OPENBAAR MINISTERIE

Parket-Generaal

Postbus 20305, 2500 EH Den Haag

[redacted]

Prins Clauslaan 16
2595 AJ Den Haag
T +31 88 699 11 00
www.om.nl

Datum 2 februari 2026
Onderdeel Bestuurlijke en Juridische Zaken
Ons kenmerk PAG/BJZ/27533 - 475894
Contactpersoon [redacted]
Doorkiesnummer(s) 088 – 699 11 17
E-mail [redacted]@om.nl
Uw kenmerk [redacted]
Bijlage(n) 1) Inventarislijst; 2) Documenten.
Onderwerp Nieuw (deel)besluit op bezwaar – onderdeel 2 Woo-verzoek

Bij beantwoording de datum en ons kenmerk vermelden.

Geachte [redacted]

In navolging van de eerste nieuwe deelbesluit op bezwaar, d.d. 5 december 2025 en met kenmerk PAG/BJZ/27533 – 460853, neem ik hierbij een besluit op onderdeel 2 van het Wob-verzoek van [redacted] van 25 januari 2022.

Voor het procesloop in deze procedure verwijs ik naar voornoemd eerder deelbesluit op bezwaar.

1. Onderdeel 2 van uw Wob-verzoek van 25 januari 2022
In onderdeel 2 van uw Woo-verzoek heeft u om openbaarmaking gevraagd van 'de documenten die zien op de volgende belangrijke besluiten en aangelegenheden':

i. Alle documenten die zijn vervaardigd in het kader van- of in reactie op het Verslag toezicht wettelijke hackbevoegdheid politie 2019;
ii. Alle documenten die zijn vervaardigd in het kader van- of in reactie op het Verslag toezicht wettelijke hackbevoegdheid politie 2020;
iii. Alle documenten die zijn vervaardigd of gedeeld in het kader van- of in voorbereiding op het Verslag toezicht wettelijke hackbevoegdheid politie 2021;

iv. Alle documenten die zijn vervaardigd in het kader van- of in reactie op de WODC Evaluatie Wet Computercriminaliteit III: de bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk;
v. Alle documenten die zien op de totstandkoming van- en beleidsvorming naar aanleiding van aanwijzingsbesluiten, haalbaarheidsonderzoeken, plannen van aanpak, resultaten van testen in een proefopstelling en processen-verbaal in het kader van de hackbevoegdheid en de digitale opsporing in algemene zin;
vi. Alle documenten die zien op de self-assessment door het DIGIT van de beveiligingsmaatregelen die gelden bij het toepassen van de hackbevoegdheid en de verwerking en analyse van gegevens;
vii. Alle documenten die zien op de werkinstructies bij het toepassen van de bevoegdheden uit de Wet Computercriminaliteit III;
viii. Alle documenten die zien op besluitvorming- en toetsingscriteria bij de keuring van technische hulpmiddelen.
   - In het bijzonder het door de minister van Justitie en Veiligheid goedgekeurde keuringsprotocol.
ix. Alle documenten die zien op het beleid bij de verwerking van persoons- en locatiegegevens door de opsporingsdiensten.
   - In het bijzonder de stukken die zien op de uitvoering van- en beleid bij de uitvoering van de in de wet gestelde eisen aan de digitale gegevensverwerking:
      1. Algemene verordening gegevensbescherming (AGV);
      2. Wet politiegegevens (Wpg);
      3. Wet justitiële en strafvorderlijke gegevens (Wsjg);
x. Alle documenten die zien op (wijzigingen in) het beleid bij de toepassing van de bevoegdheden uit de Wet Computercriminaliteit III en de verwerking van digitale gegevens; en
xi. de documenten waar verzoeker redelijkerwijs niet bekend mee kan zijn, maar die wel bestaan en vallen binnen de hierboven uiteengezette tijdsvakken en beleidsterreinen, wordt ook uitdrukkelijk verzocht om openbaarmaking (door toezending).

Bij brief van 28 mei 2025 en met kenmerk PaG/BJZ/28005/403318 is u verzocht om een specificering van hetgeen is verzocht. Hierbij is aangegeven dat:

1. subonderdeel vii wordt opgevat als een verzoek om openbaarmaking van de werkinstructies aangaande de toepassing van de artikelen 126nba/uba/zpa Wetboek van Strafvordering;
2. subonderdelen viii en ix zo worden opgevat, dat de gevraagde documenten steeds te relateren zijn aan de toepassing van de bevoegdheden neergelegd in de artikelen 126nba/uba/zpa Wetboek van Strafvordering; en

3. subonderdeel x zo wordt opgevat dat de gevraagde documenten steeds te relateren zijn aan de toepassing van de bevoegdheden neergelegd in de artikelen 126nba/uba/zpa Wetboek van Strafvordering. Tot slot is ter zake dit onderdeel verzocht of u onder 'beleid' verstaat 'formele documenten, zoals richtlijnen en werkinstructies'? Daarnaast is u verzocht wat u precies verstaat onder de 'verwerking van digitale gegevens'.

Bij e-mailbericht van 3 juni 2025 heeft u hierop gereageerd en daarbij aangegeven dat u de wijze waarop uw verzoek wordt opgevat 'in grote lijnen kunt volgen, maar dat u daar pas echt iets over kunt zeggen als u het ("officiële") antwoord op het oorspronkelijke verzoek heeft ontvangen'.
In reactie op hetgeen gestelde onder 3 van het specificeringsverzoek (ter zake subonderdeel x) heeft u gesteld dat u de hierin verwoorde lezing van uw verzoek door het Openbaar Ministerie als een 'vernauwing' van het verzoek ziet, die niet aansluit bij uw verzoek om 'alle documenten, inclusief richtlijnen en werkinstructies. U bevestigt aangaande dit subonderdeel x wel dat het gaat om 'digitale gegevens in het kader van de Wet Computercriminaliteit III'.

Bij e-mailbericht van 18 juni 2025 heeft de Woo-behandelaar aan u een reactie gstuurd, waarin is aangegeven dat de specificering niet is ingegeven met het doel om het verzoek in omvang te beperken, maar juist om de zoekslag zorgvuldig te kunnen uitvoeren (oftewel: teneinde om uw verzoek in behandeling te kunnen nemen). Derhalve zijn nog twee explicite specificeringsvoorstellen aan u gedaan, te weten:

- specificeren van de term 'beleid'. Hierbij is aangegeven dat uw verzoek terzake subonderdeel x wordt opgevat als (de totstandkoming van) de 'formele documenten' (te weten: regels, richtlijnen, werkwijzen, et cetera) met een zaaksoverstijgend karakter, waarbij het niet gaat om de 'formele' status van het document, maar om het zaaksoverstijgende karakter an het document, dat het tot beleid maakt; en
- specificeren van de reikwijdte van het beleid: aan u is nogmaals de vraag voorgelegd of het u gaat om de toepassing van de bevoegdheden als neergelegd in de artikelen 126nba/uba/zpa WvSv.

Bij e-mailbericht van 19 juni 2025 heeft u hierop instemmend geantwoord 'ja, het gaat om formele documenten (zoals in uw uitleg beschreven), en ja, het gaat om toepassing van de bevoegdheden van artikelen 126nba/uba/zpa WvSv.'.

3. Zoekslag en inventarisatie
Naar aanleiding van het gespecificeerde verzoek heb ik een zoekslag uitgevoerd binnen het Landelijk Parket. Hiertoe is uitvraag gedaan bij het Team Landelijke Taken, in het bijzonder de Landelijk officier van justitie voor Digital Intrusion (hierna: DIGIT) en de senior juridisch adviseur DIGIT. Deze medewerkers van het

Team Landelijke Zaken met de DIGIT-portefeuille zijn bij alle onderwerpen betrokken die raken aan beleid rondom de Wet Computercriminaliteit III (hierna: CCIII). Alle documenten worden - gelet op de bijzondere gevoeligheid van deze informatie - door de portefeuillehouders DIGIT op een extra beveiligde omgeving opgeslagen. Voor de zoekslag zijn alle mappen binnen deze extra beveiligde omgeving handmatig doorzocht, waarbij alle documenten in alle DIGIT-mappen handmatig zijn bekeken.
De mappen zijn per subonderdeel van (dit onderdeel van) uw verzoek doorzocht. In de bijgevoegde inventarislijst is steeds per subonderdeel aangegeven welke documenten zijn aangetroffen en hoe deze zijn beoordeeld. Hierbij is eveneens uw verzoek om de gevraagde informatie onder subonderdeel xi meegenomen.

