heeft gekregen (waarover hieronder meer) niet in volle omvang aan deze definitie voldoet. Het transport van de veiliggestelde gegevens naar de technische infrastructuur vindt in het geval van TH Brons namelijk niet geautomatiseerd

---

[477] Zie Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2020*, Den Haag: Ministerie van Justitie en Veiligheid 2021, p. 14, en Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2021*, Den Haag: Ministerie van Justitie en Veiligheid 2022, p. 20.

[478] Dit brengt ook mee dat de vermelding in deze rapportage van aantallen zaken waarin een technisch hulpmiddel al dan niet is ingezet aanleiding kan geven tot discussie. Bovendien kunnen in één zaak meer technische hulpmiddelen worden ingezet en is (binnen één zaak) ook een combinatie mogelijk van het handmatig verrichten van onderzoekshandelingen in een geautomatiseerd werk, en van het verrichten van onderzoekshandelingen met behulp van een technisch hulpmiddel in een ander geautomatiseerd werk, etc.

plaats, maar handmatig. De digit-officier merkt TH Brons evenwel (onverminderd) aan als technisch hulpmiddel, omdat TH Brons naar zijn zeggen wel degelijk de mogelijkheid in zich bergt om volautomatisch te functioneren maar er bewust voor gekozen is om één van de fasen (het transport) handmatig te laten plaatsvinden. Omdat dit een bewuste ingreep is, beschouwt de digit-officier TH Brons als technisch hulpmiddel. Daar valt echter tegen in te brengen dat TH Brons niet in verbinding staat met de technische infrastructuur van de politie, en dat in de huidige configuratie TH Brons niet in staat is om de gegevens automatisch naar de technische infrastructuur te transporteren.[479]

In een ander geval was de Inspectie van oordeel dat een door Digit zelf geschreven script – anders dan de digit-officier – wel voldeed aan de definitie die het Bogw geeft van het begrip 'technisch hulpmiddel'. Het verslag over 2019 bevat hierover de volgende passage:

> *"In 2019 heeft de officier van justitie in twee zaken bevolen dat het verrichten van onderzoekshandelingen in een geautomatiseerd werk plaatsvindt zonder een technisch hulpmiddel, dus handmatig. In een van deze zaken heeft de politie een zelf ontwikkeld script ingezet. Gelet op de functionaliteit van het script is de Inspectie van mening dat dit script valt onder de definitie van een technisch hulpmiddel. Zowel in haar haalbaarheidsonderzoek als in haar plannen van aanpak beschouwt de politie de hiermee verrichte onderzoekshandelingen echter als handmatig. Hieruit blijkt dat een verschil van inzicht over de interpretatie van deze definitie bestaat."*[480]

Wat van dit alles ook zij, in het tussenrapport van de PG-HR is hieromtrent opgemerkt dat voorlopig kan worden geconcludeerd dat het begrip 'technisch hulpmiddel' voor meerderlei uitleg vatbaar is en dat het Bogw mede als gevolg daarvan niet heel nauwkeurig afbakent welke waarborgen zijn verbonden aan het gebruik van softwareapplicaties voor het verrichten van onderzoekshandelingen in een geautomatiseerd werk, en door wie en op welk moment die waarborgen moeten worden getroffen.
Het vervolgonderzoek heeft de onderzoekers geen andere inzichten opgeleverd. In de uitvoeringspraktijk is gebleken dat de definitie van 'technisch hulpmiddel' aan dat begrip onvoldoende richting geeft en dat deze definitie zodoende – afhankelijk van de omstandigheden van het geval – ruimte laat voor uiteenlopende antwoorden op de vraag of de softwareapplicatie die (eventueel) wordt aangewend voor het verrichten van onderzoek in een geautomatiseerd werk als een technisch hulpmiddel moet worden aangemerkt. De nadere omschrijving die de digit-officier aan het begrip 'technisch hulpmiddel' heeft gegeven betreft een betrekkelijk streng criterium dat, hoewel verdedigbaar, in elk geval (nog immer) tot discussie aanleiding kan geven.

---

[479] Deze mededeling neemt tot uitgangspunt dat de technische infrastructuur van Digit bestaat uit een server die niet is verbonden met het systeem waarvan TH Brons onderdeel is. Die aanname is echter voor discussie vatbaar. De Inspectie stelde namelijk vast dat (ook) *in* het systeem waarvan TH Brons deel uitmaakt gegevens worden vastgelegd die kunnen dienen als bewijs in een strafzaak. Het Bogw schrijft voor dat dergelijke gegevens worden vastgelegd op een 'technische infrastructuur' en het Bogw formuleert eisen waaraan een dergelijke technische infrastructuur moet voldoen. Digit heeft in 2020 echter nog geen antwoord gegeven op de vraag of de componenten van het systeem van TH Brons waarop vastlegging van gegevens plaatsvindt onderdeel vormen van de door het Bogw bedoelde technische infrastructuur. Bij vastlegging van gegevens op een technische infrastructuur is onder meer voorgeschreven dat de logische toegang beperkt wordt en dat bij een selectie van gegevens gebruik wordt gemaakt van een forensische kopie. Bij de inzet en het gebruik van dit technisch hulpmiddel zijn dergelijke maatregelen in 2020 door Digit niet getroffen, aldus de Inspectie. Zie Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2020*, Den Haag: Inspectie Justitie en Veiligheid 2021, p. 15. Zie ook Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2021*, Den Haag: Inspectie Justitie en Veiligheid 2022, p. 30, waar de Inspectie constateert dat Digit een aanvang gemaakt heeft met het bepalen en vastleggen van de reikwijdte van de technische infrastructuur, maar dat dit proces in 2021 nog niet was afgerond.

[480] Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2019*, Den Haag: Ministerie van Justitie en Veiligheid 2020, p. 17-18.

Naar het oordeel van de onderzoekers valt het aan te bevelen dat als technisch hulpmiddel wordt aangemerkt: iedere applicatie waarmee wordt beoogd in een geautomatiseerd werk onderzoekshandelingen te verrichten en die qua complexiteit verder reikt dan een eenvoudig script waarvan de werking op zichzelf niet hoeft te worden afgeschermd. In dat geval komt routinematig de vraag op of de applicatie zich leent voor (aan het gebruik voorafgaande) keuring en kan daarnaar worden gehandeld. Wanneer daarentegen hogere eisen worden gesteld aan een applicatie wil het als technisch hulpmiddel kunnen worden aangemerkt (zoals de digit-officier propageert), dan heeft dit tot gevolg dat de beoordeling van de keuringsvatbaarheid ervan achterwege blijft, ook in die gevallen waarin er geen overwegende bezwaren bestaan tegen keuring (vooraf dan wel achteraf). De meer functionele uitleg van het begrip 'technisch hulpmiddel' die de onderzoekers voorstellen, heeft als voordeel dat *iedere* applicatie in principe ter keuring kan (moet) worden aangeboden, behoudens indien het gaat om een eenvoudig script (waarvan de werking niet hoeft te worden afgeschermd). De goedkeuring van applicaties vergemakkelijkt de afscherming ervan. De goedkeuring garandeert bovendien de betrouwbaarheid, integriteit en herleidbaarheid van de gegevens die zijn verkregen bij het onderzoek in een geautomatiseerd werk. Het belang van een meer formele omschrijving van het begrip 'technisch hulpmiddel' komt daarmee te vervallen.
Het voorgaande laat onverlet dat in alle gevallen waarin geen gebruik is gemaakt van een (vooraf of achteraf) goedgekeurd technisch hulpmiddel (aanvullende c.q. procedurele) waarborgen zullen moeten worden getroffen met het oog op de betrouwbaarheid, integriteit en herleidbaarheid van de gegevens die zijn verkregen bij het onderzoek in een geautomatiseerd werk. Daarop wordt hieronder teruggekomen.

De aantallen: (goedgekeurd) technisch hulpmiddel versus handmatig

Op basis van informatie van de Inspectie en van het OM kan over de jaren 2019, 2020 en 2021 worden uitgegaan van de volgende aantallen zaken waarin (eerste) bevelen tot het verrichten van onderzoekshandelingen in een geautomatiseerd werk zijn afgegeven.[481]

	Totaal zaken	Handmatig	Technisch hulpmiddel
2019	8	4	5
2020	12	3	10
2021	24	4	21
totaal	**44**	**11**	**36**

[481] Toelichting op het schema. Jaartal betreft het jaar waarin in de betreffende zaak het *eerste* bevel aan Digit is afgegeven. Het is mogelijk dat in één zaak zowel een bevel tot handmatig onderzoek als een bevel tot het verrichten van onderzoek met behulp van een technisch hulpmiddel is afgegeven. In dat geval komt die zaak terug onder zowel de kolom 'handmatig' als de kolom 'technisch hulpmiddel'. Op één complexe zaak na, is iedere zaak in het totaal aantal zaken slechts eenmaal meegeteld.
Niet meegeteld zijn: (1) zaken waarin onderzoek in een geautomatiseerd werk is uitgevoerd in een ander land en onder gezag van de justitiële autoriteiten van dat andere land, (2) zaken waarin via een rechtshulpverzoek aan een ander land om onderzoek in een geautomatiseerd werk in dat land is gevraagd, dan wel de resultaten van dergelijk onderzoek zijn verkregen, (3) zaken waarin een ander land middels een rechtshulpverzoek om onderzoek in een geautomatiseerd werk heeft verzocht. Opmerking verdient dat de wijze van tellen van aantallen zaken kan verschillen met de wijze waarop de telling heeft plaatsgehad in de verschillende verslagen van de Inspectie Justitie en Veiligheid. De cijfers zijn dan ook vooral ter indicatie bedoeld.

Hieronder volgen in onderstaande tabel de aantallen omtrent bevelen tot de inzet van een al dan niet vooraf of achteraf (goed)gekeurd technische hulpmiddel.[482]

	2019	2020	2021
Vooraf goedgekeurd	0	0	2
Achteraf goedgekeurd	0	0	1
Niet vooraf gekeurd, achteraf niet-goedgekeurd	2	0	0
Niet ter keuring aangeboden (art. 21 lid 4)	3	10	20

Het voorgaande schema laat zien dat in slechts een gering aantal zaken gebruik is gemaakt van een (vooraf) goedgekeurd technisch hulpmiddel. Dit heeft tot gevolg dat in alle resterende zaken waarin Digit uitvoering heeft gegeven aan een bevel ex artikel 126nba Sv procedurele c.q. aanvullende waarborgen moesten worden getroffen, terwijl de afscherming van het technisch hulpmiddel niet kon plaatsvinden door in het proces-verbaal van inzet te verwijzen naar het keuringsnummer.

Digit heeft in totaal vier technische hulpmiddelen zelf ontwikkeld. Eén daarvan is er in de onderzochte periode afgekeurd maar in geen zaak ingezet. Eén technisch hulpmiddel is na een eerdere afkeuring goedgekeurd, doch in de onderzochte periode niet in een zaak ingezet. Twee technische hulpmiddelen zijn uiteindelijk goedgekeurd en in één of meer zaken ingezet.

TH Brons en de keuring ervan

In 33 zaken, te weten drie in 2019, tien in 2020 en twintig in 2021, betreffen één of meer bevelen ex artikel 126nba Sv de inzet van verschillende (software)versies van een niet nader genoemd, commercieel verkregen technisch hulpmiddel dat in het toezichtonderzoek de codenaam 'TH Brons' heeft gekregen.
TH Brons vormt – volgens informatie van de digit-officier – een geïntegreerd onderdeel van een complex systeem van hardware- en softwarecomponenten, waarin functionaliteiten voor het binnendringen onlosmakelijk zijn verbonden aan functionaliteiten voor het detecteren, registreren en transporteren van gegevens die kunnen worden verkregen uit de geautomatiseerde werken van het type waarvoor het systeem is ontwikkeld.
TH Brons is op de voet van artikel 21 lid 4 Bogw niet ter keuring aangeboden omdat de aard van dit technisch hulpmiddel zich naar het oordeel van de digit-officier daartegen verzet. Voor TH Brons is volgens de digit-officier op dit moment geen alternatief voorhanden dat naar zijn aard wel geschikt is voor keuring.
Tot het oordeel dat de aard van dit technisch hulpmiddel zich verzet tegen keuring, vooraf en achteraf, is de digit-officier gekomen na overleg met onder meer verscheidene rechercheofficieren en na een bespreking van de problematiek met een zogeheten 'reflectiekamer' van het OM.[483]

---

[482] Toelichting op het schema:
vooraf goedgekeurd: aantal zaken waarin in het genoemde jaar een bevel is gegeven tot inzet van een technisch hulpmiddel dat op het moment van inzet was goedgekeurd;
achteraf goedgekeurd: aantal zaken waarin in het genoemde jaar een bevel is gegeven tot inzet van een technisch hulpmiddel dat op enig moment na de inzet is goedgekeurd;
niet vooraf gekeurd, achteraf niet-goedgekeurd: aantal zaken waarin in het genoemde jaar een bevel is gegeven tot inzet van een technisch hulpmiddel dat op enig moment wél ter keuring is aangeboden, maar dat tot op heden nog niet tot goedkeuring heeft geleid;
niet ter keuring aangeboden: aantal zaken waarin in het genoemde jaar een bevel is gegeven tot inzet van een technisch hulpmiddel dat naar het oordeel van de digit-OvJ naar zijn aard niet voor keuring geschikt is (conform artikel 21 lid 4 Bogw).

[483] Een 'reflectiekamer' wordt binnen het OM gevormd door een kring daartoe aangewezen (voornamelijk) ervaren OM'ers, met wie een lid van het OM ten behoeve van de besluitvorming in een zaak kan reflecteren over problemen van juridisch-ethische aard.

In de interviews heeft de digit-officier zijn oordeel dat TH Brons naar zijn aard ongeschikt is voor keuring kortweg als volgt toegelicht. Het is technisch niet mogelijk om het systeem waarvan TH Brons een geïntegreerd onderdeel is te laten functioneren als het niet volledig geüpdatet is. De softwarecomponenten die zijn geïnstalleerd in het systeem worden door de leverancier met een frequentie van gemiddeld ongeveer eenmaal per week aangepast en geüpdatet, zonder dat vooraf bekend is wanneer die aanpassingen en updates plaatsvinden. De gemiddelde duur van een keuringsproces bedraagt daarentegen (aanzienlijk) meer dan een maand. Het is niet mogelijk om bij een keuring achteraf de softwareversie na te bootsen die geïnstalleerd was ten tijde van de inzet van TH Brons. Hetzelfde geldt bij een eventuele voorafgaande keuring: de softwareversie die ten tijde van de inzet zal worden gebruikt, zal om de hiervoor genoemde redenen niet identiek zijn aan de gekeurde versie.
De hiervoor beschreven kenmerken van TH Brons zijn onveranderlijk. Digit is slechts één van meer afnemers van het systeem en de leverancier is niet bereid het systeem terug te zetten naar een oudere versie en/of updates (tijdelijk) niet door te voeren. Er is slechts een keuze tussen het wel of niet gebruikmaken van TH Brons. Een soortgelijk systeem van gelijke kwaliteit en functionaliteiten is niet voorhanden, aldus de digit-officier.

Bij het toezichtonderzoek hebben de onderzoekers het volgende geconstateerd. In de eerste plaats laat zich thans aanzien dat de beschreven kenmerken van het technisch hulpmiddel een keuring niet toelaten, zulks vanwege het keuringsproces zoals dat volgens de huidige regelgeving is ingericht en het tijdsbestek dat met dit proces is gemoeid. Afgaande op de mededelingen van de digit-officier is er voor het systeem momenteel geen alternatief voorhanden met functionaliteiten van een gelijk kwaliteitsniveau dat wel voor keuring in aanmerking komt. De afwegingen van de digit-officier omtrent de geschiktheid voor keuring van TH Brons komen plausibel voor.

Zaaksgerelateerde constateringen bij het toezichtonderzoek

Naar aanleiding van het door de onderzoekers uitgevoerde dossieronderzoek kunnen tot slot nog de volgende bijzonderheden worden geconstateerd omtrent de inzet van een technisch hulpmiddel.
In zeven van de onderzochte zaken is toepassing gegeven aan artikel 21 lid 2 Bogw, oftewel er zijn in die zaken een of meer bevelen afgegeven tot het gebruik van een niet-gekeurd technisch hulpmiddel. In één van die zaken is het gebruikte technisch hulpmiddel uiteindelijk ter keuring aangeboden en afgekeurd. In de overige zes zaken is gebruikgemaakt van TH Brons. In vier van de zaken waarin toepassing is gegeven aan artikel 21 lid 4 Bogw is de beslissing daartoe tijdens de inzage niet terug te vinden in het nba-dossier, noch in de processtukken. In twee van de zaken waarin toepassing is gegeven aan artikel 21 lid 4 Bogw is die beslissing wel terug te vinden in het nba-dossier. In deze zaken is een proces-verbaal van de digit-officier van justitie voorhanden waarin staat dat de officier van justitie van oordeel is dat het gebruikte technische hulpmiddel naar zijn aard niet te keuren is en dat om die reden is besloten de keuring achterwege te laten. Dit oordeel wordt in het proces-verbaal niet nader gemotiveerd.