In totaal zijn 45 documenten aangetroffen die onder de reikwijdte van uw verzoek vallen.

4. Besluit
Ik besluit ten aanzien van onderdeel 2 van uw Woo-verzoek de informatie waarover ik beschik (gedeeltelijk) openbaar te maken. Op de inventarislijst is per document aangegeven of de informatie geheel of gedeeltelijk openbaar wordt gemaakt. Mocht een document geheel of gedeeltelijk worden geweigerd, dan wordt eveneens per document vermeld welke uitzonderingsgronden ex artikelen 5.1 en 5.2 van de Woo zijn toegepast. De motivering van de toepassing van de uitzonderingsgronden vermeld ik in het navolgende onderdeel van dit besluit.

5. Motivering
5.1. Het belang van de eerbiediging van de persoonlijke levenssfeer (artikel 5.1, tweede lid, aanhef en onder e, van de Woo)
Op grond van artikel 5.1, tweede lid, aanhef en onder e van de Woo blijft het verstrekken van informatie achterwege voor zover het belang van openbaarmaking niet opweegt tegen het belang van de eerbiediging van de persoonlijke levenssfeer van de betrokkene(n).

Uit de Woo volgt dat de persoonlijke levenssfeer geen absolute bescherming geniet, maar onder omstandigheden moet wijken voor het publieke belang van het openbaar maken van informatie. Om deze uitzonderingsgrond te kunnen inroepen, moet worden vastgesteld of het belang van de eerbiediging van de persoonlijke levenssfeer in het onderhavige geval aan de orde is en zo ja, dat het belang bij openbaarmaking niet opweegt tegen het belang van bescherming van de persoonlijke levenssfeer.

Voor zover het de namen van ambtenaren betreft is hierbij het volgende van belang. Waar het gaat om het beroepshalve functioneren van ambtenaren, kan in beginsel slechts in beperkte mate een beroep worden gedaan op het belang van

eerbiediging van hun persoonlijke levenssfeer. Dit ligt anders indien het gaat om het openbaar maken van namen en andere persoonsgegevens van ambtenaren. Namen zijn immers persoonsgegevens en het belang van eerbiediging van de persoonlijke levenssfeer kan zich tegen het openbaar maken daarvan verzetten. Daarbij is van belang dat het hier niet gaat om het opgeven van een naam aan een individuele burger die met een ambtenaar in contact treedt, maar om openbaarmaking van de naam in de zin van de Woo. Ook de Afdeling Bestuursrechtspraak van de Raad van State (hierna: de Afdeling) heeft door precisering van haar jurisprudentie bevestigd dat het belang van de persoonlijke levenssfeer zich in beginsel tegen de openbaarmaking van namen verzet.[1] Dit geldt, eveneens bepaald door de Afdeling, ook voor andere direct herleidbare gegevens, zoals een telefoonnummer of een e-mailadres.[2]

Toepassing van bovenstaande heeft in de geïnventariseerde documenten geleid tot het niet openbaar maken van de namen en andere persoonsgegevens van ambtenaren. Ik acht het belang van de bescherming van de persoonlijke levenssfeer zwaarder wegen dan het algemene belang van openbaarmaking van deze informatie.

In document met nummer 14 zijn de namen van beoogde leden van een begeleidingscommissie voor een WODC-onderzoek geweigerd op deze uitzonderingsgrond, in combinatie met artikel 5.2, eerste lid van de Woo. Deze personen zijn uiteindelijk niet degenen geweest die in het uiteindelijke rapport zijn genoemd. Het nadenken over namen van beoogde leden van een begeleidingscommissie maakt onderdeel uit van de (voorbereidingen van de) benoemingsprocedure van de voorzitter en leden van een begeleidingscommissie door de directeur van het WODC en dat is een vertrouwelijke procedure. De namen van mogelijke deelnemers aan een begeleidingscommissie bij onderzoek worden genoemd terwijl zij uiteindelijk niet zijn gevraagd, c.q. niet deelnamen. Zij mochten en mogen ervan uitgaan dat het WODC persoonsgegevens niet openbaar maakt gelet op de eerbiediging van de persoonlijke levenssfeer (art. 5.1, lid 2 onder e van de Woo). Het belang hiervan verzet zich in dit geval tegen openbaar maken hiervan omdat het gaat om een vertrouwelijke procedure. Bovendien gaat het hier niet om het geven van een naam aan een individuele burger, maar om openbaarmaking in de zin van de Woo en dus openbaarmaking aan een ieder. Deze uitzonderingsgrond wordt in combinatie toegepast met artikel 5.2, eerste lid Woo, nu uit bovenstaande toelichting ook zonder meer blijkt dat dit beoogde leden van een begeleidingscommissie betreffen en derhalve als een voorstel van de betrokken ambtenaar van het WODC dient te worden gezien in het kader van intern beraad over de samenstelling van de commissie.

---

[1] ABRvS 31 januari 2018, ECLI:NL:RVS:2018:32, r.o. 3.2
[2] ABRvS 4 juni 2008, ECLI:NL:RVS:2008:BD3114, r.o. 2.5.

5.2. Het belang van de opsporing en vervolg van strafbare feiten (artikel 5.1, tweede lid, aanhef en onder c, van de Woo)
Op grond van artikel 5.1, tweede lid, aanhef en onder c, van de Woo, blijft het openbaar maken van informatie achterwege voor zover het belang daarvan niet opweegt tegen het belang van de opsporing en vervolging van strafbare feiten.

Deze uitzonderingsgrond is in de Woo opgenomen om te voorkomen dat de opsporing en vervolging van strafbare feiten, hetgeen een essentiële overheidstaak is, door vroegtijdige openbaarmaking van informatie die daarop betrekking heeft, ernstig wordt bemoeilijkt. In de wetgevingsstukken wordt genoemd dat deze grond ingeroepen kan worden ter bescherming van strategische informatie en beleidsinformatie, waarvan openbaarmaking in individuele gevallen zou kunnen leiden tot gedrag waarmee opsporing kan worden ontweken of belemmerd.[3] Gedacht kan onder meer worden aan informatie over de strategie, werkwijzen, scenario's, inzetgegevens van personeel en materieel, instructies, tolerantiegrenzen, opdrachten, doelen, operationeel beleid, handelingskaders, uitvoeringsvoorschriften en communicatiestrategie. Met die informatie kunnen kwaadwillenden anticiperen op hoe strafbare feiten worden opgespoord en vervolgd en daar hun gedrag op aanpassen. Hierdoor wordt de opsporing en vervolging ernstig bemoeilijkt.[4]

Ook door het Europese Hof van Justitie is beslist dat openbaarmaking van informatie dient te worden geweigerd, indien dit de publieke veiligheid zal ondermijnen omdat het werkwijzen zal onthullen waarvan criminelen onterecht kunnen profiteren.[5]

De documenten met nummers 17, 18, 21, 22, 29, 31, 32. 35 en 36 weiger ik geheel op deze uitzonderingsgrond. Hierbij zijn deze documenten steeds per passage beoordeeld, waarbij is geconcludeerd dat openbaarmaking van al deze passage tot dusdanige belemmering van de opsporing en vervolging van strafbare feiten leidt dat het belang van openbaarheid daarvoor moet wijken.

5.3. Het belang van het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen (artikel 5.1, tweede lid, aanhef en onder i, van de Woo)
Op grond van artikel 5.1, tweede lid, aanhef en onder i van de Woo wordt geen informatie openbaar gemaakt als dit het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen in het geding brengt en niet opweegt tegen het belang van openbaarmaking.[6] In documenten met nummers 1,

[3] Bijlage bij *Kamerstukken I* 2021/22, 33328, AB, p. 89.
[4] ABRvS 6 december 2023, ECLI:NL:RVS:2023:4525, rov. 8.1 & 8.2.
[5] HvJ 26 april 2005, ECLI:EU:T:2005:143, rov 77 and 78; HvJ 27 november 2019, ECLI:EU:T:2019:815, rov. 73 en 74.
[6] *Kamerstukken II*, 2018/19, 35112, 3, p. 21 e.v.

29 en 42 is deze uitzonderingsgrond van toepassing. Het gaat om passages die eveneens gelakt zijn als persoonlijke beleidsopvattingen. Document 1 betreft een stuk dat ziet op de interne voorbereiding bij het OM van het bestuurlijk informerend overleg tussen het OM en de Inspectie Justitie en Veiligheid. De gelakte passages in dit document zijn in de eerste plaats aan te merken als persoonlijke beleidsopvattingen (en worden ook op die grond gelakt), maar bevatten bovendien vertrouwelijke overwegingen omtrent de onderwerpen die in het overleg door het OM met de Inspectie besproken dienen te worden. Indien deze overwegingen achteraf openbaar zouden moeten worden gemaakt, dan wordt het functioneren van het Openbaar Ministerie, te weten de positionering van het OM jegens de Inspectie Justitie en Veiligheid inzake dit onderwerp, hierdoor geschaad.

In document met nummer 42 zijn passages gelakt die zien op de strategische afwegingen met betrekking tot (de prioritering van) de inzet van een technisch hulpmiddel. Deze prioritering geeft strategisch inzicht in de wijze waarop een technisch hulpmiddel wordt inzet en de mogelijke effectiviteit van die inzet. Openbaarmaking van die informatie kan de effectiviteit van die inzet schaden, alsook inzicht geven in welke onderzoeken dit wordt ingezet. Die informatie schaadt niet direct het materiële belang van de opsporing en vervolging zelf, maar kan deze wel minder effectief maken, indien kenbaar zou worden onder welke omstandigheden dit middel doorgaans niet door het OM wordt ingezet. Eenzelfde motivering geldt voor de toepassing van deze uitzonderingsgrond op document 29, aangaande de interne toets die binnen het OM wort uitgevoerd aangaande de inzet van de hackbevoegdheid ex artikel 126nba Wetboek van Strafvordering. Dit document geeft niet zozeer de methodiek van de uitvoering zelf prijs, maar juist de interne toetsing die voor de inzet van toepassing is. Openbaarmaking hiervan zou inzicht geven wanneer deze methodiek door het OM wordt ingezet en zou daarmee het goed functioneren van de inzet van deze bevoegdheid kunnen schaden, dan wel de interne controle door het OM op de inzet van die bevoegdheid kunnen hinderen. Het belang van het goed functioneren van het bestuursorgaan, al dan niet in combinatie met andere toegepaste uitzonderingsgronden, dient zwaarder te wegen dan het algemene belang bij openbaarmaking van deze informatie. Ik weiger derhalve deze informatie openbaar te maken.

5.4. Persoonlijke beleidsopvattingen (artikel 5.2, eerste lid, van de Woo)
Op grond van artikel 5.2, eerste lid, van de Woo, worden persoonlijke beleidsopvattingen in documenten die bestemd zijn voor intern beraad niet openbaar gemaakt. Het is van belang dat ambtenaren de vrijheid hebben ongehinderd hun persoonlijke beleidsopvattingen kunnen uiten bij beleidsvoorbereiding of uitvoering. Zij moeten in alle openhartigheid onderling

functioneel kunnen communiceren.[7] Genoemd artikel geeft aan dat onder persoonlijke beleidsopvattingen moet worden verstaan ambtelijke adviezen, visies, standpunten en overwegingen ten behoeve van intern beraad, niet zijnde feiten, prognoses, beleidsalternatieven, de gevolgen van een bepaald beleidsalternatief of andere onderdelen met een overwegend objectief karakter. Tegelijkertijd geldt dat indien feitelijke gegevens, hoewel deze geen persoonlijke beleidsopvattingen zijn, zodanig met die opvattingen verweven zijn en het niet mogelijk is deze te scheiden, ook deze gegevens met een beroep op artikel 5.2, eerste lid, van de Woo, worden geweigerd.[8]

Het interne karakter van een document wordt daarbij bepaald door het oogmerk waarmee dit is opgesteld. Degene die het document heeft opgesteld moet de bedoeling hebben gehad dat dit zou dienen voor hemzelf of voor het gebruik door anderen binnen de overheid. Ook documenten die afkomstig zijn van derden, die niet tot de kring van de overheid behoren, kunnen worden aangemerkt als documenten die zijn opgesteld ten behoeve van intern beraad indien de documenten met dat oogmerk zijn opgesteld en die derden geen eigen belang hebben bij dat beraad.[9]

In documenten met nummers 1, 14 en 42 zijn persoonlijke beleidsopvattingen opgenomen. Dit betreffen adviezen, visies en standpunten van ambtenaren van het Openbaar Ministerie of het WODC ten behoeve van intern beraad.

Ik maak de persoonlijke beleidsopvattingen in bovengenoemde documenten op grond van artikel 5.2, eerste lid, van de Woo, niet openbaar.

Artikel 5.2, tweede lid, van de Woo maakt het mogelijk dat een bestuursorgaan met het oog op een goede bestuursvoering informatie verstrekt in niet tot personen herleidbare vorm. Ik heb de belangen afgewogen en ik heb beslist de persoonlijke beleidsopvattingen niet openbaar te maken, ook niet in geanonimiseerde vorm. Het (geanonimiseerd) openbaar maken van de persoonlijke beleidsopvattingen is onwenselijk, nu deze persoonlijke beleidsopvattingen informatie betreffen, die nog steeds relevant zijn voor de strategische overwegingen omtrent de inzet van de hackbevoegdheid, dan wel dat deze opvattingen eveneens worden geweigerd door andere uitzonderingsgronden, die door een geanonimiseerde openbaarmaking van de persoonlijke beleidsopvatting zullen worden geschaad.

Openbaarmaking dient daarom niet het doel van een goede bestuursvoering, zoals genoemd in artikel 5.2, tweede lid, van de Woo.

---

[7] ABRvS 15 september 2018, ECLI:NL:RVS:2021:2064, r.o. 13.1.
[8] ABRvS 15 september 2018, ECLI:NL:RVS:2021:2064, r.o. 13.1.
[9] ABRvS 20 december 2017. ECLI:NL:RVS:2017:3497

5.5 Conceptversies

Documenten met nummers 2, 6, 10 betreffen conceptversies van documenten die reeds openbaar zijn gemaakt. Deze versies van documenten met nummers 6 en 10 wijken inhoudelijk niet af van de definitieve versies. Eventuele afwijkingen van de definitieve versies zijn zeer gering en zinledig van aard. Derhalve volsta ik met de verwijzing in de inventarislijst naar de vindplaats van deze reeds openbaargemaakte (definitieve versies van deze) documenten. Document 2 komt grotendeels overeen met de tekst van de definitieve versie. Daar waar het concept afwijkt van de definitieve versie, is deze afwijking inhoudelijk gering en gewijzigd n.a.v. de latere afstemming met het betrokken bestuursorgaan. Deze afstemming is vertrouwelijk van aard en juist bedoeld om de nuances van hetgeen in het verslag aan bod komt op de juiste wijze te verwoorden, zoals door de Inspectie Justitie en Veiligheid ook wordt beoogd. De tekst die in de conceptversie is opgenomen, doch in de definitieve versie is gewijzigd, geeft derhalve slechts een voorstel tot tekst, die later is herzien (juist aangescherpt of genuanceerd) door de Inspectie Justitie en Veiligheid.

Openbaarmaking van deze concepttekst maakt de vertrouwelijke nuanceringen en aanpassingen die in de definitieve versie zijn doorgevoerd feitelijk ongedaan. De opzet van de procedure van de Inspectie is om de feiten, analyse en conclusies van haar verslag te verifiëren en aan te scherpen. Openbaarmaking van de conceptversie geeft derhalve de niet aangepaste versie van dat verslag en kan leiden tot verkeerde (ongenuanceerde) conclusies bij het brede publiek, indien deze worden openbaar gemaakt. Deze niet geverifieerde conclusies kunnen, voor zover de tekst afwijkt van de definitieve versie, het goed functioneren van zowel de Inspectie als van de Politie schaden, voor zover deze op inhoudelijke onderbouwing en nuancering afwijken van de definitieve tekst. Derhalve dienen deze afwijkingen op grond van artikelen 5.1, tweede lid, aanhef en onder i en/of op grond van artikel 5.2, eerste lid van de Woo te worden geweigerd.