In één zaak is geconstateerd dat een bevel is gegeven voor het verrichten van onderzoekshandelingen met behulp van een technisch hulpmiddel, terwijl bij het verrichten van onderzoekshandelingen geen gebruik is gemaakt van het in het bevel genoemde technische hulpmiddel, althans zo is de inzet door Digit in processen-verbaal verantwoord. Uit de stukken blijkt vervolgens niet of en, zo ja, welke procedurele waarborgen zijn getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de tijdens het onderzoek vastgelegde gegevens te garanderen, zoals artikel 21 lid 5 Bogw voorschrijft in geval van een handmatige inzet.

Uit het gesprek met de digit-officier en digit-parketsecretaris bleek dat het in deze zaak ging om een zogeheten 'tcpdump' met betrekking tot een router.[484]
De digit-officier en digit-parketsecretaris hebben te kennen gegeven dat het bevel (achteraf bezien) niet geheel correct is opgemaakt, omdat op voorhand niet meteen duidelijk was of de applicatie kon worden aangemerkt als een technisch hulpmiddel. Gedurende de inzet bleek dat dit niet het geval was omdat de detectie en registratie weliswaar op het geautomatiseerd werk plaatsvonden maar de verkregen gegevens (de 'dump') vervolgens handmatig op transport moest worden gezet om opgeslagen te worden op de technische infrastructuur van Digit. De digit-officier heeft te kennen gegeven dat deze zaak aanleiding is geweest om te reflecteren op de betekenis en het bereik van het begrip 'technisch hulpmiddel' en wat daaronder wel en niet valt. Het resultaat van die reflectie is hierboven aan de orde gekomen.

In één zaak was het blijkens een verzamelproces-verbaal van Digit op een bepaald moment niet meer mogelijk om verbinding te krijgen met het technisch hulpmiddel dat was geplaatst in het geautomatiseerde werk. Hierdoor is het niet mogelijk geweest het technisch hulpmiddel te verwijderen uit het geautomatiseerd werk. De opsporingsambtenaren van Digit hebben vastgesteld dat er na een bepaald moment geen gegevens meer naar de technische infrastructuur zijn getransporteerd. De niet of niet volledige verwijdering van het technisch hulpmiddel levert geen risico's op voor het functioneren van het geautomatiseerde werk, aldus het proces-verbaal van Digit. Deze handelwijze is conform het geldende rechtskader.

5.5. Het gebruik van commerciële software en van onbekende kwetsbaarheden

In de wetsgeschiedenis is stilgestaan bij de risico's die zijn verbonden aan de verwerving (van gebruiksrechten) en aan het daadwerkelijke gebruik van commerciële systemen voor het binnendringen in geautomatiseerde werken (ook wel *intrusion* software genoemd).[485] Niet uitgesloten is dat het aangeschafte commerciële systeem gebruikmaakt van onbekende kwetsbaarheden (zero-days) in wijdverbreide en veelgebruikte hardware of software. Door dergelijke systemen aan te schaffen wordt de markt voor zero-days gestimuleerd en wordt de doorontwikkeling van deze systemen aangemoedigd, met als gevolg dat de veiligheid van het internet erbij inschiet. Bovendien kunnen deze systemen niet alleen worden aangewend voor de bestrijding van criminaliteit. Net als andere wapens kunnen ook cyberwapens in handen komen van dubieuze regimes, die er journalisten, mensenrechtenactivisten en politieke tegenstanders mee (kunnen) bespioneren. Ten slotte bestaat de mogelijkheid dat het systeem onvoldoende bescherming biedt tegen oneigenlijk gebruik ervan door derden, waaronder de leverancier en/of de producent, omdat de werking van het systeem voor de afnemer niet inzichtelijk is.
Om die redenen heeft de minister een sterke voorkeur voor het gebruik van andere methoden voor het binnendringen in geautomatiseerde werken, zoals het gebruik van inloggegevens, van *social engineering*, en van bekende kwetsbaarheden, of de toepassing van binnendringapplicaties die in eigen beheer zijn ontwikkeld.

De uitvoeringspraktijk

De uitvoeringspraktijk van artikel 126nba Sv staat op gespannen voet met het hiervoor beschreven uitgangspunt, namelijk dat in beginsel geen gebruik wordt gemaakt van commerciële software waarvan onduidelijk is of die software onbekende kwetsbaarheden exploiteert. In haar verslag van 2021 stelde de Inspectie vast dat "*in 2020 in bijna alle*

[484] Een tcpdump betreft een softwarehulpmiddel voor de diagnose en analyse van computernetwerken. Daarmee kan het dataverkeer op een netwerk worden bekeken en geanalyseerd.
[485] Zie hierover paragraaf 3.7 onder de kopjes 'Het gebruik van commerciële software en van (onbekende) kwetsbaarheden bij het binnendringen' en 'Oneigenlijk gebruik door derden'.

zaken gebruik [is] gemaakt van commerciële software waarbij de leverancier toegang heeft zonder dat de politie dit kan beperken en controleren. De Inspectie concludeert dat hierdoor risico's niet kunnen worden uitgesloten voor wat betreft de betrouwbaarheid van met de hackbevoegdheid verkregen bewijs en de privacy van de betrokkenen."[486] De Inspectie schetst in haar verslag over 2021 een vergelijkbaar beeld.[487]

De door Digit gebruikte applicatie 'TH Brons' betreft niet alleen een technisch hulpmiddel waarmee onderzoekshandelingen worden verricht. Het is tevens onderdeel van een commercieel verkregen systeem dat functionaliteiten bevat voor het binnendringen in geautomatiseerde werken. Van dit systeem zijn op commerciële basis tijdelijke licenties aangeschaft, voor elke zaak waarin TH Brons is ingezet. Deze licenties zijn zeer kostbaar. Het aanschaffen van tijdelijke licenties is naar zeggen van de digit-officier (bij lange na) niet de goedkoopste manier waarop de gebruiksrechten van het systeem kunnen worden verworven.[488]
De digit-officier laat weten dat TH Brons zijn betrouwbaarheid meermalen heeft bewezen en dat het systeem om die reden niet voorafgaand aan iedere inzet in een zo representatief mogelijke testomgeving wordt gecontroleerd indien een soortgelijk geautomatiseerd werk reeds eerder is getest en deze testresultaten voldoende representatief worden geacht voor het nieuwe onderzoek.

De bezwaren die aan de aanschaf en het gebruik van commerciële binnendringsoftware zijn verbonden, zijn in paragraaf 3.7 hierboven besproken.[489] Die bezwaren zijn in dit geval meer concreet de volgende:

- *Gebrekkige transparantie*: De leverancier verschaft de digit-officier en Digit (slechts) tot op zekere hoogte inzage in de werking van de binnendringsoftware van het systeem waarvan TH Brons onderdeel is, en (in meerdere mate) in de werking van TH Brons zelf. Deze inzage is niet volledig. Daarmee is TH Brons voor de digit-officier en Digit in bepaalde mate een zogeheten 'black box'. Dit belemmert de controle op de toepassing van het systeem en maakt het niet goed mogelijk om op basis van volledige bekendheid met de inrichting en de werking van het systeem uitspraken te doen over de betrouwbaarheid, integriteit en herleidbaarheid van de met TH Brons geregistreerde gegevens.
- *Toegang door de leverancier*: Digit kan de toegang van de leverancier tot het door Digit gebruikte exemplaar van TH Brons technisch niet beperken. De leverancier is (daardoor) in theorie in staat om ongecontroleerd kennis te nemen van de gegevens die met behulp van TH Brons worden vergaard (de bewijslogging). Daardoor valt oneigenlijk gebruik van deze gegevens technisch niet uit te sluiten.
- *Verbinding met de server van de leverancier*: Het systeem waarvan TH Brons onderdeel is staat in verbinding met de server van de leverancier.[490] Werkzaamheden die de leverancier uitvoert kunnen bovendien mogelijk zelfs tijdens de daadwerkelijke inzet invloed hebben

[486] Zie Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2020*, Den Haag: Ministerie van Justitie en Veiligheid 2021, p. 3.
[487] Zie Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2020*, Den Haag: Ministerie van Justitie en Veiligheid 2021, p. 3, en Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2021*, Den Haag: Ministerie van Justitie en Veiligheid 2022, p. 13 en 20.
[488] De Inspectie van Justitie en Veiligheid signaleert in haar rapport over 2021 overigens dat het licentiemodel zoals omschreven in paragraaf 3.7 de markt mogelijk een extra stimulans geeft, zie Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2021*, Den Haag: Ministerie van Justitie en Veiligheid 2022, p. 14.
[489] Zie hierover ook Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2020*, Den Haag: Inspectie Justitie en Veiligheid 2021, p. 13-15 en p. 20.
[490] Vgl. naast bevestiging afkomstig van de digit-officier ook Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2021*, Den Haag: Inspectie Justitie en Veiligheid 2022, p. 19.

op de werking en functionaliteiten van TH Brons.[491]

- *Opslag van gegevens in TH Brons*: De door TH Brons geregistreerde gegevens worden – niet permanent, maar wel enige tijd – opgeslagen op een locatie in TH Brons die geen onderdeel is van de 'technische infrastructuur' van Digit waarop – in overeenstemming met het Bogw – de beveiligde opslag van deze gegevens dient plaats te vinden.[492] De leverancier verricht (met toestemming) onderhoudswerkzaamheden op deze servers. Als gevolg daarvan is onbevoegde toegang tot en oneigenlijk gebruik van de gegevens technisch niet uit te sluiten.[493]
- *Mogelijk gebruik zero-days*: Niet kan worden uitgesloten dat het systeem waarvan TH Brons onderdeel is het geautomatiseerde werk binnendringt door de exploitatie van onbekende kwetsbaarheden in (software die is geïnstalleerd op) het betreffende geautomatiseerde werk. Van de eventueel door het systeem benutte onbekende kwetsbaarheden is de digit-officier, noch Digit op de hoogte.
- *Levering aan dubieuze regimes*: Niet uitgesloten is dat het systeem waarvan TH Brons onderdeel is ook wordt geleverd aan (politie- of inlichtingendiensten of vervolgingsinstanties van) landen die zich schuldig maken aan ernstige schendingen van mensenrechten of internationaal humanitair recht.

De digit-officier heeft hierover het volgende opgemerkt.
Wat betreft de toegang van de leverancier tot het door Digit gebruikte exemplaar van TH Brons heeft de digit-officier erop gewezen dat slechts een select aantal gespecialiseerde medewerkers van de leverancier toegang heeft tot het systeem dat bij Digit in gebruik is en dat het de leverancier contractueel verboden is om oneigenlijk gebruik te maken van de bij toepassing van TH Brons verkregen gegevens. De digit-officier is hierop naar eigen zeggen alert. De digit-officier heeft geen aanwijzingen dat de leverancier zijn contractuele verplichtingen in dit verband niet nakomt, en hij acht het (ook) vanuit commercieel oogpunt onwaarschijnlijk dat de leverancier overgaat tot oneigenlijk gebruik van de door middel van TH Brons verkregen gegevens. Daarnaast heeft het OM in een reactie op het conceptrapport laten weten dat Digit inmiddels de toegang van de leverancier tot het technisch hulpmiddel monitort. Digit controleert of deze toegang overeenstemt met de verzoeken die de leverancier doet om onderhoud te mogen verrichten.
Wat betreft de verbinding met de server van de leverancier merkt het OM op dat de leverancier van TH Brons alleen werkzaamheden verricht nadat daarvoor vooraf door Digit toestemming is gegeven en dat tot op heden niet is gebleken dat onderhoud invloed heeft gehad op de herleidbaarheid, betrouwbaarheid en integriteit van vergaarde gegevens.
Wat betreft de opslag van gegevens op de TH merkt het OM in een reactie op het concept van dit rapport op het bij gebruik van technisch hulpmiddelen onvermijdelijk is dat de daarmee geregistreerde gegevens tijdelijk op een lokale component van dat technische hulpmiddel worden opgeslagen.
Wat betreft het mogelijke gebruik van zero-days wijst het OM er in zijn reactie op het conceptrapport op dat in de wetsgeschiedenis expliciete overwegingen zijn gewijd aan het mogelijke gebruik van onbekende kwetsbaarheden in commerciële producten, en dat in die overwegingen is onderkend dat de eventuele aanwezigheid van dergelijke kwetsbaarheden voor politie en het OM veelal niet bekend zal zijn (vgl. bijvoorbeeld *Kamerstukken I* 2016/17,

---

[491] Zie Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2021*, Den Haag: Inspectie Justitie en Veiligheid 2022, p. 23: "*De leverancier van het technisch hulpmiddel heeft de servers die de politie hiervoor gebruikt in technisch beheer en kan hier op afstand op inloggen om beheer- en supportwerkzaamheden uit te voeren. Werkzaamheden die de leverancier uitvoert, kunnen, mogelijk zelfs tijdens uitvoering van een bevel, gevolgen hebben voor de werking en functionaliteit van het technisch hulpmiddel. De Inspectie merkt hierbij op dat deze wijze van toegang door de leverancier gebruikelijk is in de markt voor deze commerciële software.*"

[492] Naar mededeling van het OM worden de met het technisch hulpmiddel vergaarde gegevens éénmaal per etmaal opgeslagen op de technische infrastructuur van Digit.

[493] Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2021*, Den Haag: Inspectie Justitie en Veiligheid 2022, p. 30-31.

34 372, D (MvA I), p. 21). De wetgever heeft (niettemin) de mogelijkheid geboden tot gebruik van commerciële binnendringsoftware.
Wat betreft de mogelijkheid dat de producent van TH Brons tevens levert aan dubieuze regimes heeft de digit-officier meegedeeld dat de AIVD na screening geen bezwaar heeft afgegeven omtrent de producent van TH Brons.[494]
De inzet van TH Brons is in 2019 besproken met rechercheofficieren en is voorgelegd aan een reflectiekamer, aldus de digit-officier. De genoemde risico's en bezwaren zijn afgewogen tegen het belang van de bestrijding van ernstige criminaliteit, aldus de digit-officier.

Bij het toezichtonderzoek hebben de onderzoekers geconstateerd dat Digit bij de uitvoering van het bevel ex artikel 126nba Sv structureel gebruikmaakt van een commerciële binnendringapplicatie, te weten (verschillende softwareversies) van het systeem waarvan TH Brons onderdeel is. De daaraan verbonden risico's en bezwaren kunnen, voor zover technisch al mogelijk, niet uitgesloten worden.[495] De onderzoekers onderschrijven in dit verband ook het oordeel van de Inspectie Justitie en Veiligheid[496] dat geen hoge verwachtingen mogen worden gekoesterd van de door de minister omschreven toets op de vraag of het product TH Brons wordt geleverd aan dubieuze regimes.[497] De AIVD-screening waarop de digit-officier heeft gewezen, heeft inderdaad plaatsgehad, doch voor zover tijdens de onderzoeksperiode is geconstateerd, slechts eenmalig, te weten in 2019. Hoewel uit de beantwoording van Kamervragen blijkt dat de politietoets inmiddels periodiek wordt herhaald,[498] blijft het enkele antwoord van de leverancier op de vraag of hij niet heeft geleverd aan landen waartegen vanuit de EU of de VN restrictieve sancties bestaan, zonder nadere informatie over het verkoopbeleid van de leverancier, nauwelijks te controleren.

---

494 Dat is conform een mededeling van de Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2020*, Den Haag: Inspectie Justitie en Veiligheid 2021, p. 13: "*Zoals vermeld in het Verslag van de Inspectie over 2019 is volgens de daartoe vastgestelde procedure screening van de betreffende leverancier bij de AIVD aangevraagd. In die procedure is opgenomen dat als de AIVD binnen vier weken geen bericht geeft, er vanuit gegaan wordt dat er geen nadelige gegevens zijn gevonden. De teamleiding van DIGIT heeft de Inspectie JenV aangegeven dat er geen bericht van de AIVD is ontvangen, waaruit afgeleid wordt dat er voor de AIVD geen belemmeringen bestaan voor deze leverancier.*"

495 Zie ook de constateringen van de Inspectie in haar verslag over 2020: "*De Inspectie stelt daarnaast vast dat dit technisch hulpmiddel aantoonbaar niet voldoet aan de technische eisen uit het Besluit. De leverancier van het technisch hulpmiddel heeft zelfstandig en op elk moment toegang tot het middel. De leverancier kan daarmee mogelijk ook toegang verkrijgen tot de bewijslogging die met dit middel is verkregen. Werkzaamheden die de leverancier uitvoert, kunnen, mogelijk zelfs tijdens uitvoering van een bevel, gevolgen hebben voor de werking en functionaliteit van het technisch hulpmiddel. De politie kan de toegang door de leverancier niet beperken en beschikt niet over mogelijkheden om controle uit te voeren van de toegang en uitgevoerde werkzaamheden door de leverancier. De Inspectie merkt hierbij op dat deze wijze van toegang door de leverancier gebruikelijk is in de markt voor deze commerciële software die mogelijk gebruik maakt van onbekende kwetsbaarheden. De politie stelt dat er geen alternatief voorhanden is dat dezelfde functionaliteit biedt zonder deze nadelen. Het betreffende middel is een 'black box' voor de politie, waarbij voor hen onbekend is wat er technisch precies gebeurt. Bepaalde functionaliteit kan niet worden uitgezet, waardoor het gebruik van dit middel zou kunnen conflicteren met de eis dat het technisch hulpmiddel uitsluitend gegevens ten behoeve van de in het bevel vermelde functionaliteit detecteert en registreert.*" Zie Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2020*, Den Haag: Inspectie Justitie en Veiligheid 2021, p. 15.