6. Vragen

Indien u nog vragen heeft over deze brief, dan kunt u – via bovengenoemd telefoonnummer – contact opnemen met de bovengenoemde contactpersoon.

Ik vertrouw erop u hiermee tot zover naar behoren te hebben geïnformeerd.

Hoogachtend,

de Minister van Justitie en Veiligheid,
namens de Minister,
het College van procureurs-generaal,
namens het College,
het Hoofd Bestuurlijke en Juridische Zaken,

[redacted]

mr. B.B.M. Vroegindeweij

U kunt tegen deze beschikking beroep instellen bij de sector bestuursrecht van de rechtbank van de rechtbank binnen het rechtsgebied waarin hij zijn woonplaats heeft. Het beroepschrift moet binnen zes weken na de dag waarop de beschikking u is toegezonden door de rechtbank zijn ontvangen. U kunt ook digitaal beroep instellen via http://loket.rechtspraak.nl/bestuursrecht. Daarvoor moet u wel beschikken over een elektronische handtekening (DigiD). Kijk op de genoemde site voor de precieze voorwaarden.

Bijlage 1: Inventarisatielijst Woo-verzoek mr. Reissinger d.d. 25 januari 2022

Verzoek	#	Titel document	Datum	Openbaar maken (ja/nee/gedeeltelijk)	Uitzonderingsgronden	Toelichting
1. Alle documenten die zijn vervaardigd in het kader van- of in reactie op het Verslag toezicht wettelijke hackbevoegdheid politie 2019.	1	Memo t.b.v. PaG ivm verslag Inspectie Hackbevoegdheid politie 2019	29-7-2020	gedeeltelijk openbaar maken	5.1,2e, 5.1,2i en 5.2,1	
	2	Concept verslag toezicht hackbevoegdheid politie 2019	28-5-2020	def: versie reeds openbaar	5.1,2i en 5.2,1	Def versie reeds openbaar: https://www.inspectie-jenv.nl/documenten/2020/08/20/verslag-toezicht-wettelijke-hackbevoegdheid-politie-2019:
	3	Verslag bestuurlijk gesprek OM-J&V	30-7-2020	gedeeltelijk openbaar maken	5.1,2e	
2. Alle documenten die zijn vervaardigd in het kader van- of in reactie op het Verslag toezicht wettelijke hackbevoegdheid politie 2020.	4	Notitie tbv PaG mbt Inspectie verslag 2020	16-6-2021	gedeeltelijk openbaar maken	5.1,2e	
	5	Intern OM conceptverslag bestuurlijk gesprek hackbevoegdheid	24-6-2021	gedeeltelijk openbaar maken	5.1,2e	
	6	Concept Verslag toezicht wettelijke hackbevoegdheid politie 2020 wederhoor	4-5-2021	def: versie reeds openbaar		https://www.inspectie-jenv.nl/documenten/2021/06/29/rapport-verslag-toezicht-wettelijke-hackbevoegdheid-politie-2020
	7	Verslag toezicht wettelijke hackbevoegdheid politie 2020	2-6-2021	reeds openbaar		https://www.inspectie-jenv.nl/documenten/2021/06/29/rapport-verslag-toezicht-wettelijke-hackbevoegdheid-politie-2020
	8	Verslag bestuurlijk gesprek OM-IJenV inz Verslag wettelijke hackbevoegdheid 2020 DEF	24-6-2021	gedeeltelijk openbaar maken	5.1,2e	

Verzoek	#	Titel document	Datum	Openbaar maken (ja/nee/gedeeltelijk)	Uitzonderingsgronden	Toelichting
3. Alle documenten die zijn vervaardigd of gedeeld in het kader van- of in voorbereiding op het Verslag toezicht wettelijke hackbevoegdheid politie 2021.	9	Notitie tbv PaG mbt inspectie verslag 2021	20-4-2022	gedeeltelijk openbaar maken	5.1,2e	
	10	bijlage 1 conceptverslag 2021 t.b.v. wederhoor politie	15-4-2022	def. versie reeds openbaar		https://www.inspectie-jenv.nl/documenten/2022/05/31/verslag-toezicht-wettelijke-hackbevoegdheid-politie-2021
	11	brief aan OM inzake hackbevoegdheid	14-2-2022	gedeeltelijk openbaar maken	5.1,2e	
	12	Verslag wettelijke hackbevoegdheid 2021	14-4-2022	reeds openbaar		https://www.inspectie-jenv.nl/documenten/2021/06/29/rapport-verslag-toezicht-wettelijke-hackbevoegdheid-politie-2020
4. Alle documenten die zijn vervaardigd in het kader van- of in reactie op de WODC Evaluatie Wet Computercriminaliteit III: de bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk.	13	Kernconclusies en hoofdpunten WODC - Hackbevoegdheid in de praktijk	Onbekend	openbaar maken		
	14	Startnotitie WODC evaluatie CCIII	11-12-2019	gedeeltelijk openbaar maken	5.1,2e, 5.2,1	
5. Alle documenten die zien op de totstandkoming van- en beleidsvorming naar aanleiding van aanwijzingsbesluiten, haalbaarheidsonderzoeken, plannen van aanpak, resultaten van testen in een proefopstelling en processen-verbaal in het kader van de hackbevoegdheid en de digitale opsporing in algemene zin.	15	PV bevindingen ex 21 lid 4 Bogw - geen bewijs ZAAKSOVJ	16-10-2020	openbaar maken		

Verzoek	#	Titel document	Datum	Openbaar maken (ja/nee/gedeeltelijk)	Uitzonderingsgronden	Toelichting
6. Alle documenten die zien op de self-assessment door het DIGIT van de beveiligingsmaatregelen die gelden bij het toepassen van de hackbevoegdheid en de verwerking en analyse van gegevens.	16	geen documenten aangetroffen				
7. Alle documenten die zien op de werkinstructies bij het toepassen van de bevoegdheden uit de Wet Computercriminaliteit III.	16	Notitie uitgangspunten binnendringen	28-8-2018	gedeeltelijk openbaar maken	5.1,2e	
	17	Notitie binnendringen door AAA (variant XXX)	24-4-2020	weigeren	5.1,2c	
	18	Notitie binnendringen door BBB (variant YYY)	16-11-2020	weigeren	5.1,2c	
	19	Inzet BOB ter ondersteuning van 126nba	16-11-2020	gedeeltelijk openbaar maken	5.1,2e	
	20	Juridische kaders binnendringen bij 126nba	16-11-2020	gedeeltelijk openbaar maken	5.1,2e	
	21	Notitie verwerven en ontsluiten breached databases door DIGIT	2-3-2021	weigeren	5.1,2c	
	22	Notitie binnendringen door CCC (variant ZZZ)	19-8-2021	weigeren	5.1,2c	
	23	Treffen aanvullende waarborgen bij TH	25-10-2021	gedeeltelijk openbaar maken	5.1,2c en 5.1,2e	
	24	Binnendringen ex art. 138ab Sr en art. 126nba	21-12-2021	gedeeltelijk openbaar maken	5.1,2e	

Verzoek	#	Titel document	Datum	Openbaar maken (ja/nee/gedeeltelijk)	Uitzondering sgronden	Toelichting
8. Alle documenten die zien op besluitvorming- en toetsingscriteria bij de keuring van technische hulpmiddelen. In het bijzonder het door de minister van Justitie en Veiligheid goedgekeurde keuringsprotocol.		Aangetroffen documenten worden in het besluit van de landelijke eenheid meegenomen.				
9. Alle documenten die zien op het beleid bij de verwerking van persoons- en locatiegegevens door de opsporingsdiensten. o In het bijzonder de stukken die zien op de uitvoering van- en beleid bij uitvoering van de in de wet gestelde eisen aan de digitale gegevensverwerking: • Algemene verordening gegevensbescherming (AGV). • Wet politiegegevens (Wpg). • Wet justitiële en strafvorderlijke gegevens (Wsjg).		Geen gegevens aangetroffen				
10. Alle documenten die zien op (wijzigingen in) het beleid bij de toepassing van de bevoegdheden uit de Wet Computercriminaliteit III en de verwerking van digitale gegevens	25	Notitie 126m en 126l vs vastlegging	20-9-2019	gedeeltelijk openbaar maken	5.1,2e	
	26	Notitie 126m - buiten provider om	16-4-2020	gedeeltelijk openbaar maken	5.1,2e	
	27	Toetsing en rol RC bij art. 126nba Sv	16-11-2020	gedeeltelijk openbaar maken	5.1,2e	
	28	Toegang tot (online) gegevens	6-1-2021	gedeeltelijk openbaar maken	5.1,2e	
	29	Stappenplan CTC bij toetsing 126nba	1-3-2022	Weigeren	5.1,2c en 5.1,2i	