496 In het verslag over 2021 heeft de Inspectie opgemerkt: "*Zoals de Inspectie in haar verslagen over 2019 en 2020 heeft vermeld, is volgens de daartoe vastgestelde procedure, screening van de betreffende leverancier bij de AIVD aangevraagd en is de toets aangaande het niet leveren aan dubieuze regimes door de politie uitgevoerd door een verklaring hierover op te vragen bij de leverancier. Afgevraagd kan worden, wat de waarde is van een dergelijke eigen verklaring die niet inhoudelijk wordt getoetst. De Inspectie merkt tevens op dat wet- en regelgeving niet verplicht tot het periodiek doorlopen van het proces van de screeningsaanvraag en de toets of de leverancier niet levert aan dubieuze regimes. De screeningsaanvraag en toets hebben dan ook eenmalig al in 2019 plaatsgevonden.*" Zie Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2021*, Den Haag: Ministerie van Justitie en Veiligheid 2022, p. 13.

497 Zie voor de door de minister omschreven toets paragraaf 3.7.

498 Zie de brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties en de minister van Justitie en Veiligheid d.d. 23 juni 2022 in antwoord op Kamervragen van de leden Omtzigt en Van Dijk over het gebruik van hacksoftware, zoals Pegasus, in Nederland, *Aanhangsel Handelingen II* 2021/22, 3252, p. 6.

Tegenover de hierboven omschreven reeks van risico's en bezwaren staat dat de toepassing van TH Brons in de onderzochte zaken daadwerkelijk heeft geleid tot onderzoeksresultaten waartoe de inzet van TH Brons strekte. De afweging van de hierboven geschetste risico's en bezwaren enerzijds en het belang van de bestrijding van ernstige criminaliteit anderzijds, waarbij aan het tweede prioriteit is gegeven, is binnen het OM centraal en op zichzelf zorgvuldig tot stand gekomen. Het OM heeft het geldende rechtskader daarbij niet miskend.

Het structurele gebruik van commercieel verkregen binnendringapplicaties staat op gespannen voet met het hierboven verwoorde uitgangspunt van de minister. Niettemin is het gebruik van dergelijke binnendringsoftware op zichzelf verenigbaar met de geldende wettelijke voorschriften en kan niet worden geoordeeld dat dit gebruik als zodanig in strijd is met de beginselen van proportionaliteit, subsidiariteit en behoorlijkheid in individuele zaken. Het probleemveld is voor het overige politiek van aard, zodat hier met de signalering van het voorgaande wordt volstaan.

Uitstel melding onbekende kwetsbaarheden

De digit-officier heeft in de onderzochte periode eenmaal toepassing gegeven aan de procedure van artikel 126ffa Sv.[499]
Het gebruik van TH Brons heeft de digit-officier geen aanleiding gegeven voor toepassing van de procedure van artikel 126ffa Sv (uitstel melding onbekende kwetsbaarheid).[500]

5.6. De procedurele c.q. aanvullende waarborgen

Uitgangspunten

Indien de aard van het technische hulpmiddel zich naar het oordeel van de officier van justitie tegen keuring verzet, vermeldt de officier van justitie in de processtukken dat toepassing is gegeven aan artikel 21 lid 4 Bogw en vermeldt hij welke aanvullende waarborgen zijn getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de met het technisch hulpmiddel vastgelegde gegevens te garanderen, aldus schrijft deze bepaling voor.
In geval van een handmatige inzet vloeit uit artikel 21 lid 5 Bogw voort dat uit de processtukken blijkt of en, zo ja, welke procedurele waarborgen zijn getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de tijdens het onderzoek vastgelegde gegevens te garanderen.
Zoals in paragraaf 3.8 uiteengezet kunnen enerzijds de procedurele waarborgen en anderzijds de aanvullende waarborgen ondanks het verschil in terminologie in essentie dezelfde maatregelen betreffen en dienen zij in elk geval hetzelfde doel. Deze waarborgen, zowel de aanvullende als de procedurele, strekken er namelijk toe de betrouwbaarheid, integriteit en herleidbaarheid van de bij het onderzoek verzamelde gegevens te verzekeren.

Vraagpunten

Hierboven is opgemerkt dat in slechts een gering aantal van de zaken waarin Digit uitvoering heeft gegeven aan een bevel ex artikel 126nba Sv gebruik is gemaakt van een (vooraf) goedgekeurd technisch hulpmiddel. Om die reden moesten in veruit de meeste zaken waarborgen worden getroffen. De vraag rijst hoe daarin in de praktijk is voorzien en hoe dat is georganiseerd. Op gezag van welke officier van justitie zijn die waarborgen getroffen, als ze zijn getroffen? Het Bogw maakt wat dit betreft geen onderscheid tussen de digit-officier

[499] Zie de op 12 augustus 2021 gepubliceerde (ongedateerde) beschikking van de rechter-commissaris in de rechtbank Den Haag, ECLI:NL:RBDHA:2013:19764.
[500] Zie hierboven paragraaf 3.7, onder het kopje 'Uitstel van het bekendmaken van een onbekende kwetsbaarheid op de voet van artikel 126ffa Sv'. Zie voor de bevindingen van de Inspectie ter zake: Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2020*, Den Haag: Inspectie Justitie en Veiligheid 2021, p. 16.

en de zaaksofficier. Daarmee laat de regelgeving open dat zowel de digit-officier als de zaaksofficier toeziet op het treffen van de waarborgen.
Evenmin voorziet het Bogw in een bepaling over het moment waarop de onderscheidene waarborgen moeten worden getroffen. Bepaalde waarborgen kunnen praktisch gezien alleen tijdens het verrichten van onderzoekshandelingen worden getroffen, maar niet uitgesloten is dat waarborgen (ook) op een later moment worden genomen.

Beleid inzake de door Digit getroffen waarborgen

De digit-officier heeft meegedeeld dat hij het tot zijn taak rekent erop toe te zien (i) dat Digit waarborgen treft en (ii) dat de zaaksofficier ervoor zorgdraagt dat ook het tactische team waarborgen treft. Wat betreft de (voornamelijk: 'aanvullende') waarborgen die door Digit kunnen worden getroffen heeft de digit-officier gewezen op de volgende mogelijkheden:[501]

- de toevoeging aan het procesdossier van een omschrijving van de functionele specificaties van het technisch hulpmiddel;
- de voeging van een digitale kopie van de software en/of de broncode van het technisch hulpmiddel in het procesdossier;
- het voorafgaand aan het gebruik ervan testen in een test- en verificatieopstelling van de in het bevel opgenomen functionaliteiten van het technisch hulpmiddel op een testapparaat (i.e. een nabootsing van de hardware en software van het geautomatiseerde werk dat is omschreven in het bevel ex artikel 126nba Sv). Daarbij wordt geverifieerd of de gegevens die met de functionaliteiten van het technisch hulpmiddel worden verkregen overeenkomen met de gegevens op het testapparaat;
- het tijdens het verrichten van onderzoekshandelingen separaat mee laten lopen van een testapparaat waarop hetzelfde technische hulpmiddel is aangebracht;
- de vastlegging van schermopnames van de onderzoekshandelingen (bewegende beelden dan wel screenshots);
- de vastlegging van toetsaanslagen van de onderzoekshandelingen (keylogging);
- het audiovisueel vastleggen van de verrichtingen van Digit;
- toepassing van het vierogenprincipe door Digit;
- de aanwezigheid van de digit-officier op het moment dat Digit daadwerkelijk uitvoering geeft aan het bevel;
- het beveiligen van de verbindingen tussen het binnengedrongen geautomatiseerde werk en de technische infrastructuur van Digit;
- het beveiligen van gegevenstransport door middel van encryptie;
- het gebruik van certificaten om de identiteit van communicerende geautomatiseerde werken vast te stellen;
- het berekenen en vergelijken van de hashwaarde(s) van de gedetecteerde gegevens voor en na het transport.

De logging die is voorgeschreven in artikel 5 Bogw e.v. (zie paragraaf 3.10 hierboven), waaronder eveneens het registreren van screenshots valt, rekent de digit-officier dus ook tot de (mogelijke) waarborgen.[502]
Bij het handmatig verrichten van onderzoekshandelingen op een wijze die niet verschilt van die waarop een reguliere gebruiker gegevens tot zich neemt, zijn naar het oordeel van de digit-officier niet veel (in dat geval: 'procedurele') waarborgen nodig. Een voorbeeld betreft het geval waarin na het inloggen met de gebruikersgegevens van een verdachte, via een

[501] Daarbij heeft de digit-officier blijkens de gekozen bewoordingen mede acht geslagen op p. 45 van de nota van toelichting op het Bogw.

[502] Dat er zodoende een samenval is van de naleving van art. 21 Bogw (het treffen van waarborgen) met de loggingsvoorschriften (art. 5 Bogw) acht de digit-officier niet bezwaarlijk. Hij wijst daartoe op een passage in de nota van toelichting op het Bogw waarin "*audiovisueel vastleggen van de uitvoering van de onderzoekshandelingen*" expliciet als aanvullende waarborg is genoemd (nota van toelichting op het Bogw, p. 45). Zie voor het citaat hoofdstuk 3.7 hierboven.

standaardprotocol (als POP3), e-mails van een mailserver worden opgehaald, aldus de digit-officier. De waarborgen in een dergelijk geval betreffen volgens de digit-officier (i) het opmaken van een ambtsedig proces-verbaal, (ii) het vierogenprincipe, (iii) het opnemen van beeld- en toetsaanslagen (als waarborg en dus niet alleen als loggingseis), en (iv) de aanwezigheid van een toezichthoudend opsporingsambtenaar.
Bovendien heeft de digit-officier in gesprekken met de onderzoekers te kennen gegeven dat artikel 21 lid 5 Bogw niet vereist dat de procedurele waarborgen die bij een handmatige inzet worden genomen in de processtukken worden vermeld. Naar de letterlijke tekst van die bepaling heeft de digit-officier het gelijk aan zijn zijde, maar uit de toelichting op het Bogw blijkt onomwonden dat de officier van justitie wel degelijk geacht wordt in de processtukken te vermelden welke procedurele waarborgen zijn getroffen om de betrouwbaarheid, integriteit en de herleidbaarheid van de vastgelegde gegevens te garanderen.[503] Het OM heeft in reactie op het concept van dit rapport laten weten dat de digit-officier dit standpunt sinds begin oktober 2021 niet langer handhaaft en dat ook de procedurele waarborgen in de processtukken worden verantwoord.

Beleid inzake de door het tactisch team getroffen waarborgen

Globaal beschreven worden de zaaksofficieren door LP Digit geadviseerd/geïnstrueerd om de gegevens die ter uitvoering van het bevel ex artikel 126nba Sv zijn verkregen te verifiëren. Verificatie vindt plaats door deze gegevens te vergelijken met gegevens die zijn vergaard door toepassing van andere opsporingsbevoegdheden en met behulp van andere opsporingsmiddelen, zoals: de (latere) inbeslagneming van het geautomatiseerde werk waarop Digit de onderzoekshandelingen heeft verricht en het onderzoek van gegevens die daarin zijn opgeslagen, het vorderen van gegevens bij derden (bijvoorbeeld een telecomprovider), een telefoon- en internettap, OVC, observatie, e.d. Wanneer de met dergelijke middelen vergaarde gegevens geheel of ten dele overeenstemmen met gegevens die ter uitvoering van het bevel ex artikel 126nba Sv zijn vastgelegd, dan vormt dit een bevestiging, en dus een (extra) waarborg voor de betrouwbaarheid, integriteit en herleidbaarheid van de laatstbedoelde gegevens, aldus de digit-officier. Waarborgen zullen in elk geval (moeten) worden getroffen wanneer de identiteit van het technische hulpmiddel, de broncode en/of de specificaties ervan niet kunnen worden prijsgegeven.
De zaaksofficieren met wie semigestructureerde interviews hebben plaatsgehad bevestigen dat LP Digit hen heeft geïnstrueerd om erop toe te zien dat ook het tactisch team waarborgen treft. De zaaksofficier wordt daartoe geadviseerd, zowel mondeling tijdens voorbesprekingen, als schriftelijk in de vorm van uitgebreide, gedetailleerde handreikingen waarin de mogelijkheden voor eventuele waarborgen zijn opgesomd en beschreven. Van het tactisch team en de zaaksofficier wordt in dit verband het opstellen van een plan van aanpak gevergd met betrekking tot het treffen van de aanvullende waarborgen. Dit plan is voorwerp van toetsing en advisering door de CTC.

Constateringen bij het dossieronderzoek

Geconstateerd kan worden dat in de fase van besluitvorming ook de CTC zich buigt over de vraag of er waarborgen worden getroffen en, zo ja, welke.

Bij de inzage bleek dat de nba-dossiers niet altijd duidelijkheid verschaften over de aard en de omvang van de door Digit voorgestelde en/of daadwerkelijk getroffen waarborgen. In de rapporten haalbaarheidsonderzoek die aanwezig zijn in de nba-dossiers, wordt met name niet altijd concreet gemaakt welke waarborgen Digit had getroffen. Navraag bij LP Digit

[503] Zie over deze kwestie meer uitgebreid paragraaf 3.8 hierboven en zie met name de nota van toelichting op het Bogw, p. 21 en 22.

gaf meer duidelijkheid over de getroffen waarborgen, maar de voorgeschreven vastlegging ervan is slechts globaal.[504]

In één zaak werd bijvoorbeeld ten aanzien van de inzet van een niet-gekeurd technisch hulpmiddel in de CTC-stukken vermeld dat (technische) waarborgen zullen worden getroffen. Daarin werden echter geen concrete voorbeelden genoemd. Daarnaast werd de niet nader aangeduide 'mogelijkheid van verificatie' vermeld. Tot slot werd in de stukken van die zaak gesproken over de mogelijkheid om in de vervolgingsfase openheid te geven over het ingezette technische hulpmiddel, de specificaties daarvan en de getroffen waarborgen.
De digit-officier heeft in een gesprek daarover echter te kennen gegeven dat er géén waarborgen zijn getroffen. Dat er (uiteindelijk) geen vervolging is ingezet in deze zaak, ligt daaraan mogelijk ten grondslag. Sommige waarborgen dienen echter al tijdens de inzet te worden getroffen zodat een beslissing hierover reeds bij de voorbereiding van de inzet zal moeten worden genomen en in gang gezet. Dit is dan ook een leerpunt geweest volgens LP Digit. Het technische hulpmiddel is in deze zaak uiteindelijk ook afgekeurd door de keuringsdienst.
De digit-officier heeft aangegeven dat in een dergelijk geval, te weten een bij keuring achteraf *af*gekeurd technisch hulpmiddel, de wet strikt genomen niet voorziet in de verplichting om waarborgen te treffen. Dat is op zichzelf genomen juist, maar de ratio van artikel 21 Bogw is naar het oordeel van de onderzoekers anders.[505] Juist door het treffen van waarborgen kunnen resultaten eventueel wel bruikbaar worden.

In diezelfde zaak is geconstateerd dat een bevel is gegeven voor het verrichten van onderzoekshandelingen met behulp van een technisch hulpmiddel, terwijl bij het verrichten van onderzoekshandelingen uiteindelijk geen gebruik is gemaakt van het in het bevel genoemde technische hulpmiddel (zie ook paragraaf 5.4). Uit de stukken blijkt niet of en, zo ja, welke procedurele waarborgen zijn getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de tijdens het onderzoek vastgelegde gegevens te garanderen, zoals artikel 21 lid 5 Bogw voorschrijft in geval van een handmatige inzet.

In een andere zaak waarin sprake was van een handmatige inzet, werd geconstateerd dat de (procedurele) waarborgen die werden getroffen reeds standaardeisen betroffen die volgen uit het Bogw. Het ging daarbij om het verbaliseren van de aangetroffen gegevens, schermopnamen en geautomatiseerde logging van de systeemhandelingen. Dit is in lijn met de hierboven ingenomen stelling van de digit-officier, namelijk dat weinig of geen nadere waarborgen nodig zijn indien wordt gehandeld zoals 'de normale gebruiker' doet. De zaaksofficier van justitie heeft te kennen gegeven dat aan tactische zijde de volgende waarborgen zijn genomen: "*IP-tap, aanwezigheid digit rondom locaties tijdens enkele hack-pogingen en validatie verkregen gegevens op basis van de blockchain*".

Van de hierboven opgesomde, mogelijke door Digit getroffen waarborgen zijn de eerste twee (omschrijving functionele specificaties van het technisch hulpmiddel en voeging van

[504] De Inspectie heeft in dit verband vastgesteld: "*Op basis van de analyse van de inzetlogging stelt de Inspectie vast dat geen vastlegging beschikbaar is van door het technisch team getroffen waarborgen die aanvullend zijn op de standaard maatregelen die in (de toelichting bij) het wettelijk kader zijn beschreven. Op basis van de toelichting bij het Bogw, vindt de Inspectie het moment van de daadwerkelijke uitvoering van de hackbevoegdheid het meest voor de hand liggende moment voor het treffen van aanvullende waarborgen. Het is echter ook denkbaar dat de officier van justitie besluit aanvullende waarborgen te treffen buiten de inzet van het technisch team, die buiten het toezicht van de Inspectie JenV vallen. Bijvoorbeeld door een review op de toegepaste technieken te laten uitvoeren door een externe expert.*" Zie Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2019*, Den Haag: Ministerie van Justitie en Veiligheid 2020, p. 9-10.

[505] Zie paragraaf 3.8, onder het kopje 'Uitzondering op de hoofdregel (1): keuring achteraf', laatste alinea.

een digitale kopie van de software en/of de broncode van het technisch hulpmiddel in het dossier) in geen enkele zaak (volledig[506]) toegepast.
Aanvankelijk is TH Brons wel getest in een test- en verificatieopstelling, maar het technisch hulpmiddel werd op enig moment geacht zich in voldoende mate bewezen te hebben zodat bij een soortgelijk geautomatiseerd werk deze test niet telkens weer opnieuw plaatsvindt.
Daarentegen is het maken van schermopnamen en keylogging, afgezien van in de praktijk gebleken technische onvolkomenheden daarbij,[507] nagenoeg standaard,[508] evenals de toepassing van het vierogenprincipe en de aanwezigheid van de digit-officier. Het beveiligen van de verbindingen en het gegevenstransport is nagenoeg standaard, evenals het berekenen van de hashwaarde(s) voor en na het transport.

Bij het dossieronderzoek is gebleken dat de procesdossiers (wel) duidelijk maakten welke waarborgen van de zijde van het tactische team waren getroffen. De resultaten van de inzet van opsporingsmiddelen maakten het de rechter en procesdeelnemers mogelijk om de resultaten die waren verkregen ter uitvoering van het bevel ex 126nba Sv te verifiëren op de wijze als hierboven omschreven. De waarborgen die aan tactische zijde worden getroffen zijn in veel zaken omvangrijk en adequaat. In elk geval is er van tactische zijde, dat wil zeggen: van de kant van de zaaksofficier en het tactische team, veel aandacht om ervoor te zorgen dat de informatie verkregen door toepassing van artikel 126nba Sv geverifieerd kan worden op basis van andere opsporingsmiddelen. LP Digit heeft daarvoor (gedurende de onderzoeksperiode) diverse kaders en handvatten opgesteld voor de zaaksofficieren. De zaaksofficieren hebben daaraan, samen met het tactisch team, daadwerkelijk gevolg gegeven.

5.7. De logging

Bevindingen van de Inspectie
Digit dient bij de uitvoering van onderzoek in een geautomatiseerd werk voorschriften voor logging in acht te nemen.[509] De Inspectie heeft in het kader van haar toezichthoudende taak, met gebruikmaking van de logging onderzoek gedaan naar eventuele onregelmatigheden bij de uitvoering van onderzoek in een geautomatiseerd werk.
Voor haar verslag over 2019 heeft de Inspectie per zaak de beschikbare logging geanalyseerd en daarbij verscheidene onvolkomenheden vastgesteld.[510] Daaraan heeft de Inspectie als conclusie verbonden dat het ontbreken van logging de Inspectie heeft bemoeilijkt in de uitoefening van haar toezichthoudende taak, maar dat zij op basis van de wél beschikbare logging de uitgevoerde handelingen grotendeels heeft kunnen reconstrueren en dat zij hierbij geen aanwijzing heeft dat hierdoor onregelmatigheden onopgemerkt zijn gebleven die van invloed waren op de betrouwbaarheid en integriteit van de vastgelegde gegevens of dat er buiten de reikwijdte van het bevel is gehandeld.

Ook in haar verslag over 2020 is de Inspectie kritisch. Zo heeft de Inspectie vastgesteld dat:

> *"– de logging van verrichte handelingen ter uitvoering van een bevel onvolledig is voor alle zaken waarin in 2020 onderzoekshandelingen zijn verricht. Dit is mede veroorzaakt door*

[506] De omschrijving van de functionele specificaties van TH Brons is wel vastgelegd in de '21.4-processen-verbaal van bevindingen', echter summier.
[507] Zie ook de (kritische) bevindingen van de Inspectie hierover die in de volgende paragraaf over logging ter sprake komen.
[508] Tot voor kort *was* 'keylogging' nagenoeg standaard, aldus mededelingen van de Inspectie Justitie en Veiligheid. Daarin is vanaf jaar 2022 verandering gekomen. Keylogging wordt sindsdien wegens de geringe toegevoegde waarde meer en meer achterwege gelaten.
[509] Zie paragraaf 3.10 hierboven.
[510] Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2019*, Den Haag: Ministerie van Justitie en Veiligheid 2020, p. 21-22.

het in heel 2020 niet goed functioneren van de voorziening voor het registreren van beeldschermopnames. Daarnaast heeft het technisch team niet alle handelingen uitgevoerd via systemen waarvan beeldschermopnames en toetsaanslagen worden vastgelegd. Ook kan op basis van de logbestanden niet worden vastgesteld in hoeverre verwijdering van de in 2020 ingezette technisch hulpmiddelen daadwerkelijk volledig heeft plaatsgevonden;
- *niet door de politie is uitgewerkt hoe per zaak invulling wordt gegeven aan de vereiste doorlopende en automatische vastlegging van gegevens in logbestanden. Deze uitwerking is van belang voor de politie om te kunnen komen tot het treffen van passende maatregelen voor de betrouwbaarheid en de integriteit van de logbestanden en het effectief uitvoeren van de eigen interne controle;*
- *de politie geen structurele controle heeft uitgevoerd op een juiste en volledige registratie in logging en andere verslaglegging."*[511]

In haar verslag over 2021 constateert de Inspectie diverse verbeteringen maar ziet zij ook nog onvolkomenheden. Zij stelt onder andere vast dat in 2021:

"– *op enkele kleine hiaten na, het samenstel van de automatisch en handmatig vastgelegde logging voldoende basis biedt voor het reconstrueren van alle in 2021 verrichte opsporingshandelingen op basis van de afgegeven bevelen;*
- *de volledigheid van de vastgelegde beeldschermopnames gedurende 2021 sterk is verbeterd. Zowel in 2019 als in 2020 en gedurende de eerste helft van 2021 was sprake van hiaten, mede doordat de voorziening voor het registreren van deze opnames niet goed functioneerde. Dit is inmiddels verbeterd;*
- *de politie is gestart met een volledigheidscontrole op de schermopnames van de handelingen die zijn verricht met het ingekochte technisch hulpmiddel voor de inzet waarvan in 23 van de 28 zaken bevel is gegeven. (...);*
- *in slechts één zaak de registratie van toetsaanslagen volledig is vastgelegd. Hierbij merkt de Inspectie op dat de registratie van toetsaanslagen in het merendeel van de zaken inhoudelijk geen waarde toevoegt;*
- *de politie is gestart met het testen van een softwarematige oplossing voor het vastleggen van beeldschermopnames en toetsaanslagen. Deze voorziening wordt ingezet bovenop de reeds aanwezige oplossing, waardoor het risico op ontbrekende beeldschermopnames en toetsaanslagen wordt verkleind;*
- *in de handmatige zaken niet vastgelegd is welke scripts ingezet zijn. Hierdoor is niet controleerbaar welke (versies van) scripts precies zijn ingezet en wat deze scripts deden;*
- *de journalisering sterk is verbeterd ten opzichte van de situatie in 2020. Verbeteringen zijn zichtbaar in de tijdigheid, detaillering en volledigheid. Wel heeft de Inspectie ook in 2021 in het journaal enkele verschrijvingen en omissies geïdentificeerd."*[512]

Constateringen toezichtonderzoek

Logging behoort in de eerste plaats tot de taken en verantwoordelijkheden van Digit. Niettemin doen deze kritiekpunten de vraag rijzen hoe de door de Inspectie vastgestelde manco's zich verhouden tot de wijze waarop LP Digit toezicht uitoefent op Digit.

Naar de mededelingen van de digit-officier voert LP Digit controle uit op de bewijslogging, omdat het daarbij gaat om de vastlegging van de gegevens die eventueel tot het bewijs in de strafzaak kunnen dienen. In haar verslag over 2021 stelt de Inspectie in dat verband vast dat de opslag van de bewijslogging verenigbaar is met de eisen van het Bogw. In het bijzonder constateert de Inspectie dat in 2021:

---

[511] Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2020*, Den Haag: Ministerie van Justitie en Veiligheid 2021, p. 11-12.

[512] Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2021*, Den Haag: Ministerie van Justitie en Veiligheid 2022, p. 27.

"– *de door DIGIT verkregen bewijslogging opgeslagen is in deze voorziening die onderdeel uitmaakt van de technische infrastructuur;*
– *maatregelen van kracht waren om de gegevens in deze voorziening te beschermen tegen wijzigingen en tegen kennisneming door onbevoegden;*
– *de gegevens uitsluitend toegankelijk waren voor medewerkers van DIGIT en de Inspectie;*
– *de opslag van de gegevens in deze voorziening plaatsvindt op een beveiligde politieserver in beheer van de politie die zich in Nederland bevindt."*[513]

De Inspectie maakt echter wel een uitzondering voor de tijdelijke opslag van de bewijslogging op (bijvoorbeeld) een voorziening in TH Brons zelf.[514] In dat geval is niet aan de hiervoor bedoelde waarborgen voor beveiligde opslag voldaan. Een van de risico's daarvan is dat ook anderen dan de aangewezen personen met toegang tot de technische infrastructuur kunnen kennisnemen van deze gegevens. Het OM heeft in reactie op het concept van dit rapport laten weten dat het bij gebruik van technisch hulpmiddelen onvermijdelijk is dat de daarmee geregistreerde gegevens tijdelijk op een lokale component van dat technische hulpmiddel worden opgeslagen. In het geval van TH Brons worden de gegevens ieder etmaal naar de technische infrastructuur van Digit getransporteerd en daar opgeslagen als bewijslogging.

Op de overige drie vormen van logging (zie paragraaf 3.10 hierboven) houdt LP Digit minder direct toezicht omdat dit in eerste instantie een taak is van Digit zelf. Ondanks de door de Inspectie geconstateerde (en door de digit-officier niet betwiste) onvolkomenheden acht de digit-officier de toestand niet dermate zorgwekkend dat er aanleiding is voor ingrijpen. Het betreft maar een klein percentage van de gevallen waarin logging ontbreekt en in die gevallen is daarvoor een redelijke verklaring te geven. Naar aanleiding van de verslagen van de Inspectie is LP Digit wel in gesprek gegaan met Digit over de logging en zijn er ook alternatieven ontwikkeld, bijvoorbeeld een zelfgebouwd beeldscherm- en toetsaanslagenregistratiesysteem.
LP Digit herkent zich niet in de kritiek van de Inspectie omtrent het ontbreken van een intern kwaliteitssysteem, waarvan een goede logging nu juist de basis kan zijn volgens de Inspectie.[515] LP Digit ziet meer in een vorm van controle die gebruikelijk is in de opsporing: "*een ambtsedig relaterend ambtenaar, een dossiervormer die meekijkt, de toevoeging van een operationeel jurist aan het team, een teamleider die meekijkt en twee heftig gespecialiseerde OM-medewerkers die ook nog met het product meekijken*", aldus de digit-officier.
De onderzoekers constateren dat de inhoud van het begrip 'onregelmatigheid' in artikel 6, 23 en 24 Bogw aanleiding kan geven tot discussie.[516] De digit-officier hanteert in dit verband een vrij strikte uitleg daarvan en is van oordeel dat alleen die onregelmatigheden die afbreuk doen aan de bewijskracht van de gegevens dienen te worden geverbaliseerd. Dat oordeel achten de onderzoekers goed verdedigbaar.[517]

---

[513] Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2021*, Den Haag: Ministerie van Justitie en Veiligheid 2022, p. 30.
[514] Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2021*, Den Haag: Ministerie van Justitie en Veiligheid 2022, p. 30-31. Deze uitzondering is hierboven reeds gesignaleerd bij de bespreking van het gebruik van TH Brons (zie: opslag van gegevens in TH Brons onder 5.5).
[515] Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2020*, Den Haag: Ministerie van Justitie en Veiligheid 2021, p. 17 en p. 21.
[516] Zie bijv. Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2021*, Den Haag: Ministerie van Justitie en Veiligheid 2022, p. 28, waarin de Inspectie kritisch vaststelt dat een "*nadere uitwerking van welke gebeurtenissen de politie als 'onregelmatigheid' ziet, (…) in 2021 niet aangetroffen*" is en dat "*een controleerbaar afwegingskader ontbreekt, waardoor de eerste afweging of sprake is van een onregelmatigheid in belangrijke mate gebaseerd is op de professionele inschatting door individuele medewerkers van DIGIT.*"
[517] Zie hierover paragraaf 3.10, onder het kopje 'Logging als middel van controle en toezicht', en de voetnoten bij die tekst.

Behoudens de signalering van de problematiek van de opslag van de bewijslogging op een voorziening binnen TH Brons zelf, geven de voorgaande constateringen de onderzoekers geen aanleiding tot nader commentaar.

5.8. Het opmaken van proces-verbaal

In paragraaf 3.11 is uiteengezet dat niet alleen de gegevens die zijn verkregen met uitoefening van de bevoegdheid van artikel 126nba Sv, maar ook de wijze waarop die gegevens zijn verkregen in een proces-verbaal moet worden gerelateerd. Op die manier wordt controle op de uitoefening van bevoegdheden mogelijk gemaakt.
Bij het dossieronderzoek werden aanvankelijk tekortkomingen gezien, met name wat betreft de duur van de periode die is gelegen tussen het onderzoek in een geautomatiseerd werk en de verslaglegging ervan. Op basis hiervan werd in het tussenrapport geconstateerd dat in enkele van de onderzochte nba-dossiers tijdens de inzage geen proces-verbaal aanwezig bleek met verslaglegging van het verrichten van onderzoekshandelingen in het geautomatiseerde werk, het eventuele plaatsen en verwijderen van een technisch hulpmiddel, en het overdragen van gegevens aan het tactische team, met bijvoorbeeld informatie over de vragen of er aanleiding was voor een selectie van gegevens en of er onregelmatigheden hadden plaatsgehad bij het onderzoek in een geautomatiseerd werk. De verbaliseringsplicht betrof in deze gevallen verrichtingen die vrij veel maanden daarvoor hadden plaatsgehad. Vanwege deze tekortkomingen bleef aanvankelijk ook onduidelijk welke gegevens waren overgedragen aan het tactische team[518] en of zich overigens onregelmatigheden hadden voorgedaan. Deze tekortkoming in de verantwoording van het onderzoek in een geautomatiseerd werk door Digit was overigens niet aan de aandacht van LP Digit ontsnapt. Door LP Digit is bij Digit meermalen navraag gedaan naar de processen-verbaal.
Hoewel niet in alle zaken, is bij het vervolgonderzoek in meer recente zaken verbetering geconstateerd. LP Digit liet weten dat het erop heeft toegezien dat Digit een 'inhaalslag' heeft gemaakt.[519]

De constatering dat niet altijd ten spoedigste proces-verbaal is opgemaakt kan worden genuanceerd door het volgende. Enige vertraging in het definitief opmaken van het proces-verbaal behoeft niet bezwaarlijk te zijn, zolang in elk geval maar in een andere vorm van verslaglegging is voorzien die wel spoedig is gevolgd op de desbetreffende opsporingsverrichting. In dat kader is door LP Digit te kennen gegeven dat alle onderzoekshandelingen van Digit wel tijdig en nauwkeurig worden opgenomen in een journaal.[520] Dat journaal vormt vervolgens de basis van het opmaken van het proces-verbaal. De betrouwbaarheid van de neerslag van hetgeen bevonden of ter opsporing is verricht, is in dat geval in beginsel toereikend gewaarborgd, terwijl in beginsel doeltreffend kan worden gereageerd op een verzoek van de rechter tot nadere verantwoording omtrent het betreffende gedeelte van het opsporingsonderzoek.[521]

---

[518] Zie paragraaf 3.9 hierboven.

[519] Vgl. ook Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2021*, Den Haag: Inspectie Justitie en Veiligheid 2022, p. 31: "*De Inspectie stel vast dat in 2021 (…) processen-verbaal kort na het afronden van de betreffende handelingen of het optreden van de betreffende gebeurtenissen zijn opgesteld en ondertekend. Dit is een verbetering ten opzichte van de situatie in 2019 en 2020 (…).*"

[520] De toetsing van de inhoud van de journaals van de politie valt onder de toezichttaak van de Inspectie van Justitie en Veiligheid.