Verzoek	#	Titel document	Datum	Openbaar maken (ja/nee/gedeeltelijk)	Uitzondering sgronden	Toelichting
	30	Notitie uitgangspunten binnendringen	28-8-2018		gelijk aan doc 29	
	31	Notitie binnendringen door AAA (variant XXX)	24-4-2020	Weigeren	5.1,2c	
	32	Notitie binnendringen door BBB (variant YYY)	28-1-2020	Weigeren	5.1,2c	
	33	Inzet BOB ter ondersteuning van 126nba	16-11-2020		gelijk aan doc 32	
	34	Juridische kaders binnendringen bij 126nba	16-11-2020		gelijk aan doc 33	
	35	Notitie verwerven en ontsluiten breached databases door DIGIT	2-3-2021	Weigeren	5.1,2c	
	36	Notitie binnendringen door CCC (variant ZZZ)	19-9-2021	Weigeren	5.1,2c	
	37	Treffen aanvullende waarborgen bij TH	25-10-2021		gelijk aan doc 36	
	38	Binnendringen ex art. 138ab Sr en art. 126nba	21-12-2021	gedeeltelijk openbaar maken	5.1,2e	
	39	Notitie aanvullende of procedurele waarborgen DEF	11-7-2019	gedeeltelijk openbaar maken	5.1,2e	
	40	Schema TH uitgewerkt	23-8-2019	openbaar maken		
	41	Stroomschema inzet TH	23-8-2019	openbaar maken		
	42	Prioritering technisch hulpmiddel DEF	11-11-2019	gedeeltelijk openbaar maken	5.1,2i en 5.2,1	
	43	Diverse overwegingen mbt TH of handmatige inzet	16-3-2020	gedeeltelijk openbaar maken	5.1,2e	
	44	Toelichting 21 lid 4 Bogw tbv zaaksOvJ	16-10-2020	gedeeltelijk openbaar maken	5.1,2e	
	45	Handelingskader inzet technisch hulpmiddel en handmatige inzet	28-6-2021	openbaar maken		

BIJLAGE 2

Document 1

OPENBAAR MINISTERIE

Parket-Generaal

Memo

Aan	Gerrit van der Burg
Van	[redacted], afgestemd met [redacted]
Datum	27 juli 2020
Onderdeel	PaG/B&S
Onderwerp	Informerend/bestuurlijk gesprek Verslag toezicht wettelijke hackbevoegdheid politie 2019

Dag Gerrit,

Op 29 juli heb jij van 11.00 – 12.00 een informerend/bestuurlijk gesprek met Henk Korvinus, inspecteur-generaal bij de inspectie JenV, m.b.t. het 'verslag toezicht wettelijke hackbevoegdheid 2019'. Dit gesprek is ingepland nadat jullie op 8 juli telefonisch hebben bijgepraat over het werkprogramma 2021 van de inspectie JenV.

Voor het gesprek is geen agenda bekend. Daarnaast ben ik ook niet op de hoogte van de inhoud van jullie gesprek van 8 juli. Daarom focust dit memo zich uitsluitend op het verslag dat begin deze maand aan de minister en politie is verstuurd.

Groet,

[redacted]

Agenda

Geen toelichting. Er is geen agenda opgesteld voorafgaand aan de vergadering. Ik heb hieronder een advies uiteengezet en daarna de achtergrond toegelicht.

Bijlagen

Input voor gesprek:

1. Verslag toezicht wettelijke hackbevoegdheid politie 2019_def

Ter kennisgeving:

2. 2968898 – Brief aanbieding vastgesteld verslag aan politie
3. Tabel wederhoor CCIII_reacties politie en IJenV

Toelichting: Bijlage 1, het verslag, is **wel** gedeeld met het OM vanuit de inspectie ter voorbereiding voor dit gesprek. Bijlage 2 en 3 zijn **niet** van de inspectie afkomstig, maar heeft het OM van de politie ontvangen.

5.1,2i en 5.2,1 [redacted]

Advies

Mijn advies is tweeledig bestaande uit wat niet en wat wel te bespreken:

1. Advies om niet te bespreken:

5.1,2i en 5.2,1

5.1,2i en 5.2,1

5.1,2i en 5.2,1

5.1,2i en 5.2,1

2. Advies om wel te bespreken:

Het verslag is begin deze maand aangeboden aan de minister, die 6 weken heeft voor een beleidsreactie. Zowel LP als politie geven aan te wachten op een eerste concept van de beleidsreactie die door het departement zal worden voorbereid.

Achtergrond
Hieronder heb ik een aantal punten uitgelicht waarvan het mij nuttig lijkt kennis van te nemen voorafgaand aan het gesprek dat jij voert met Henk Korvinus.

Verslag IJV

- Op 1 maart 2019 is de Wet Computercriminaliteit III (Wet CCIII) in werking getreden. De Wet CCIII introduceert met artikel 126nba Sv. de bevoegdheid voor de politie om een geautomatiseerd werk zoals een laptop of een smartphone dat in gebruik is bij een verdachte, heimelijk en op afstand binnen te dringen en hier onderzoek in te doen. De Inspectie Justitie en Veiligheid (Inspectie JenV) is de toezichthouder op de taakuitvoering door de politie.

- Het eerste verslag over de periode 1 maart 2019 (de datum van inwerkingtreding van de wet) tot en met 31 december 2019 van de inspectie J&V over het team bij de politie dat exclusief bevoegd is om de hackbevoegdheid uit te voeren (team DIGIT) is begin deze maand aan de minister en de politie verstuurd. De minister heeft 6 weken voor een beleidsreactie, die wordt verwacht op 20 augustus. Daarna wordt het verslag (en vermoedelijk ook de wederhoor tabel) openbaar gemaakt.

- [redacted]

5.1,2i en 5.2,1

- [redacted]

5.1,2i en 5.2,1

Rol van het OM

- Het OM heeft geen contact gehad met de inspectie JenV over de inhoud van het verslag, ook niet in de concept-fase. OM is formeel geen partij bij het toezicht van de inspectie op de politie.

- Het LP en de politie hebben in parallel aan het onderzoekstraject van de inspectie (constructief) discussie gevoerd met het departement over praktijkervaringen en knelpunten met het keuringsproces t.a.v. technische hulpmiddelen die worden ingezet. Het departement heeft daardoor veel actuele kennis over de praktijk van het (niet) keuren van technische hulpmiddelen.

Potentiele gevoeligheden, niet bespreken

- [redacted]

5.1.2i en 5.2.1

- [redacted]

5.1.2i en 5.2.1

- [redacted]

5.1.2i en 5.2.1

Document 3

Inspectie Justitie en Veiligheid
Ministerie van Justitie en Veiligheid

Inspectie Justitie en Veiligheid

Datum
29 juli 2020

Datum vaststelling
30 juli 2020

Notulist
[redacted]

verslag

Bestuurlijk gesprek Verslag wettelijke hackbevoegdheid politie 2019

Omschrijving	Informerend gesprek op bestuurlijk niveau naar aanleiding van het Verslag van het toezicht door de Inspectie Justitie en Veiligheid op de toepassing door de politie van de bevoegdheid op basis van de Wet Computercriminaliteit III om in een geautomatiseerd werk binnen te dringen en onderzoek te doen.
Vergaderdatum en -tijd	29 juli 2020, 11:00 uur
Vergaderplaats	Parket-Generaal - Den Haag
Aanwezig	Openbaar Ministerie: Gerrit van der Burg [redacted] Inspectie Justitie en Veiligheid: Henk Korvinus [redacted]

1 Introductie door Henk:

- De toepassing van de nieuwe bevoegdheid is door de politie en het OM goed opgepakt.
- In de praktijk loopt men tegen diverse problemen aan, waaronder het feit dat de politie niet beschikt over (vooraf) goedgekeurde technische hulpmiddelen.
- Er is sprake van een nauwe verwevenheid tussen het handelen van de politie en het optreden van het OM. De Inspectie houdt toezicht op het handelen van de politie. Indien de Inspectie in aanraking komt met mogelijke schendingen van wettelijke voorschriften door of in opdracht van het OM, dan signaleert de Inspectie dit. Het oordeel hierover is aan de PG-HR.