[521] Vgl. A.M. van Hoorn in: *Tekst & Commentaar Strafvordering*, Deventer: Kluwer, art. 152, aant. 2 (online, bijgewerkt tot 1 januari 2022), en HR 19 december 1995, ECLI:NL:HR:1995:ZD0328, rov. 11.2.1. Daarin heeft de Hoge Raad bepaald dat indien het opmaken van een proces-verbaal achterwege blijft, wel moeten worden voorzien in een zodanige verslaglegging van de desbetreffende verrichtingen en bevindingen dat doeltreffend kan worden gereageerd op een verzoek van de rechter in het eindonderzoek tot nadere verantwoording omtrent dat gedeelte van het opsporingsonderzoek.

In dat verband is evenwel van belang op te merken dat de Inspectie in haar verslag over 2020 heeft vastgesteld dat de "*verantwoording* [in processen-verbaal en het journaal] *onvolledig is en soms ontbreekt. Voor de wel aanwezige processen-verbaal geldt dat hieruit niet kan worden opgemaakt welke onderzoekshandelingen door wie op welk moment zijn uitgevoerd. In enkele gevallen kan dit ook niet worden vastgesteld op basis van het journaal en de aanwezige logging.*"[522]
In haar verslag over 2021 merkt de Inspectie echter op dat het bijhouden van het journaal ten opzichte van 2020 vollediger, meer gestructureerd en meer uniform plaatsvindt en daarmee sterk verbeterd is. Tegelijkertijd constateert zij dat de *"afgelegde verantwoording in enkele processen-verbaal op onderdelen niet geheel overeenkomt met de daadwerkelijke uitvoering"* en dat "*het journaal (…) niet in alle gevallen juist is wanneer dit afgezet wordt tegen de feitelijke verrichtingen op basis van systeemlogging. Dit heeft gevolgen voor de juistheid van de processen-verbaal omdat de processen-verbaal gebaseerd zijn op de informatie uit het journaal.*"[523]

Aandachtspunt achten de onderzoekers de betrekkelijk globale wijze waarop de verslaglegging van onderzoekshandelingen (in het proces-verbaal) plaatsvindt, bijvoorbeeld de plaatsing en verwijdering van het technisch hulpmiddel en de overdracht van gegevens. Die elementen van de uitvoering van het onderzoek worden door Digit steeds in één standaardzin omschreven. Ofschoon het belang van afscherming hierbij in aanmerking genomen kan worden, is controle daardoor nagenoeg onmogelijk. Dat wil zeggen: daardoor kan niet door alle procesdeelnemers onmiddellijk worden nagegaan wanneer plaatsing en verwijdering hebben plaatsgehad. Alleen wanneer de rechter uitdrukkelijk beveelt om dat bekend te maken kan dat alsnog.
In dit kader kan nog een onvolkomenheid worden gesignaleerd. In twee van de in het dossieronderzoek onderzochte zaken is, zoals gezegd, binnengedrongen in een geautomatiseerd werk (smartphone) met een IMEI-nummer dat niet correspondeerde met het IMEI-nummer in het bevel. In één zaak is in de later opgemaakte processen-verbaal, nadat door de politie dus was geconstateerd dat in feite op een smartphone met een ander IMEI-nummer was binnengedrongen, nog steeds het verkeerde IMEI-nummer vermeld van de smartphone waarop zou zijn binnengedrongen. Anders gezegd: de processen-verbaal geven niet de juiste omschrijving van het toestel waarop feitelijk is binnengedrongen. Vermoedelijk zijn per abuis de gegevens van het bevel overgenomen en niet de gegevens van het geautomatiseerd werk waarop in feite was binnengedrongen. Na constatering hiervan door de onderzoekers zijn de processen-verbaal daarop (alsnog) aangevuld.

Ook aan tactische zijde laten de processen-verbaal in procesdossiers in sommige gevallen lang op zich wachten, met dien verstande dat het begrijpelijk is dat processen-verbaal waarin de verificaties worden weergegeven (dat wil zeggen: de aanvullende waarborg dat de gegevens die met de toepassing van artikel 126nba Sv zijn verkregen worden geverifieerd aan de hand van de onderzoeksresultaten die met andere opsporingsmiddelen zijn behaald) niet eerder dan na afronding van het onderzoek en de analyse van de onderzoeksresultaten kunnen worden opgemaakt. Daarnaast kan worden opgemerkt dat aan tactische zijde niet altijd processen-verbaal voorhanden zijn waarin kenbaar wordt gemaakt welke gegevens precies van Digit zijn ontvangen. In de zaak in kwestie waren weliswaar processen-verbaal van Digit voorhanden, maar daarin was niet méér opgenomen dan dat "*gegevens zijn vastgelegd en overgedragen*".

[522] Zie Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2020*, Den Haag: Inspectie Justitie en Veiligheid 2021, p. 12. Zie ook p. 20-21.
[523] Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2021*, Den Haag: Inspectie Justitie en Veiligheid 2022, p. 31.

Samenvattend is de belangrijkste constatering dat de betrekkelijk globale en gestandaardiseerde wijze waarop de onderzoekshandelingen van Digit worden omschreven problematisch is. Als gevolg daarvan kunnen controle en toezicht hierop slechts zeer beperkt plaatsvinden. De digit-officier heeft te kennen gegeven dat onder zijn verantwoordelijkheid voor deze wijze van verbalisering is gekozen uit het oogpunt van afscherming van methoden en technieken. Het journaal, dat niet bij de processtukken wordt gevoegd, bevat naar de mededelingen van de digit-officier zodanige informatie dat eventuele vragen van de rechter adequaat kunnen worden beantwoord. Naar het oordeel van de onderzoekers is echter een gedetailleerder proces-verbaal geboden.

5.9. De notificatie en de vernietiging van gegevens

LP Digit wijst de zaaksofficieren standaard op het bestaan en de reikwijdte van de notificatieplicht.[524] In geen van de in het dossieronderzoek onderzochte zaken heeft notificatie plaatsgehad, omdat het opsporingsonderzoek in geen van de zaken (ten tijde van de onderzoeksperiode) is afgerond.[525]
Omtrent de vernietiging van gegevens bevindt zich in de onderzochte nba-dossiers en procesdossiers geen informatie, uitgezonderd (1) de hiervoor onder paragraaf 5.3 vermelde zaak waarin de zaaksofficier van justitie tot vernietiging van de verkregen gegevens heeft besloten nadat in een ander geautomatiseerd werk was binnengedrongen dan in het bevel was opgenomen, en (2) de werkwijze omtrent de vernietiging van aangetroffen geheimhoudersgegevens, die hiervoor bij paragraaf 4.3 ter sprake is gekomen. De noodzaak van vernietiging van gegevens kan pas worden geverifieerd indien voldoende aan de verbaliseringsplicht is tegemoetgekomen.

5.10. Geheimhoudersgegevens en het verschoningsrecht

In paragraaf 4.3 is reeds het door het OM vastgelegde beleid omschreven aangaande de registratie of kennisneming van mogelijke geheimhoudersgegevens. Het beleid voorziet in het verhinderen dat geheimhoudersgegevens ter kennis komen van het tactisch team, maar voorziet niet in de filtering van dergelijke gegevens uit de technische infrastructuur van Digit en uit de forensische kopieën die worden vervaardigd van de gegevensdragers waartoe Digit zich bij het onderzoek in een geautomatiseerd werk toegang heeft verschaft.
De praktijk laat zien dat het onder bepaalde omstandigheden ook anders kan, namelijk in de weinig voorkomende gevallen waarin Digit zelf tijdig kan opmerken dat verschoningsgerechtigd materiaal wordt geregistreerd, en daarvan melding wordt gemaakt aan de digit-officier, waarna de verdere registratie (eventueel) in zijn opdracht wordt beëindigd. Dit betreft echter uitzonderingsgevallen en ook dan gelden volgens het OM beperkingen in de mogelijkheden. Daarnaast hebben de zaaksofficieren in een zaak te kennen gegeven bewust van inzet van OVC over de band van artikel 126nba Sv af te zien op momenten dat sprake is van een geheimhouderslocatie of indien een geheimhouder wordt waargenomen in aanwezigheid van de verdachte.

Het dossieronderzoek brengt de onderzoekers daarnaast nog tot de volgende opmerkingen. In één zaak was de verdachte zelf een geheimhouder en is daarvoor een separaat protocol ontwikkeld om de zorgvuldigheid te waarborgen.

[524] Zie paragraaf 3.13 hierboven.
[525] De inspectie signaleert wel dat in 2021 in één zaak notificatie inclusief de vernietiging van gegevens heeft plaatsgevonden. Zie Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2021*, Den Haag: Inspectie Justitie en Veiligheid 2022, p. 33.

In een andere zaak kan worden betwijfeld of de omgang met geheimhoudersgegevens plaatshad overeenkomstig het hiervoor omschreven beleid. Op schriftelijke vragen heeft de zaaksofficier namelijk laten weten: "*bij het tactisch team werden de data eerst gelezen door* één *persoon*". Indien zich hieronder geheimhoudersgegevens bevinden, zou direct contact worden opgenomen met de officier van justitie om deze aan hem voor te leggen met het oog op de mogelijke verwijdering ervan uit de dataset. Deze gang van zaken wekt evenwel het vermoeden dat er geen sprake was van een afzonderlijke geheimhoudersfunctionaris. Navraag hiernaar heeft tot op heden geen duidelijkheid gegeven.

5.11. Internationale aspecten van de toepassing van de bevoegdheid

In vijf van de in het dossieronderzoek onderzochte zaken werd de bevoegdheid van artikel 126nba Sv buiten het grondgebied van Nederland ingezet, dan wel werd bij de inzet van de bevoegdheid met de autoriteiten van een ander land samengewerkt. Daarover de volgende opmerkingen.
In één zaak deed zich de situatie voor dat één van de geautomatiseerde werken die in gebruik waren bij de verdachte(n) zich bevond op het grondgebied van een andere staat die partij is bij het Cybercrimeverdrag. In dit geval heeft de digit-officier via de e-mail contact opgenomen met zijn ambtgenoot in de betreffende andere staat en is het onderzoek in dat geautomatiseerde werk niet eerder aangevangen dan na het verkrijgen van diens instemming. Die instemming was vastgelegd in het nba-dossier. In het licht van artikel 6 van de EU-rechtshulpovereenkomst, roept de gevolgde procedure geen vragen op.[526]

In een andere zaak werd aan de desbetreffende buitenlandse autoriteit (alleen) toestemming gevraagd voor het opnemen van vertrouwelijke communicatie (OVC) op basis van artikel 126l Sv. Daarbij werd niet vermeld dat daartoe heimelijk en op afstand een geautomatiseerd werk zou worden binnengedrongen, als bedoeld in artikel 126nba Sv. Dit was overigens conform het advies van de CTC. De vraag is echter of het verzwijgen van de methode niet indruist tegen internationale afspraken. Daartegen pleit dat voor het onderzoeksdoel waar het om gaat, te weten het afluisteren, expliciet toestemming was verkregen en dat het binnendringen in een geautomatiseerd werk reeds in Nederland had plaatsgevonden.

Een zaak die daarop lijkt betreft een geval waarin uiteindelijk geen inzet van de bevoegdheid in het buitenland heeft plaatsgevonden. Wel werden de resultaten van de toepassing van de bevoegdheid van artikel 126nba Sv in Nederland gedeeld met de buitenlandse autoriteiten. Om problemen in het buitenland te voorkomen heeft de betrokken zaaksofficier van justitie blijkens e-mailwisselingen laten weten dat het de voorkeur verdient om in het proces-verbaal dat ten behoeve van de autoriteiten in het buitenland zou worden opgemaakt kenbaar te maken dat de onderzoeksresultaten waren verkregen bij de uitvoering van een bevel tot het aftappen en opnemen van telecommunicatie (ex artikel 126m Sv) en het opnemen van vertrouwelijke communicatie (OVC) met een technisch hulpmiddel (ex artikel 126l Sv), zonder daarbij (eveneens) te vermelden dat ook toepassing was gegeven aan artikel 126nba Sv. Afschermingsbelangen zullen hierbij een rol hebben gespeeld. Andere aanwijzingen in het dossier duiden er echter weer op dat de buitenlandse autoriteiten wel degelijk over de toepassing van artikel 126nba Sv zijn geïnformeerd, zodat niet kan worden vastgesteld dat

[526] Nederland en de betreffende staat zijn partij bij de EU-rechtshulpovereenkomst, volledig: Overeenkomst, door de Raad vastgesteld overeenkomstig artikel 34 van het Verdrag betreffende de Europese Unie, betreffende de wederzijdse rechtshulp in strafzaken tussen de lidstaten van de Europese Unie, van 29 mei 2000, *Trb.* 2000, 96. Rechtshulpverzoeken kunnen overeenkomstig dit verdrag niet alleen schriftelijk worden gedaan en beantwoord, maar ook op zodanige wijze dat het verzoek schriftelijk kan worden vastgelegd en de ontvangende lidstaat de echtheid ervan kan vaststellen. Het is derhalve mogelijk om verzoeken via bijvoorbeeld fax en e-mail te doen. Er wordt echter wel als eis gesteld dat de aangezochte lidstaat zich ervan moet kunnen vergewissen dat een verzoek authentiek is.

het aan transparantie heeft ontbroken. Net als de vorige zaak roept deze gang van zaken echter wel de vraag op of de voorgestelde werkwijze conform internationale afspraken is.

In weer een andere zaak ging het om de inzet van de bevoegdheid in een ander land dan Nederland binnen het Koninkrijk der Nederlanden. Uit het dossier bleek niet wat de juridische grondslag was van deze inzet. Volgens LP Digit was er geen rechtshulpverzoek nodig omdat één van de verdachten een militair was. Daarop is binnen het gehele Koninkrijk het Wetboek van Strafvordering van het Europese deel van Nederland van toepassing, aldus de digit-officier.[527] De zaaksofficier gaf op schriftelijke vragen te kennen dat het uitvoeren van onderzoek in een geautomatiseerd werk tevens had plaatsgevonden op basis van een interregionaal rechtshulpverzoek op de grondslag van artikel 36 van het Statuut voor het Koninkrijk der Nederlanden.[528] Dit sluit aan bij de CTC-stukken in het dossier waarin ook melding wordt gemaakt van een interregionaal rechtshulpverzoek. Naast de militair, zou het hier gaan om de inzet op een andere verdachte, die geen Nederlandse militair is.

Tot slot een zaak waarin het onder meer ging om de ontoegankelijkmaking van een botnet. Het botnet strekte zich uit over een groot aantal landen met potentieel zeer veel geïnfecteerde geautomatiseerde werken, verspreid over de hele wereld. Het tactische team heeft onderzoek verricht in samenwerking met verscheidene andere Europese landen, de Verenigde Staten en Canada. In dat samenwerkingsverband werd aan de Nederlandse justitie en politie de taak toebedeeld om het botnet – na voltooiing van het tactische onderzoek dat was gericht op de identificatie van de verdachten – ontoegankelijk te maken (conform onderzoeksdoelstelling e van artikel 126nba lid 1 Sv). Noch voorafgaand, noch na afloop van de op zich succesvolle ontoegankelijkmaking zijn internationale-rechtshulpverzoeken verzonden naar landen waarin zich geïnfecteerde geautomatiseerde werken bevonden. Voorafgaand aan de inzet kon namelijk niet worden vastgesteld om welke landen het op het moment van de inzet precies zou gaan; dit was afhankelijk van de vraag of een of meer van de gecompromitteerde geautomatiseerde werken in een bepaald land op het moment van de inzet was of waren verbonden met de *command and control server* waarop zou worden binnengedrongen. Alleen in dat geval zou de inzet zich ook uitstrekken tot het betreffende geautomatiseerde werk. Tijdens en na de inzet kon echter in principe (definitief) worden vastgesteld om welke (vele) IP-adressen en welke (vele) landen het ging.
Binnen het samenwerkingsverband hebben de vertegenwoordigers van de betrokken landen desgevraagd ingestemd met de methode van ontoegankelijkmaking. Tot slot werd de code waarmee de geautomatiseerde werken met het botnetvirus waren geïnfecteerd gepubliceerd, zodat elke potentiële gebruiker kon nagaan of zijn computer was geïnfecteerd.

---

[527] Opmerking onderzoekers: op zichzelf is dat standpunt juist, doch uitsluitend voor zover het onderzoek in een geautomatiseerd werk de militair betreft. Art. 1 lid 3 van de Wet militaire strafrechtspraak, een rijkswet, bepaalt dat op (kort gezegd) Nederlandse militairen het Wetboek van Strafvordering van het Europese deel van Nederland van toepassing is, tenzij daarvan in die rijkswet wordt afgeweken. Ingevolge art. 58 van de Wet militaire strafrechtspraak kunnen opsporingsambtenaren in Aruba, Curaçao en Sint Maarten en in de openbare lichamen Bonaire, Sint Eustatius en Saba bij de uitoefening van hun bevoegdheden echter niet dan met inachtneming van de grenzen in de ter plaatse geldende wetgeving voor de gewone strafvordering gesteld, inbreuk maken op de rechten van personen die niet aan de rechtsmacht van de militaire rechter zijn onderworpen. Zie ook de volgende twee voetnoten.

[528] Art. 36 van het Statuut voor het Koninkrijk der Nederlanden (hierna: het Statuut) bepaalt (slechts) dat Nederland, Aruba, Curaçao en Sint Maarten elkander hulp en bijstand verlenen. Deze bepaling vormt de grondslag voor (i) het doen van en (ii) het gevolg geven aan interregionale verzoeken om rechtshulp. Ingevolge artikel 40 van het Statuut kunnen vonnissen, gewezen door de rechter in Nederland, Aruba, Curaçao of Sint Maarten, en bevelen, door hem uitgevaardigd, mitsgaders grossen van authentieke akten, aldaar verleden, in het gehele Koninkrijk ten uitvoer worden gelegd, met inachtneming van de wettelijke bepalingen van het land waar de tenuitvoerlegging plaatsvindt. Een soortgelijke bepaling voor de bevelen van officieren van justitie bevat het Statuut niet. Volgens art. 39 lid 1 van het Statuut (waarin het concordantiebeginsel is belichaamd) worden (onder meer) het strafrecht en de strafvordering in Nederland, Aruba, Curaçao en Sint Maarten zoveel mogelijk op overeenkomstige wijze geregeld. Die bepaling brengt echter niet mee dat de strafvordering binnen de landen van het Koninkrijk gelijkluidend (eenvormig) is geregeld, althans dat dit zo zou moeten zijn. Zie hierover o.m.: J.M. Reijntjes, *Het interregionale strafrecht van het Koninkrijk der Nederlanden*, Den Haag: Boom juridisch 2015, p. 11-24.

Mede tegen de achtergrond van de daarmee gemoeide belangen van de gebruikers van de gecompromitteerde geautomatiseerde werken en het grote aantal daarvan, valt de keuze van het OM voor de hiervoor geschetste procedure te verdedigen. Niettemin moet worden geconstateerd dat de Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv[529] niet voorziet in een op deze situatie toegesneden uitzondering. De uitgangsgegevens in deze zaak voldoen niet aan de criteria voor het achterwege laten van internationale-rechtshulpverzoeken aan de landen waarin zich de betrokken geautomatiseerde werken bevonden. Het valt aan te bevelen de Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv zodanig aan te passen dat daarin alsnog wordt voorzien in een op dergelijke zaken toegesneden uitzondering.

Ten slotte heeft de Inspectie in zijn algemeenheid erop gewezen dat in de logging de locatie van het binnengedrongen geautomatiseerde werk niet automatisch en doorlopend wordt vastgelegd. Ook uit de verslaglegging van Digit kon de Inspectie niet altijd vaststellen op welke locatie en in welk land een geautomatiseerd werk zich tijdens een actie bevond. De Inspectie kan hierdoor voor enkele onderzoekshandelingen niet – op basis van de logging – bepalen of het OM en/of Digit hiervoor toestemming had.[530] De digit-officier heeft er in dat verband op gewezen dat het automatisch en doorlopend vastleggen van de locatie van het binnengedrongen geautomatiseerde werk in feite neerkomt op de stelselmatige observatie van de gebruiker van dat geautomatiseerde werk, terwijl daarvoor niet in alle gevallen een bevel is afgegeven.

Kort gezegd hebben de onderzoekers geconstateerd dat de uitoefening van de bevoegdheid van artikel 126nba Sv buiten het grondgebied van Nederland in één geval niet heeft plaatsgehad in overeenstemming met de door het OM zelf opgestelde Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv. Tevens kan de Inspectie niet altijd aan de hand van de logging nagaan in welk land een geautomatiseerd werk zich tijdens een actie bevond. In dit manco kan mogelijk worden voorzien door alleen tijdens het daadwerkelijke binnendringen en verrichten van onderzoekshandelingen in een geautomatiseerd werk (‘een actie’) de locatiegegevens van het binnengedrongen geautomatiseerde werk te loggen, en indien en voor zover die actie van langere duur is daartoe een bevel stelselmatige observatie ex artikel 126g Sv af te geven met het oog op het vastleggen van de locatiegegevens die het geautomatiseerde werk in kwestie genereert.

[529] Zie nogmaals paragrafen 3.11 en 4.3 hierboven.

[530] Zie Inspectie Justitie en Veiligheid, *Verslag toezicht wettelijke hackbevoegdheid politie 2020*, Den Haag: Inspectie Justitie en Veiligheid 2021, p. 10-11.

6. Samenvatting, conclusie en aanbevelingen

6.1. Samenvatting

De vraag die in dit onderzoek centraal heeft gestaan is of de wijze waarop het OM toepassing geeft aan de bevoegdheid tot onderzoek in een geautomatiseerd werk voldoet aan de daarvoor geldende wettelijke voorschriften en de beginselen van proportionaliteit, subsidiariteit en behoorlijkheid, en of het toezicht op de uitvoering daarvan toereikend is.

Die vraag is onderzocht aan de hand van de volgende deelvragen:

1. Welk normatief kader is op basis van relevante verdragsbepalingen, het Wetboek van Strafvordering en overige wet- en regelgeving, jurisprudentie, literatuur alsmede de beginselen van proportionaliteit en subsidiariteit, van toepassing op de beslissing tot het uitvoeren van onderzoek in een geautomatiseerd werk en het toezicht van de zijde van het OM daarop?
2. In hoeverre en op welke gronden wordt tot toepassing van de bevoegdheid tot het uitvoeren van onderzoek in een geautomatiseerd werk overgegaan en wat zijn hierbij de gehanteerde criteria en procedurele waarborgen?
3. Hoe wordt door het OM de controle (tijdens en achteraf) op de inzet van de bevoegdheid nader vormgegeven?
4. Op welke wijze wordt de verantwoordelijkheid van de officier van justitie voor het onderzoek in een geautomatiseerd werk en het toezicht op de uitvoering daarvan in de praktijk en in het concrete geval vormgegeven?
5. Welke rol speelt de politie, in het bijzonder het technische team in de praktijk bij de beslissing tot het uitvoeren van onderzoek in een geautomatiseerd werk en het toezicht daarop? Hoe verhoudt deze rol zich tot de taakverdeling tussen politie en OM, waarbij de officier van justitie de leiding heeft over en toezicht houdt op het opsporingsonderzoek dat wordt uitgevoerd door opsporingsambtenaren?
6. Hoe geeft de officier van justitie vorm en inhoud aan zijn schakelfunctie tussen enerzijds het technische team dat daadwerkelijk binnendringt en onderzoekshandelingen verricht in het geautomatiseerde werk en anderzijds het tactische team van de politie dat het opsporingsonderzoek verricht in de strafzaak in het kader waarvan wordt binnengedrongen in het geautomatiseerde werk?

Deze eindrapportage betreft (uitsluitend) de werkwijze van het OM over de jaren 2019, 2020 en 2021. Het onderzoek is niet alomvattend geweest: van de zaken tijdens de onderzoeksperiode waarin door het OM is besloten tot de uitvoering van onderzoek in een geautomatiseerd werk zijn door de onderzoekers negen uitvoerig bestudeerd. Van de overige zaken is niet of slechts globaal kennisgenomen. De resultaten van het onderzoek zijn weergegeven in de hoofdstukken 3 tot en met 5. In deze paragraaf worden de belangrijkste bevindingen samengevat. Voor een compleet overzicht van alle onderzoeksresultaten wordt verwezen naar de desbetreffende hoofdstukken. In deze samenvatting wordt de volgorde van de hiervoor weergegeven onderzoeksvragen aangehouden.

6.1.1. Het normatief kader (deelvraag 1)

Ter beantwoording van de vraag naar het normatieve kader waarbinnen het OM opereert, is in hoofdstuk 3 een schets gegeven van de regels en waarborgen die de uitvoering van onderzoek in een geautomatiseerd werk omringen. Het betreft uitsluitend een bespreking van het nationaalrechtelijke kader voor zover dat is toegesneden op het hier besproken onderzoek. Deze bespreking verantwoordt tevens de items die in dit toezichtonderzoek (in het bijzonder het dossieronderzoek) zijn getoetst.
De normen die zijn neergelegd in het Besluit onderzoek in een geautomatiseerd werk (Bogw) dragen volgens de minister een kaderstellend karakter en laten ruimte voor invulling in de praktijk. Niettemin maakt de schets van dit regelkader duidelijk dat de bevoegdheid die in de artikelen 126nba lid 1, 126uba lid 1 en 126zpa lid 1 Sv aan de officier van justitie is toegekend

(op sommige punten) betrekkelijk minutieus is geregeld. Dat bergt het risico van een zekere starheid in zich, die het OM beperkt in de ruimte om in te spelen op nieuwe ontwikkelingen of om rekening te houden met de omstandigheden van het geval.

6.1.2. Het beleid omtrent de besluitvorming (deelvraag 2)

De procedure waarbinnen en de gronden waarop de bevoegdheid wordt ingezet zijn (thans) door het OM nader vormgegeven door de 'Instructie voor de inzet van de bevoegdheid ex artt. 126nba, 126uba, 126zpa en 126ffa Sv' (hierna wederom: de Instructie) en de Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv, *Stcrt.* 2019, 10277, afkomstig van het College van procureurs-generaal. Bij aanvang van de onderzochte periode (maart 2019) bestond de Instructie nog niet en was het werkproces omschreven in een interne notitie van 1 maart 2019. Op 15 oktober 2021 is de Instructie in werking getreden. Naar de mededelingen van het OM beschrijft deze Instructie adequaat het werkproces waaraan vanaf 1 maart 2019 uitvoering is gegeven.
Volgens de Instructie is met inachtneming van de hiërarchische lijnen binnen het OM een daartoe aangewezen officier van justitie, de digit-officier, exclusief verantwoordelijk voor de uitvoering door Digit, het technische team van de landelijke eenheid van de Nationale politie, van onderzoek in een geautomatiseerd werk. Uitsluitend aan de digit-officier worden de kennis en besluitvorming toevertrouwd aangaande de daarbij door Digit toegepaste methodieken. Deze strikte scheiding tussen de werkzaamheden van de digit-officier en de zaaksofficier correspondeert met de in het Bogw voorgeschreven scheiding tussen enerzijds het technische team, Digit, dat onder leiding van de digit-officier opereert, en anderzijds het tactische team, dat onder het gezag van de zaaksofficier opsporingsonderzoek uitvoert in de strafzaak waarin de bevoegdheid wordt uitgeoefend.

Tot inzet van de bevoegdheid wordt niet overgegaan alvorens de stappen in de Instructie zijn doorlopen. Binnen dat kader wordt de inzet van de bevoegdheid getoetst aan de wettelijke criteria, waarbij uitvoerig stilgestaan wordt bij de vraag of er alternatieven voorhanden zijn die minder ingrijpen in de persoonlijke levenssfeer van de betrokkene(n). De vragen naar de noodzaak, het verwachte resultaat en het afbreukrisico, alsook het risico voor het geautomatiseerde werk worden telkens uitvoerig onder ogen gezien.
Het onderzoek heeft laten zien dat in de loop der tijd de bevoegdheid in steeds meer zaken wordt ingezet maar dat het nog gaat om een relatief beperkt aantal zaken. Van een grootschalig gebruik is geen sprake.

In de Instructie is een essentiële rol toegekend aan de Centrale toetsingscommissie (CTC). Het bestaan van de CTC en haar werkzaamheden zijn gegrond op de Aanwijzing opsporingsbevoegdheden, nr. 2014A009, *Stcrt.* 2014, 24442, afkomstig van het College van procureurs-generaal. Deze aanwijzing voorziet echter niet in een rol van de CTC in het hiervoor beschreven werkproces voor de uitoefening van de bevoegdheid ex artikel 126nba Sv. De Aanwijzing opsporingsbevoegdheden is daarmee al drie jaar niet in overeenstemming met de mededelingen van de minister bij de parlementaire behandeling van de Wet computercriminaliteit III en de nota van toelichting op het Bogw. Bovendien strookt deze aanwijzing evenmin met de uitvoeringspraktijk. De Aanwijzing opsporingsbevoegdheden correspondeert evenmin met de Instructie.

De Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv strookt met het in de Kamerstukken weergegeven uitgangspunt van de minister van Justitie en Veiligheid, te weten dat in afwachting van de verdere ontwikkeling van het internationaalrechtelijke kader voor de uitoefening van rechtsmacht bij de bestrijding van computercriminaliteit zelfstandig moet kunnen worden opgetreden om te voorkomen dat het internet een vrijplaats wordt voor criminaliteit. Dit kan met zich brengen dat opsporingshandelingen (moeten) worden verricht met betrekking tot gegevens die niet in Nederland zijn opgeslagen, aldus de minister.

Geconstateerd kan worden dat de Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv correspondeert met dit door de minister verwoorde uitgangspunt, zonder dat op voorhand moet worden geoordeeld dat de inhoud van deze aanwijzing zich naar de huidige stand van zaken niet verdraagt met het internationale recht. Voor verdergaande toetsing bestaat geen aanleiding.

6.1.3. Het beleid omtrent de controle op de uitoefening van de bevoegdheid (deelvraag 3)

De Instructie schrijft voor dat binnen het OM een landelijk officier van justitie voor *digital intrusion* wordt aangesteld. Deze functionaris is in deze rapportage steeds 'de digit-officier' genoemd. De reden voor het aanstellen van deze functionaris is blijkens de Instructie dat de toepassing van de bevoegdheid ex artikel 126nba Sv specialistische (technische) kennis vergt in een mate waarvan niet kan worden verwacht dat iedere officier van justitie daarover beschikt. Met die aanstelling wordt tevens beoogd te waarborgen dat het tactische team en de zaaksofficier van justitie geen invloed kunnen uitoefenen op de wijze waarop het technische team (Digit) het bevel ex artikel 126nba Sv uitvoert. De digit-officier oefent met inachtneming van het bepaalde bij of krachtens het Wetboek van Strafvordering en de Politiewet 2012 en in overeenstemming met het Bogw het gezag uit over Digit.

De digit-officier bepaalt de kaders waarbinnen Digit uitvoering geeft aan de bevoegdheid tot het binnendringen van een geautomatiseerd werk en het verrichten van onderzoekshandelingen. Deze kaders omvatten ook de wijze van verbaliseren van de door Digit verrichte handelingen. De digit-officier legt in voorkomende gevallen voorgenomen methodieken of handelingen voor aan de rechercheofficier van justitie van het landelijk parket.

De digit-officier bepaalt in overleg met de teamleiding van Digit, aan de hand van de beleidsprioriteiten, de operationele prioriteiten bij de uitvoering van de bevoegdheid ex artikel 126nba Sv. Naast het hieronder te noemen beleid omtrent geheimhoudersgegevens zijn er geen andere dan de hierboven genoemde formele beleidsinstrumenten die de controle op de inzet van de bevoegdheid nader invullen. Of de bestaande instrumenten afdoende zijn, is afhankelijk van de hierna te bespreken uitvoeringspraktijk. Op deze plek geeft deze vaststelling geen aanleiding tot nadere opmerkingen.

Geheimhoudersgegevens en het verschoningsrecht

Artikel 126aa Sv en het Besluit bewaren en vernietigen niet-gevoegde stukken verplichten tot het vernietigen van gegevens die binnen het bereik vallen van het verschoningsrecht van een professionele geheimhouder, zoals artsen of advocaten. Uit artikel 7 lid 1 en artikel 28 lid 1 Bogw vloeit echter voort dat geen wijzigingen mogen worden aangebracht in de bewijslogging, respectievelijk de gegevens die op een technische infrastructuur zijn vastgelegd, ongeacht of deze gegevens binnen het bereik van een verschoningsrecht vallen. Deze bepalingen beogen de betrouwbaarheid, integriteit en herleidbaarheid van de bij het onderzoek in een geautomatiseerd werk verkregen gegevens te waarborgen.