2 Reactie OM:

- De hackbevoegdheid is hard nodig, dat blijkt uit de praktijk. Voorkomen moet worden dat op basis van de evaluatie van de wet CCIII de reflex ontstaat om deze bevoegdheid weer in te trekken. Het OM heeft de behoefte aan een podium om de knelpunten op de juiste manier voor het voetlicht te brengen.

- Een belangrijk knelpunt is de internationale context: tussen Europese landen bestaan grote verschillen in de wijze waarop de hackbevoegdheid mag worden ingezet.
- Een ander knelpunt is de spanning tussen de formuleringen in het wettelijk kader over de uitoefening van de heimelijke informatie-inwinning enerzijds en de toepassing in de praktijk anderzijds: door de voortschrijding van de techniek en de praktijkervaringen blijkt de werkelijkheid af te wijken van het beeld ten tijde van het opstellen van het wettelijk kader. Bijvoorbeeld in het keuringstraject blijkt dat de eisen uit het wettelijk kader door verschillende IT'ers verschillend worden geïnterpreteerd.
- Indien in een strafzaak bewijs wordt ingebracht dat middels de hackbevoegdheid is verkregen, zal de rechter dit altijd waarderen in samenhang met de overige beschikbare bewijsmiddelen.
- Het OM heeft zelf gevraagd om een onderzoek door de PG-HR naar de bevoegdheden in het digitale domein, waaronder deze hackbevoegdheid. Dit met name voor de zaken die niet voor de strafrechter komen.
- In het parlementaire traject bij de totstandkoming van de Wet CCIII waren de drie grootste zorgpunten:
  - Misbruik van de hackbevoegdheid door de politie
  - Het openhouden van onbekende kwetsbaarheden
  - Het stimuleren van de markt voor commerciële binnendringsoftware.

  Als onderdeel van de evaluatie door het WODC wil het OM graag dat deze politieke gevoeligheden op het speelveld gelegd worden.
- Het OM is tevreden over de manier waarop de Inspectie toezicht houdt.
- Een risico van publicatie van het verslag is dat het de evaluatie naar voren haalt. Voor de evaluatie zijn echter ook andere perspectieven van belang, met name de noodzaak van deze bevoegdheid en de internationale context.

Document 4

OPENBAAR MINISTERIE

Landelijk Parket

Notitie

Aan [redacted]
Van [redacted]
Doorkiesnummer(s) 06 – [redacted]

Datum 16 juni 2021
Onderdeel Landelijk Parket – DIGIT
Onderwerp Verslag Inspectie J&V m.b.t. inzet van de hackbevoegdheid.

1 Aanleiding

Op 24 juni 2021 vindt er een bestuurlijk overleg plaats over het Verslag van de Inspectie J&V m.b.t. inzet van de hackbevoegdheid (art. 126nba Sv) door de politie in 2020. Dit verslag ligt op dit moment bij het departement van J&V voor het voorbereiden van een reactie beleidsreactie van de minister. Daarbij is de planning om de beleidsreactie en het rapport voor het reces aan de tweede kamer te zenden.

We hebben deze week op diverse momenten contact met het departement en de politie gehad over de concept beleidsreactie.

We hebben daarnaast de politie van input voorzien voor de wederhoor tabel.

2 Korte algemene reactie op het verslag

Net als het voorgaande verslag (over 2019) vallen er in algemene zin een aantal zaken op aan het verslag.

Inspectie hanteert een wijze van verslaglegging waarbij bijna alleen gekeken wordt naar hetgeen niet volledig compliant is. Zaken die deels geregeld zijn of goed geregeld zijn worden niet benoemd. Daardoor ontstaat een onevenwichtig beeld.

De inspectie verwoord zeer stellig dat verbeteringen zijn uitgebleven, terwijl dat geen recht doet aan de inspanningen die zijn gedaan. Op diverse punten zijn verbeteringen doorgevoerd, maar omdat die nog niet tot 100% compliance leiden worden ze niet als zodanig benoemd. Daardoor ontstaat eveneens een onevenwichtig beeld. In het verslag wordt weinig rekening gehouden met de 'normale' praktijk rond nieuwe wetgeving waarbij de uitvoering zich na het wetgevingstraject in de praktijk ontwikkeld. De hackbevoegdheid is een nieuwe bevoegdheid waarvan het wettelijk kader op veel punten geen precedent elders in de opsporing heeft, soms zaken op micro niveau zijn geregeld en waar verschil bestaat tussen wat er tijdens de totstandkoming in theorie is bedacht en na 2 jaar

in de praktijk operationeel werkbaar blijkt.

Tot slot hecht ik er aan om op te merken dat de opmerkingen die de inspectie maakt over de gebreken in de logging, geen betrekking hebben op de bewijslogging, maar vooral zien op de andere vormen van logging die het Bogw voorschrijft.

Ik verwacht n.a.v. dit verslag voor concrete onderzoeken / strafzaken geen problemen. Het verslag zal wel nadelig kunnen zijn voor het komende traject met het departement waarin we – na de evaluatie van het WODC – willen kijken op welke wijze de regelgeving aangepast kan worden?

3 Toezicht Inspectie vs. gezag officier van justitie

N.a.v. het verslag van de inspectie over 2019 merkten we op 27 juli 2020 (in het memo dat voorafging aan het bestuurlijk overleg van 29 juli 2020) al op dat de inspectie op een aantal punten oordelen geeft die de besluitvorming van de officier van justitie betreffen. De inspectie trad daarmee buiten haar taak / opdracht bij het houden van toezicht.

Na dat verslag heb ik een aantal maal gesproken met de inspecteurs. Daarbij bleek dat ze zeer weinig tot geen inzicht hadden in de wijze waarop het Openbaar Ministerie functioneert en de manier waarop we als het gezag van de opsporing onze (toezichtshoudende)rol op de politie vorm geven. Om die reden heb ik het afgelopen jaar vooral geïnvesteerd in hen informeren op dit punt, zodat de afbakening van hun rol/taak en die van het OM duidelijker zou worden.

Dat lijkt niet het gewenste resultaat te hebben gehad. In het verslag over 2021 (en in de daaraan voorafgaande brieven aan de politie) begeeft de inspectie zich nog steeds en meer op het terrein waarin het Openbaar Ministerie het gezag over de opsporing voert.

De inspectie doet dit in het verslag met opmerkingen over gebruik voor bewijs van vastgelegde gegevens (p. 10, 3 alinea en p. 21, 2e alinea), de wijze van verbaliseren (p. 12, voorlaatste alinea), het treffen van aanvullende waarborgen (p. 15, eerste alinea), het voldoen van een technisch hulpmiddel aan de eisen van het Bogw (p. 15, tweede alinea en p. 20, 3e alinea) en de beoordeling van het OM dat of sprake is van een technisch hulpmiddel (p. 16, eerste alinea)

Op p. 10 schrijft de inspectie het volgende:

> *"Het door de officier van justitie afgegeven bevel vormt het kader waarbinnen de politie uitvoering aan deze bijzondere bevoegdheid mag geven. In het bevel vermeldt de officier van justitie onder andere een aanduiding van het geautomatiseerde werk, de periode van uitvoering en de doelen van het onderzoek inclusief eventuele beperkende voorwaarden. De Inspectie heeft onderzocht in*

hoeverre de politie in 2020 heeft gehandeld binnen de reikwijdte van de door de officier van justitie afgegeven bevelen."