Met het oog op het garanderen van de betrouwbaarheid, integriteit en herleidbaarheid van de bij het onderzoek in een geautomatiseerd werk verkregen gegevens, heeft de digit-officier volgens een door het OM op 18 december 2020 vastgestelde interne notitie beslist dat – vanwege de specifieke toepasselijkheid van het Bogw op de uitoefening van de bevoegdheid van de artikelen 126nba, 126uba en 126zpa Sv – de bepalingen van het Bogw voorrang hebben op de bepalingen in het Besluit bewaren en vernietigen niet-gevoegde stukken. LP Digit hanteert in vervolg hierop beleidsregels. Ingeval communicatie waaraan een professionele geheimhouder deelneemt bij onderzoek in een geautomatiseerd werk wordt onderschept, wordt deze communicatie (in de vorm van elektronische gegevens) in beginsel onveranderd geregistreerd en bewaard op de technische infrastructuur van Digit. Bij overdracht van de gegevens aan het tactische team is het in beginsel aan een medewerker geheimhouders om – onder verantwoordelijkheid van de zaaksofficier van

justitie – de gegevens waarover het verschoningsrecht zich uitstrekt te filteren. Niet eerder dan na deze filtering worden de gegevens aan de leden van het tactische team die met het opsporingsonderzoek zijn belast voor kennisneming ter beschikking gesteld.
Problematisch aan het in de notitie verwoorde standpunt van de digit-officier, en daarmee ook aan het op dit terrein geïntroduceerde beleid, is dat het hier niet (uitsluitend) gaat om conflicterende rechtsregels van gelijke rangorde. De vernietiging van gegevens waarover het verschoningsrecht zich uitstrekt wordt voorgeschreven door een bepaling uit het Wetboek van Strafvordering, te weten artikel 126aa lid 2, dat van hogere rangorde is dan het Bogw. De artikelen 4 en 4a van het Besluit bewaren en vernietigen niet-gevoegde stukken werken dit voorschrift slechts nader uit. Het staat de digit-officier alleen al om die reden niet vrij om vast te stellen dat het Bogw, als de meer specifieke regeling, prevaleert boven de bepalingen van het Besluit bewaren en vernietigen niet-gevoegde stukken.

Het komt de onderzoekers voor dat de hiervoor beschreven ongerijmdheid in de regelgeving de aandacht behoeft van de minister en dat daarin niet, althans niet op langere termijn, kan worden voorzien door uitsluitend beleidsregels van het OM. De onderzoekers achten het raadzaam om in dit verband een (wettelijke) grondslag te geven aan een regisserende rol voor de rechter-commissaris. In afwachting van nieuwe regelgeving zou (ook) het OM erop kunnen aansturen de rechter-commissaris een regisserende rol toe te kennen.
De kwestie zou bovendien onderdeel moeten zijn van het bredere debat over de wijze waarop het verschoningsrecht bij de uitoefening van bijzondere opsporingsbevoegdheden in acht wordt genomen en over de methode van het (selectief) bewaren c.q. vernietigen van digitale gegevens waarop het verschoningsrecht (mogelijk) van toepassing is.

6.1.4. De concrete uitvoeringspraktijk (deelvraag 4)

Hieronder worden de belangrijkste bevindingen ten aanzien de uitvoeringspraktijk samengevat. Voor een uitgebreide beschrijving van de uitvoeringspraktijk wordt verwezen naar hoofdstuk 5.

De organisatie van het werkproces
Het werkproces zoals dat wordt uitgevoerd door de digit-officier en de digit-parketsecretaris, beiden werkzaam binnen het OM-onderdeel 'LP Digit', vindt plaats in overeenstemming met de Instructie voor de inzet van de bevoegdheid ex artt. 126nba, 126uba, 126zpa en 126ffa Sv. LP Digit vormt een gespecialiseerd onderdeel van het (landelijk parket van het) OM, waaraan dienovereenkomstige, hoge eisen worden gesteld. De personele invulling van de functies van de digit-officier en digit-parketsecretaris is wat dit betreft geheel op orde.
Mede doordat over de wijze waarop het onderzoek in een geautomatiseerd werk wordt uitgevoerd – ook binnen het OM – strikte geheimhouding wordt betracht, bestaat het gevaar dat veel kennis en informatie vrijwel uitsluitend zijn belegd bij LP Digit en Digit. Die stand van zaken bergt organisatorische risico's in zich, zoals het verlies van essentiële kennis bij het onverhoopte uitvallen van de digit-officier en de digit-parketsecretaris, alsmede het gevaar van onvoldoende gecontroleerd, solistisch optreden. Bij het toezicht onderzoek is echter niet gebleken van een organisatorische kwetsbaarheid, en net zomin van solistisch optreden van de digit-officier en de digit-parketsecretaris. Veel kennis en ervaring van LP Digit is vastgelegd in (door de rechercheofficier geaccordeerde) notities en aantekeningen. Het toezicht dat door de landelijke rechercheofficier(en) op LP Digit wordt uitgeoefend is toereikend.

De besluitvorming omtrent de inzet van de bevoegdheid
De verschillende voorgeschreven stappen in het besluitvormingsproces bleken in alle onderzochte zaken telkens vastgelegd in het nba-dossier.
In alle gevallen waarin de bevoegdheid van artikel 126nba Sv is uitgeoefend, is de gerezen verdenking voldoende geconcretiseerd in het projectvoorstel (i.e. het proces-verbaal van aanvraag, met bijlagen), alsook in de adviesaanvraag aan de CTC en in het advies van de

CTC zelf. Bovendien is in die documenten telkens uitvoerig stilgestaan bij de vraag of er alternatieven voorhanden zijn die minder ingrijpen in de persoonlijke levenssfeer van de betrokkene(n). De vragen naar de noodzaak, het verwachte resultaat en het afbreukrisico, alsook het risico voor het geautomatiseerde werk zijn nadrukkelijk (en telkens uitvoerig) onder ogen gezien. De daaraan gewijde passages betreffen geen routinematige 'standaardbeschouwingen'.
Bovendien is in het toezichtonderzoek nagegaan of de vorderingen aan de rechter-commissaris tot het verlenen van een machtiging voor het bevel ex artikel 126nba Sv, alsmede dat bevel zelf, ook overigens voldeden aan de eisen die de wet daaraan stelt. Datzelfde geldt voor de verlenging, wijziging of aanpassing van een en ander, indien van toepassing. Over het algemeen is vastgesteld dat de vorderingen en de bevelen correspondeerden met elkaar en met de machtigingen. De vorderingen en de bevelen voldeden aan de wettelijke voorschriften. Wel zijn een betrekkelijk gering aantal onvolkomenheden en bijzonderheden geconstateerd. Het verdient aanbeveling om de informatie waarvan de wet voorschrijft dat die wordt opgenomen in het bevel, zo concreet mogelijk te omschrijven.

De uitvoering van het bevel

In de onderzochte zaken zijn enkele bijzonderheden geconstateerd met betrekking tot de uitvoering van het bevel (zie ook de verschillende deelaspecten hieronder). In veel gevallen leidt dit niet zonder meer tot het oordeel dat daarmee de inzet niet naar behoren of niet zorgvuldig was. In twee onderzochte gevallen, waarin is binnengedrongen in een ander geautomatiseerd werk dan in het bevel is omschreven, is echter wel sprake van een onvolkomenheid.
Daarnaast heeft de Inspectie over 2021 enkele gevallen geconstateerd waarin op het moment dat Digit onderzoekshandelingen verrichtte, deze handelingen (nog) geen basis hadden in een bevel van de officier van justitie.
Op deze plaats verdient opmerking dat het opnemen van vertrouwelijke communicatie (OVC) in combinatie met het onderzoek in een geautomatiseerd werk in de praktijk bijzondere aandacht heeft en ook verdient. Anders dan bij reguliere OVC ex artikel 126l Sv, waarbij een microfoon (een 'bug') wordt geplaatst op een vaste plek (in een woning bijvoorbeeld), kan OVC in het kader van artikel 126nba worden ingezet op bijvoorbeeld een mobiele telefoon. De OVC bevindt zich in dat geval niet op een gefixeerde locatie, waarbij normaliter de OVC-functie doorlopend aanstaat. De OVC-functie wordt daarom alleen geactiveerd wanneer het geautomatiseerd werk zich op een specifieke plaats bevindt of aanwezig is bij een ontmoeting tussen bepaalde betrokkenen. De CTC is in dit soort zaken van oordeel dat het van belang is om goed te verantwoorden wanneer en bij welke ontmoetingen OVC op de mobiele telefoon wel en niet ingeschakeld wordt, zulks om willekeur te voorkomen. De onderzoekers achten het gericht aan- en uitzetten van de OVC niet problematisch en zelfs aan te bevelen. Op die manier wordt immers voorkomen dat wordt opgenomen op andere plekken dan in het bevel voorzien. Wel dient – om willekeur te voorkomen en disproportioneel optreden tegen te gaan – te worden verantwoord waarom op bepaalde plekken en tijden al dan niet wordt opgenomen. In de onderzochte zaken waarbij sprake was van OVC hebben de onderzoekers geen stukken aangetroffen waaruit de verantwoording achteraf expliciet blijkt. Wel volgt uit de stukken duidelijk dat voorafgaand aan de uitoefening van de bevoegdheid is vastgelegd op welke plekken gesprekken (zullen) worden opgenomen, en waarom.

Binnendringen in een geautomatiseerd werk vergt doorgaans voorbereiding en eventueel de toepassing van methoden die het binnendringen mogelijk maken of faciliteren, bijvoorbeeld doordat op een of andere wijze inloggegevens worden achterhaald waarmee vervolgens kan worden binnengedrongen in een geautomatiseerd werk of doordat een bug wordt geplaatst in een geautomatiseerd werk met behulp waarvan op een later moment (andermaal) wordt binnengedrongen. Er zijn aanzienlijk meer van dergelijke gevallen denkbaar, maar die worden omwille van de afscherming van methodieken hier niet uiteengezet.
In het toezichtonderzoek is meermalen aandacht besteed aan de vraag wat de wettelijke grondslag kan zijn voor het verrichten van dergelijke faciliterende verrichtingen van

de zijde van de politie. Is dat bijvoorbeeld artikel 3 Politiewet, een andere bijzondere opsporingsbevoegdheid dan die van artikel 126nba/uba/zpa Sv, dan wel uitsluitend artikel 126nba/uba/zpa Sv?
De Inspectie heeft geconstateerd dat Digit methodieken waarvan de vraag is of zij zijn voorzien van een wettelijke basis, voorafgaand aan de toepassing ervan overeenkomstig de richtsnoeren van LP Digit voor instemming en ter toetsing voorlegt aan de digit-officier.
Bij het toezichtonderzoek is geconstateerd dat in bepaalde gevallen faciliterende methodieken, als hier bedoeld, zijn toegepast die louter waren gegrond op artikel 3 Politiewet. Het toezichtonderzoek wijst uit dat toetsing door de digit-officier plaatsvindt aan de hand van criteria die in overeenstemming zijn met de wet en de heersende jurisprudentie van de Hoge Raad dienaangaande. Binnen het bestek van het uitgevoerde dossieronderzoek geeft de uitkomst van deze toetsingen de onderzoekers geen reden voor commentaar. De digit-officier heeft aangegeven dat het inmiddels huidige praktijk is dat de faciliterende methoden als hier bedoeld worden gedekt door een bevel ex artikel 126nba Sv.

Het technisch hulpmiddel

De uitvoeringspraktijk van artikel 126nba Sv staat op gespannen voet met het door de minister van Justitie en Veiligheid (in de parlementaire geschiedenis van de Wet computercriminaliteit III en in de toelichting op het Bogw) tot uitdrukking gebrachte uitgangspunt dat bij het uitvoeren van onderzoek in een geautomatiseerd werk in beginsel gebruik wordt gemaakt van een (vooraf) goedgekeurd technisch hulpmiddel.
Weliswaar wijst het toezichtonderzoek uit dat de onderzoekshandelingen in de binnengedrongen geautomatiseerde werken in de meeste zaken zijn verricht met behulp van een technisch hulpmiddel (en dus niet handmatig), dit technisch hulpmiddel is evenwel in slechts een gering aantal zaken (vooraf) goedgekeurd, en in veruit de meeste zaken – met toepassing van artikel 21 lid 4 Bogw – niet ter keuring aangeboden. Om die reden moeten in al deze zaken waarborgen worden getroffen, terwijl de afscherming van het technisch hulpmiddel niet kan plaatsvinden door in het proces-verbaal van inzet te verwijzen naar het keuringsnummer.
Het technisch hulpmiddel waarvan de digit-officier heeft geoordeeld dat het naar zijn aard niet voor keuring geschikt is, betreft een technisch hulpmiddel dat onderdeel is van een commercieel verkregen, kostbaar systeem dat in het toezichtonderzoek de codenaam 'TH Brons' heeft gekregen. Het besluit van de digit-officier om geheel af te zien van de keuring van TH Brons steunt op de geldende regelgeving (artikel 21 lid 4 Bogw). De afwegingen die hieraan ten grondslag liggen zijn op zichzelf zorgvuldig tot stand gekomen en verdedigbaar.

Tot slot over het onderscheid tussen onderzoek door middel van een technisch hulpmiddel en handmatig onderzoek het volgende. Volgens artikel 1 onder f Bogw is een technisch hulpmiddel een "*softwareapplicatie die gegevens detecteert, registreert en transporteert en waarmee onderzoekshandelingen worden verricht ter uitvoering van een bevel*." Bij de uitleg van deze definitie hanteert het OM het criterium van de 'directe betrokkenheid' van een lid van het technische team (Digit) bij het verrichten van onderzoekshandelingen in een geautomatiseerd werk. 'Directe betrokkenheid' doet zich voor wanneer de (handmatige) verrichtingen van de technische opsporingsambtenaar in de plaats komen van één of meer van de drie kenmerken van een technisch hulpmiddel, te weten dat het functionaliteiten bevat voor het automatisch (1) detecteren, (2) registreren en (3) transporteren van gegevens. Indien in een van die fasen directe betrokkenheid van Digit is vereist en het proces (dus) niet volledig automatisch kan plaatsvinden door een functionaliteit van de applicatie, beschouwt het OM het onderzoek in een geautomatiseerd werk als handmatig verricht.
Uit het onderzoek is gebleken dat de definitie van 'technisch hulpmiddel' aan dat begrip onvoldoende richting geeft en dat deze definitie zodoende – afhankelijk van de omstandigheden van het geval – ruimte laat voor uiteenlopende antwoorden op de vraag of de softwareapplicatie die (eventueel) wordt aangewend voor het verrichten van onderzoek in een geautomatiseerd werk als een technisch hulpmiddel moet worden aangemerkt. De nadere omschrijving die het OM aan het begrip 'technisch hulpmiddel' heeft gegeven

betreft een betrekkelijk streng criterium dat, hoewel verdedigbaar, in elk geval (nog immer) tot discussie aanleiding kan geven. Bovendien merkt het OM TH Brons aan als technisch hulpmiddel terwijl de transport van gegevens, hoewel dat technisch wel mogelijk is, (bewust) niet automatisch plaatsvindt.
Naar het oordeel van de onderzoekers valt het aan te bevelen dat iedere applicatie waarmee wordt beoogd in een geautomatiseerd werk onderzoekshandelingen te verrichten en die qua complexiteit verder reikt dan een eenvoudig script waarvan de werking op zichzelf niet hoeft te worden afgeschermd, wordt aangemerkt als technisch hulpmiddel. In dat geval komt routinematig de vraag op of de applicatie zich leent voor (aan het gebruik voorafgaande) keuring en kan daarnaar worden gehandeld. Wanneer daarentegen hogere eisen worden gesteld aan een applicatie wil het als technisch hulpmiddel kunnen worden aangemerkt (zoals de digit-officier propageert), dan heeft dit tot gevolg dat de beoordeling van de keuringsvatbaarheid ervan achterwege blijft, ook in die gevallen waarin er geen overwegende bezwaren bestaan tegen keuring (vooraf dan wel achteraf). De meer functionele uitleg van het begrip 'technisch hulpmiddel' die de onderzoekers voorstellen, heeft als voordeel dat *iedere* applicatie in principe ter keuring kan (moet) worden aangeboden, behoudens indien het gaat om een eenvoudig script (waarvan de werking niet hoeft te worden afgeschermd). De goedkeuring van applicaties vergemakkelijkt de afscherming ervan. De goedkeuring garandeert bovendien de betrouwbaarheid, integriteit en herleidbaarheid van de gegevens die zijn verkregen bij het onderzoek in een geautomatiseerd werk. Het belang van een meer formele omschrijving van het begrip 'technisch hulpmiddel' komt daarmee te vervallen.