De inspectie miskent hiermee dat naast bevelen van officieren van justitie in specifieke zaken, ook door de landelijk DIGIT officier aan de politie (algemene) kaders / opdrachten worden gegeven voor diverse handelingen die DIGIT uitvoert. Op het gebied van bijvoorbeeld het binnendringen, de omgang met geheimhouders, de omvang van wat wel/niet een technisch hulpmiddel is en de wijze van verbaliseren, zijn door de landelijk DIGIT officier kaders aan de politie gesteld als gezag over de opsporing. De inspectie hanteert een te nauw en beperkt kader voor wat het OM doet.

Op 24 juni 2021 staat – na het bestuurlijk gesprek tussen de inspecteur-generaal en de voorzitter van het College – een gesprek gepland tussen de landelijk DIGIT officier en twee inspecteurs om nader te spreken over de rol van het OM als gezag over de opsporing en de rol van de inspectie als toezichthouder op de politie. Het doel daarvan is om scherper af te bakenen waar de inspectie een rol heeft en waar het OM een rol heeft. Dat zal mogelijk tot weerstand of wrevel leiden.

Om voor de komende periode te zorgen dat voor de inspectie helder is waar de politie handelt op last van de officier van justitie, zijn we met de politie bezig om te zorgen dat dit op diverse plekken (beter) wordt vastgelegd in journaals of andere documenten. Met de inspectie zullen we bespreken wat zij nodig hebben om hierin niet buiten hun toezicht te treden.

Ik denk dat het wenselijk is om hier in het bestuurlijk gesprek tussen de inspecteur-generaal en de voorzitter van het College alvast op te anticiperen.

16 juni 2021

[redacted]

Document 5

OM intern verslag bestuurlijk gesprek inspectie inzake de hackbevoegdheid

Deelnemers inspectie: Henk Korvinus, Angela van der Putten, [redacted]

Deelnemers OM: Gerrit van der Burg, [redacted]

Henk: Algemene introductie. Inspectie wil graag spreken over de lijn die wordt gezien. Inspectie kijkt naar de taakuitvoering van de politie en PG Hoge Raad naar die van het OM. Het inspectieverslag is een opmaat naar de evaluatie van de wet op de hackbevoegdheid. Deze wet is ingegeven door wantrouwen vanuit het parlement voor het toekennen van deze bevoegdheid. Het zou technisch neutraal moeten zijn, maar praktijk lijkt anders.

Gerrit: waardering voor het initiëren van dit overleg. Goed om nog eens te kijken waar inspectie en OM voor staan. Er is een trend waarneembaar dat politie en OM in de gezagsrol aan het zoeken zijn naar de invulling van de wet. Wat opvalt in het verslag is:

- Er wordt vooral benadrukt wat nog niet volledig geregeld is. Dingen die wel goed op stoom zijn worden weggelaten. Daar maakt het OM zich zorgen over. Door disbalans in wat wel/niet goed gaat wordt geen recht gedaan aan de inspanningen van de politie.
- Wat OM ook steeds in ogen houdt is dat het een nieuwe wet betreft waar in de uitvoering ook tegen allerlei elementen wordt aangelopen waar oplossingen voor moeten worden bedacht.
- Inspectie kan inderdaad niet naar het OM kijken, maar we zien dat er wel tegenaan wordt geschurkt. Het is niet aan de inspectie om een uitspraak over de gezagsrol van het OM te doen. Er zijn verscheidene voorbeelden in het verslag waar dit uit blijkt. Daar kan ook afzonderlijk nog het gesprek over worden gevoerd.
- Dat als eerste opmerkingen onder de waardering van het werk dat door de inspectie is verricht. Ook fijn dat de inspectie contact onderhoudt met de PG Hoger Raad.

[redacted]: De blik van de inspectie op de bedrijfsvoering van DIGIT stelt het OM in staat om e.e.a. aan te scherpen. Het is weliswaar zoeken waar de signalerende rol van de inspectie stopt en waar het OM verder gaat. De gezagsrol van het OM wordt nu in het rapport wel te nauw beschreven. Hierover zijn eerder gesprekken gevoerd tussen OM en inspectie en zal ook op worden doorgesproken. Het is vervelend voor dit politieteam als er twee toezichthouders zijn.

Henk: Het beeld van [redacted] wordt herkent vanuit de wederhoortabel die door de politie is aangeleverd in reactie op het verslag. Inspectie probeert haar rol uit te voeren met de wet in de hand. Fijn dat inspectie en OM hier nader over kunnen doorspreken.

[redacted]: Focus van de inspectie ligt op de taakuitvoering, maar daar zit een grijs gebeid. Wat is echt de politie aan te rekenen en wat komt vanuit de gezagsrol van het OM. Het is belangrijk dat we elkaar daar in gaan vinden. We spreken ook met de PG hoge raad hoe ver we kunnen gaan.

Angela: de politie gaf ook expliciet aan dat de inspectie met het OM in gesprek moeten omdat zij zich tussen twee werelden in voelen.

5.1.2e Inspectie focust zich op de naleving van de wettelijke bepaling. Daarin wordt getracht objectief te kijken of de wettelijke bepaling al dan niet worden nageleefd. Ook wat betreft het technisch hulpmiddel zijn er een aantal regels. Dat zijn zaken waar de inspectie geen oordeel over heeft, maar er wordt wel geconstateerd dat er niet altijd wordt voldaan aan de onderliggende eisen. Een andere gevoeligheid is de betrouwbarheid van het bewijs. Als de inspectie een risico ziet, moet dat worden benoemd. Dat is ook afgestemd met de PG Hoge Raad

Henk: Meer algemeen als de inspectie enig risico ziet bij de taakuitoefening van de politie, dan moeten daar iets over gemeld worden. De vervolgstappen daarop en gevolgen zijn aan andere partijen.

5.1.2e De beoordeling of iets en technisch hulpmiddel is valt volledig onder het OM. Daarmee ook onder het gezag van het OM. Daarin zit ingebakken dat de OvJ een oordeel geeft. Als het verslag daar op ziet, kun je je afvragen of de inspectie zich niet teveel op het terrein van het OM begeeft.

Gerrit: Goed dat er nader wordt doorgesproken over de rolafbakening. Het gezag van het OM heeft een smal en een breed kader. Het is van belang om vanuit dat kader naar de voorbeelden in het rapport te kijken.

Henk: Goed dat de politie constateert en dat betrokken partijen (OM en inspectie) (idealiter) overeenstemming bereiken over de rolafbakening. De inspectie zal dit ook in het contact met de PG Hoge Raad aanstippen. Als we zien dat de politie anders handelt dan de opdracht van het OM is, dan kunnen we stellen dat er enig risico ontstaat. Hoe daarmee verder te gaan is dan aan de OvJ.

Angela: Wij kijken er naar wat er in de wet staat.

Henk: Er is ook nog de evaluatie van het WODC. De diepere vraag aan de wetgever is 'weet je wel wat je vraagt van politie?'. In hoeverre bevat de vraag die voorligt daadwerkelijk de waarborgen waar de wetgever initieel zorgen over had.

[redacted] Richting evaluatie zijn de twee verslagen natuurlijk heel waardevol. Daar is voor de inspectie wel een lastige positie. Vanuit OM is er de uitdaging om de wet nog nader in te vullen.

Vwb de signalering dat technische hulpmiddel niet goed is toegepast helpt het OM enerzijds. Anderzijds wordt er een zin aan toegevoegd waar de inspectie niet over kan oordelen. De opmerking dat er een consequentie is voor het bewijs past in optiek van het OM niet in het verslag. Dit kan er ook toe leiden dat de inpsectie als getuigedeskundige worden gevraagd een ordeel te geven.

Het OM stelt voor dat inspectie stopt bij signalering en niet over gaat op oordeelsvorming.

Henk: De toelichting wordt door de inspectie als nuttig ervaren. De inspectie kijkt op basis van deze toelichting en 'horizonverbreding' naar de mogelijke consequenties van bepaalde zinsneden uit het rapport. De inspectie heeft uiteraard wel een onafhankelijke positie.

Gerrit: Een ander punt is dat wat het OM betreft de toonzetting kort door de bocht is geformuleerd. Al is er uiteraard ook begrip voor het referentiekader van de inspectie.

Angela: De inspectie weerspreekt dat de toon kort door de bocht is. Het eerste jaar is relatief coulant opgetreden. Er zijn een aantal zaken die in de ogen van de inspectie niet goed geregeld zijn.