Gebruik van commerciële software en van onbekende kwetsbaarheden

De uitvoeringspraktijk van artikel 126nba Sv staat ook op gespannen voet met het door de minister van Justitie en Veiligheid in de wetsgeschiedenis tot uitdrukking gebrachte uitgangspunt dat bij het uitvoeren van onderzoek in een geautomatiseerd werk in beginsel geen gebruik wordt gemaakt van commerciële software waarvan onduidelijk is of die software onbekende kwetsbaarheden exploiteert.
In de meeste zaken waarin een bevel ex artikel 126nba Sv is afgegeven is bij het verrichten van onderzoekshandelingen in een geautomatiseerd werk gebruikgemaakt van TH Brons. Van dit commerciële systeem maakt ook binnendringsoftware deel uit. Aan de toepassing hiervan zijn nadelen verbonden die bij de totstandkoming van de Wet computercriminaliteit III en het Bogw aan de orde zijn geweest. Niet uitgesloten is namelijk dat de binnendringsoftware van het systeem waarvan TH Brons onderdeel is, gebruikmaakt van onbekende kwetsbaarheden (zero-days). Of het systeem daadwerkelijk gebruikmaakt van onbekende kwetsbaarheden en zo ja welke, is de digit-officier en Digit niet bekend omdat de leverancier geen volledig inzicht geeft in de inrichting en werking van het systeem. Het systeem waarvan TH Brons deel uitmaakt, staat in verbinding met de server van de leverancier, terwijl de met behulp van TH Brons verkregen gegevens tijdelijk worden opgeslagen op een voorziening in TH Brons die eveneens in verbinding staat met de server van de leverancier. Werkzaamheden die de leverancier uitvoert kunnen mogelijk zelfs tijdens de daadwerkelijke inzet invloed hebben op de werking en functionaliteiten van TH Brons. Hoewel de leverancier van TH Brons door de AIVD is gescreend en de AIVD geen bezwaar heeft afgegeven, laat de door de politie uitgevoerde (thans: periodieke) toets de mogelijkheid open dat het systeem waarvan TH Brons onderdeel is ook wordt geleverd aan (politie- of inlichtingendiensten of vervolgingsinstanties van) landen die zich schuldig maken aan ernstige schendingen van mensenrechten of internationaal humanitair recht.
Daar staat tegenover dat de aanwending van het systeem waarvan TH Brons onderdeel is, in de onderzochte zaken daadwerkelijk heeft geleid tot onderzoeksresultaten waartoe de inzet van TH Brons strekte. Kort gezegd, het systeem doet wat het moet doen.
De afweging van de hierboven geschetste risico's en bezwaren enerzijds en het belang van de bestrijding van ernstige criminaliteit anderzijds, waarbij aan het tweede prioriteit is gegeven, is binnen het OM centraal en op zichzelf zorgvuldig, namelijk in een uitvoerig afwegingsproces, tot stand gekomen.

Zoals gezegd staat het structurele gebruik van commercieel verkregen binnendringapplicaties op gespannen voet met het hierboven verwoorde uitgangspunt van de minister. Het gebruik van dergelijke binnendringsoftware is op zichzelf verenigbaar met de geldende wettelijke voorschriften en met de beginselen van proportionaliteit, subsidiariteit en behoorlijkheid in individuele zaken. Het probleemveld is voor het overige politiek van aard, zodat hier met de signalering van het voorgaande wordt volstaan.

De procedurele en aanvullende waarborgen

Bij de inzage bleek dat de nba-dossiers niet altijd duidelijkheid verschaften over de aard en de omvang van de door Digit voorgestelde en/of daadwerkelijk getroffen waarborgen. In de rapporten haalbaarheidsonderzoek die aanwezig zijn in de nba-dossiers, wordt met name niet altijd concreet gemaakt welke waarborgen Digit had getroffen. Navraag bij LP Digit gaf meer duidelijkheid over de getroffen waarborgen, maar de vastlegging ervan is globaal.
Bij het dossieronderzoek is gebleken dat de procesdossiers (wel) duidelijk maakten welke waarborgen van de zijde van het tactische team waren genomen. De resultaten van de inzet van opsporingsmiddelen maakten het de rechter en procesdeelnemers mogelijk om de resultaten die waren verkregen door de uitvoering van een bevel ex 126nba Sv te verifiëren. De waarborgen die aan tactische zijde worden getroffen zijn in veel zaken omvangrijk en adequaat.

De logging

Logging (zoals bedoeld in artikel 5 Bogw) behoort in de eerste plaats tot de taken en verantwoordelijkheden van Digit. Artikel 6 Bogw schrijft voor dat logging op zodanige wijze plaatsheeft dat kan worden vastgesteld of een onregelmatigheid heeft plaatsgevonden die van invloed is op de betrouwbaarheid en integriteit van de ter uitvoering van het bevel vastgelegde gegevens op een technische infrastructuur. Naar de mededelingen van de digit-officier voert LP Digit controle uit op de bewijslogging, omdat het daarbij gaat om de vastlegging van de gegevens die eventueel tot het bewijs in de strafzaak kunnen dienen. Op de overige drie vormen van logging (inzetlogging, authenticatie- en autorisatielogging en systeemlogging, zie paragraaf 3.10 hierboven) houdt LP Digit minder direct toezicht omdat dit in eerste instantie een taak is van Digit zelf. Ondanks de door de Inspectie geconstateerde (en door de digit-officier niet betwiste) onvolkomenheden, zoals onvolledige logging, gebrekkige beeldschermopnamen en toetsaanslagenregistratie, acht de digit-officier de toestand niet dermate zorgwekkend dat er aanleiding is voor ingrijpen. Dit standpunt achten de onderzoekers verdedigbaar. De bewijslogging is daarnaast wel op orde, behoudens de signalering van de problematiek van de tijdelijke opslag van de bewijslogging op een voorziening binnen TH Brons zelf. Omdat deze tijdelijke opslaglocatie in verbinding met en onder beheer van de leverancier staat, is onbevoegde toegang tot en oneigenlijk gebruik van de gegevens technisch niet uit te sluiten. In dat geval is niet aan de waarborgen voor beveiligde opslag voldaan.

Uit het onderzoek is gebleken dat de inhoud van het begrip ‘onregelmatigheid’ in artikel 6 (en 23 en 24) Bogw aanleiding kan geven voor discussie. De digit-officier hanteert in dit verband een uitleg waarin alleen die onregelmatigheden die afbreuk doen aan de betrouwbaarheid en de integriteit van de gegevens die kunnen dienen als bewijs in een strafzaak dienen te worden geverbaliseerd. Dat oordeel achten de onderzoekers goed verdedigbaar.

Het opmaken van proces-verbaal

Bij het dossieronderzoek werden aanvankelijk tekortkomingen gezien, met name wat betreft de duur van de periode die is gelegen tussen het onderzoek in een geautomatiseerd werk en de verslaglegging ervan. Hoewel niet in alle zaken, is bij het vervolgonderzoek in meer recente zaken verbetering geconstateerd.
Al met al blijft de betrekkelijk globale en gestandaardiseerde wijze waarop de onderzoekshandelingen van Digit worden omschreven problematisch. Als gevolg daarvan kunnen controle en toezicht hierop slechts zeer beperkt plaatsvinden. De digit-officier heeft

te kennen gegeven dat onder zijn verantwoordelijkheid voor deze wijze van verbalisering is gekozen uit het oogpunt van afscherming van methoden en technieken. Het journaal, dat niet bij de processtukken wordt gevoegd, bevat naar de mededelingen van de digit-officier zodanige informatie dat eventuele vragen van de rechter adequaat kunnen worden beantwoord. Naar het oordeel van de onderzoekers is echter een gedetailleerder proces-verbaal geboden.

De notificatie en de vernietiging van gegevens
LP Digit wijst de zaaksofficieren standaard op het bestaan en de reikwijdte van de notificatieplicht. In geen van de onderzochte zaken heeft notificatie plaatsgehad, omdat het opsporingsonderzoek in geen van de zaken (ten tijde van de onderzoeksperiode) is afgerond.

Geheimhoudersgegevens en het verschoningsrecht
De uitvoeringspraktijk ten aanzien van geheimhoudersgegevens geeft geen aanleiding tot nadere opmerkingen behalve dat in één zaak niet voldoende duidelijk is geworden of de omgang met geheimhoudersgegevens plaatshad overeenkomstig het hiervoor omschreven beleid.

Internationale aspecten van de toepassing van de bevoegdheid
Kort gezegd hebben de onderzoekers geconstateerd dat de door het OM zelf opgestelde Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv niet in alle gevallen een adequate oplossing biedt wanneer de uitoefening van de bevoegdheid van artikel 126nba Sv buiten het grondgebied van Nederland plaatsheeft. In een geval waarin het ging om de ontoegankelijkmaking van een wereldwijd verspreid botnet viel te verdedigen dat voor de ontoegankelijkmaking geen toestemming is gevraagd aan alle landen waarin zich gecompromitteerde geautomatiseerde werken bevonden. Niettemin moet worden geconstateerd dat de Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv niet voorziet in een uitzondering voor een dergelijk geval.

6.1.5. De rol van de politie en de verhouding met de officier van justitie (deelvraag 5)

Op grond van het Bogw mag het bevel van de officier van justitie tot het binnendringen en doen van onderzoek in een geautomatiseerd werk enkel worden uitgevoerd door een technisch team dat onderdeel uit maakt van de landelijke eenheid van Nationale politie. Dit technisch team is een team dat in opsporingsonderzoeken ondersteuning verleent aan de tactische rechercheteams. Voor de onderhavige bevoegdheid is daarvoor een specialistisch team opgericht dat in dit rapport Digit wordt genoemd.

Hoewel uit het onderzoek is gebleken dat in voorkomende gevallen afstemming en rechtstreeks contact bestaat tussen het tactisch team en het technisch team, bepaalt Digit onafhankelijk van het tactisch team op welke wijze uitvoering wordt gegeven aan een bevel ex artikel 126nba Sv. Het tactisch team mag volgens de Instructie geen invloed uitoefenen op het binnendringen in het geautomatiseerd werk en de plaatsing, inzet en verwijdering van een technisch hulpmiddel. De methodieken die Digit gebruikt voor het binnendringen zijn afgeschermd en niet kenbaar voor het tactische team.

De zaaksofficier van justitie heeft de leiding en de eindverantwoordelijkheid over het opsporingsonderzoek waarin de bevoegdheid ex artikel 126nba Sv wordt ingezet. De toepassing van de bevoegdheid wordt door hem geïnitieerd en – na het doorlopen van een besluitvormingsprocedure – ook bevolen. De digit-officier heeft de leiding over en is verantwoordelijk voor de uitvoering van het bevel van de zaaksofficier door Digit.
Uit het onderzoek is gebleken dat Digit niet tot uitvoering overgaat alvorens de digit-officier daarvoor toestemming geeft. De digit-officier dan wel de digit-parketsecretaris is nagenoeg altijd aanwezig tijdens een actie van Digit. Zij zien erop toe dat zij doorlopend worden

geïnformeerd over de status van de inzet en dat zij worden geraadpleegd op relevante beslismomenten. Ook wordt toegezien op de verslaglegging door Digit.
Zowel Digit als het tactisch team nemen de wettelijke taak- en gezagsverdeling tussen de politie en de officier van justitie in acht.

6.1.6. De schakelfunctie van de officier van justitie (deelvraag 6)

Met de aanstelling van een landelijke digit-officier en de toekenning van de bij die functie passende taken en verantwoordelijkheden heeft het OM de door het Bogw voorgeschreven organisatorische scheiding tussen enerzijds het werkproces van het technische team (het uitvoeren van onderzoek in een geautomatiseerd werk) en anderzijds het werkproces van het tactische team (het opsporingsonderzoek) geïmplementeerd binnen de eigen organisatie.
De nota van toelichting op het Bogw schrijft aan de (zaaks)officier van justitie een zogenoemde schakelfunctie voor teneinde samenwerking tussen het technische en tactisch team mogelijk te maken. Volgens de Instructie wordt die schakelfunctie vervuld in het overleg tussen de digit-officier (aanspreekpunt Digit) en de zaaksofficier (aanspreekpunt van het tactische team). Zowel uit de Instructie als uit de praktijk blijkt dat de schakelfunctie over twee schakels loopt. De zaaksofficier en de digit-officier informeren elkaar over en weer en beleggen de informatie bij hun eigen teams. Ook kan gezamenlijk overleg met beide teams plaatsvinden.

Uit het onderzoek is gebleken dat rechtstreeks contact tussen Digit en het tactische team voorkomt in de praktijk, zonder tussenkomst van de zaaksofficier, doorgaans als Digit tijdens de daadwerkelijke uitvoering van onderzoek in een geautomatiseerd werk over bepaalde informatie moet beschikken. De digit-officier heeft in die gevallen meer betrokkenheid omdat het gebruikelijk is dat hij op cruciale momenten tijdens een actie van Digit op locatie aanwezig is. De zaaksofficier heeft daarentegen niet noodzakelijkerwijs steeds diezelfde mate van betrokkenheid bij een actie van Digit, zodat het praktisch minder goed uitvoerbaar is om het contact tussen Digit en het tactisch team telkens (tevens) via de zaaksofficier te laten verlopen. Dit vormt volgens de onderzoekers geen probleem. Door de nauwe betrokkenheid van de digit-officier en digit-parketsecretaris is de schakelfunctie voldoende geborgd. Van de zijde van het OM bestaat voldoende controle op hetgeen met de schakelfunctie wordt beoogd, namelijk vermijden dat het tactische team (op oneigenlijke gronden) invloed kan uitoefenen op het binnendringen in het geautomatiseerde werk en de plaatsing, inzet en verwijdering van een technisch hulpmiddel. Hiermee niet in strijd is de vaststelling van de Inspectie Justitie en Veiligheid dat tijdens acties in 2019 en 2021 enkele malen direct (telefonisch) contact heeft plaatsgevonden tussen Digit en leden van het tactisch team.

6.2. Conclusie

De beantwoording van de vraag of de wijze waarop het OM toepassing geeft aan de bevoegdheid tot onderzoek in een geautomatiseerd werk voldoet aan de in artikel 126nba Sv opgenomen voorschriften en de beginselen van proportionaliteit, subsidiariteit en behoorlijkheid, en of het toezicht op de uitvoering daarvan toereikend is, luidt als volgt.

De wijze waarop het OM toepassing geeft aan de bevoegdheid tot het uitvoeren van onderzoek in een geautomatiseerd werk voldoet ten aanzien van de onderzochte gevallen tijdens de onderzoeksperiode 2019-2021 grosso mode aan de wettelijke voorschriften. In alle onderzochte zaken is op zichzelf voldaan aan beginselen van proportionaliteit en subsidiariteit. Niettemin zijn er bij het toezichtonderzoek enkele onvolkomenheden geconstateerd die in aanmerking komen voor verbetering en zijn er knelpunten gesignaleerd.

6.3. Aanbevelingen

In de samenvatting en conclusie ligt besloten dat de onderzoekers van oordeel zijn dat het OM bij de uitoefening van zijn taak ten aanzien van de onderzochte gevallen tijdens de onderzoeksperiode 2019-2021 de wettelijke voorschriften grosso modo wel, doch op een aantal punten nog niet naar behoren handhaaft of uitvoert.

Op grond van artikel 122 RO is de PG-HR bevoegd de minister van dit oordeel in kennis te stellen, waarmee de ministeriele verantwoordelijkheid wordt geactiveerd. Daarbij is het primair aan de minister om te bepalen of het oordeel van de PG-HR aanleiding geeft om stappen te ondernemen en welke stappen dat zouden moeten zijn. De PG-HR kan wel van de gelegenheid gebruikmaken suggesties te doen die de minister bij de besluitvorming in overweging kan nemen. Daarbij behoort aan de kant van de PG-HR de nodige terughoudendheid te worden betracht. Met inachtneming van die terughoudendheid kunnen de volgende aanbevelingen worden gedaan:

1. Aanbevolen wordt om de Aanwijzing opsporingsbevoegdheden, nr. 2014A009, Stcrt. 2014, 24442, aan te passen zodat deze voldoet aan het in hoofdstuk 3 genoemde normatief kader en de in hoofdstuk 4 genoemde Instructie, in het bijzonder wat betreft het opnemen van de rol van de CTC ten aanzien van de bevoegdheid onderzoek in een geautomatiseerd werk.
2. Het verdient aandacht om de informatie waarvan de wet voorschrijft dat die wordt opgenomen in het bevel, zo concreet mogelijk te omschrijven.
3. Het verdient (blijvend) aandacht om de inzet van OVC met betrekking tot (mobiele) geautomatiseerde werken te verantwoorden, bijvoorbeeld in processen-verbaal.
4. Het verdient aanbeveling om het begrip ‘technisch hulpmiddel’ uit te leggen als: iedere applicatie waarmee wordt beoogd in een geautomatiseerd werk onderzoekshandelingen te verrichten en die qua complexiteit verder reikt dan een eenvoudig script waarvan de werking op zichzelf niet hoeft te worden afgeschermd.
5. Het verdient aanbeveling het opmaken van proces-verbaal tijdiger en volledi ger, dat wil zeggen: voorzien van meer concrete informatie, te doen plaatsvinden. Onder andere de verslaglegging over de door Digit getroffen waarborgen verdient aandacht.
6. Het verdient aanbeveling tijdens het daadwerkelijke binnendringen en verrichten van onderzoekshandelingen in een geautomatiseerd werk (‘een actie’) de locatiegegevens van het binnengedrongen geautomatiseerde werk te loggen, en indien en voor zover die actie van langere duur is daartoe een bevel stelselmatige observatie ex artikel 126g Sv af te geven met het oog op het vastleggen van de locatiegegevens die het geautomatiseerde werk in kwestie genereert.
7. Het verdient aanbeveling om (eventueel in afwachting van nieuwe regelgeving) de rechter-commissaris een regisserende rol toe te kennen bij het filteren van gegevens die afkomstig zijn van geheimhouders.
8. Het verdient aanbeveling om te bezien of de Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv dient te worden aangepast om te voorzien in de situatie waarin een wereldwijd netwerk van een grote hoeveelheid botnets wordt ontmanteld.

Procureur-generaal bij de Hoge Raad
der Nederlanden

Korte Voorhout 8
Postbus 20303
2500 EH Den Haag

info@hogeraad.nl
www.hogeraad.nl