[redacted] In aanvulling daarop ziet de inspectie wel dat er goede richtingen zijn ingezet. Maar over 2020 zijn er weinig feiten die onderbouwd kunnen worden. De hoop is dat 2021 anders is, al wordt nu al geconstateerd dat de Logging niet helemaal op orde is. Het is wachten op concrete resultaten.

[redacted] Er is een verschil in prioritering door OM en inspectie. Inspectie kijkt veelal naar de bedrijfsvoering. OM hecht grote waarde in welke mate DIGIT ondersteuning kan bieden en de opsporingsbevoegdheid kan inzetten. De progressie op dat vlak is gigantisch. Er is mogelijk daardoor minder progressie in de bedrijfsvoering. Dat is niet het primaat waar dit team voor op aarde is. De vragen vanuit tactische teams en vanuit zaaksofficieren wordt door de DIGIT OvJ gekanaliseerd. Het is ook aan het OM om de inspectie inzicht te geven in hetgeen er in opdracht van het gezag gebeurt en wat DIGIT zelf doet.

Gerrit: ook procedureel heeft het OM sterke eisen gesteld. Het is een ingewikkeld proces hoe je vooraf e.e.a. al kan inkleden. De wet had natuurlijk wel wat open eindjes. Daar wordt nog steeds invulling aan gegeven.

Henk: Het schrikbeeld van de kamer is dat de wet at random en zomaar wordt ingezet. En het OM wil juist de wet graag inzetten wanneer echt nodig. We hebben dit jaar te weinig verbeteringen gezien. Ook in 2021 moet er echt wel even opgelet worden.

Document 8

Inspectie Justitie en Veiligheid
Ministerie van Justitie en Veiligheid

Inspectie Justitie en Veiligheid

Datum
24 juni 2021

Notulist
[redacted]

verslag

Bestuurlijk gesprek Verslag wettelijke hackbevoegdheid politie 2020

Omschrijving	Informerend gesprek op bestuurlijk niveau naar aanleiding van het Verslag van het toezicht door de Inspectie Justitie en Veiligheid op de toepassing door de politie van de bevoegdheid op basis van de Wet Computercriminaliteit III om in een geautomatiseerd werk binnen te dringen en onderzoek te doen.
Vergaderdatum en -tijd	24 juni 2021, 11:30 uur
Vergaderplaats	WebEx
Aanwezig	Openbaar Ministerie: Gerrit van der Burg [redacted] Inspectie Justitie en Veiligheid: Henk Korvinus [redacted]

- Henk Korvinus schetst op basis van het uitgevoerde toezicht de lijn die de Inspectie ziet en refereert aan het eerder deze week gehouden bestuurlijk gesprek met de politie. De Inspectie kijkt naar de taakuitvoering door de politie. Waar het de taakuitvoering van het OM betreft, heeft zij geen opvatting maar beschrijft zij dit wel.

- Gerrit van der Burg spreekt waardering uit voor het vele werk van de Inspectie en realiseert zich dat het een ingewikkeld onderwerp is. Het OM maakt zich zorgen over het onevenwichtige beeld dat bij de gemiddelde lezer van het verslag kan ontstaan. Dit doet volgens het OM geen recht aan de inspanning die door de politie is geleverd omdat op diverse punten verbeteringen zijn doorgevoerd. Deze hebben misschien nog niet tot 100% compliance van de regelgeving geleid. Benadrukt wordt dat de wet nieuw is. Ook in de uitvoering wordt nog tegen allerlei elementen aangelopen. Met elkaar moet daarvoor een oplossing worden bedacht.

- [redacted] geeft aan dat in het eerste verslag van de Inspectie een coulance oordeel is gegeven om juist de opstartfase te benadrukken. Het afgelopen jaar is wel progressie geweest, maar deze is minimaal geweest.

- [redacted] vult aan dat het verslag het jaar 2020 betreft en optekent wat 31 december echt gerealiseerd is. De richting is door de politie uitgezet, op concrete resultaten wacht de Inspectie nog.

- Gerrit van der Burg ziet een paar keer in het verslag dat de Inspectie dicht nadert tot het terrein van het OM, bijvoorbeeld als de Inspectie uitspraken doet over de toelaatbaarheid van het bewijs. Dat is aan de officier van justitie en later ter beoordeling aan de rechter en niet aan de Inspectie om daar uitspraken over te doen.

- [redacted] spreekt waardering uit voor de meer bedrijfsmatige focus waarmee de Inspectie kijkt naar wat de politie doet. Dit geeft mooie handvatten om een en ander scherper te maken. De Inspectie belicht niet de operationele progressie van het team en het resultaat dat zij in de opsporingspraktijk hebben geboekt. Op aangeven van het OM heeft de politie ook het afgelopen jaar de prioriteit gelegd op het opdoen van operationele ervaring.

- [redacted] geeft aan dat nog niet duidelijk is waar de signalering van de Inspectie stopt en waar het OM op basis van dat signaal conclusies trekt en corrigerend naar de politie optreedt. De gezagsrol van het OM is breder dan waar nu in het toezicht door de Inspectie vanuit wordt gegaan. Als in het verslag concluderend wordt gesproken over het technisch hulpmiddel dan is dat een impliciete waardering van de onder het gezag van de officier genomen beslissing. Het is in het belang van alle partijen dat de politie niet tussen twee toezichthoudende partijen klem komt te zitten. Het moet duidelijk zijn waar de politie handelt op last van het gezag van het OM en waar zij dit zelfstandig doet. Over deze standpunten zal in het reguliere overleg na afloop van het bestuurlijk gesprek met de Inspecteurs verder van gedachte worden gewisseld.

- [redacted] reageert dat vanuit het toezicht objectief naar de naleving van de wettelijke bepalingen gekeken wordt. De Inspectie constateert de feiten zoals ze zijn op basis van die regels. Als het gaat om technische hulpmiddelen dan zijn er een aantal regels. Gesignaleerd is dat het gebruik van het technisch hulpmiddel risico's met zich meebrengt voor de betrouwbaarheid van de middels dat hulpmiddel verkregen gegevens. Hierover is ook afstemming gezocht met de PG-HR over het mogen en moeten benoemen van het risico.

- Henk Korvinus vindt het betekenisvol dat ook de politie dit aan de orde stelt. Daarmee worden de partijen uitgenodigd om nader tot overeenstemming te komen. Het is goed dat [redacted] daar vanmiddag met de Inspecteurs over doorpraat. In het komende contact met de PG-HR zal dit ook aangestipt worden. De Inspectie kan aangeven dat er enig risico ontstaat als door de politie anders gehandeld is dan de opdracht van het OM. Het is aan het OM en de politie om te bezien hoe daar mee omgegaan moet worden.

- [redacted] schetst de handelswijze van het OM nadat de Inspectie vastgesteld had dat in twee situaties niet door de politie is gesignaleerd dat de politie in het verkeerde geautomatiseerde werk is binnengedrongen. In de ene situatie heeft dit geleid tot het vernietigen van de gegevens, in de andere situatie heeft stellingname door de rechter-commissaris plaatsgevonden. Dit komt in het dossier terecht waarmee de zittingsrechter dit kan toetsen. Hiermee is de rechtssituatie hersteld. De gevolgtrekking die de Inspectie daaraan verbindt in het verslag gaat verder dan alleen het signaleren en kan leiden tot consequenties in een zitting.

- Gerrit van der Burg wijst erop dat de consequentie kan zijn dat de Inspectie later in de positie gebracht wordt om als getuige-deskundige tekst en uitleg te komen geven. Uiterste voorzichtigheid is op zijn plaats bij het kiezen van de zinsconstructie en bewoording.

- Henk Korvinus geeft aan dat ook het agenderende ten aanzien van de evaluatie speelt. Geconstateerd kan worden dat de wetgever nogal wat eisen heeft gesteld waar de politie zich allemaal aan moet houden, maar niet altijd door de politie gedaan wordt. Dit constateert de Inspectie ook, waarbij meer verbetering was verwacht dan er nu is. Gelijktijdig is er ook een diepere vraag of de wetgever zich realiseert wat allemaal gevraagd wordt aan de politie en tot welke belasting dit leidt. Deze kwestie moet zeker aan de orde komen bij de evaluatie.

- [redacted] geeft aan dat de twee verslagen van de Inspectie heel waardevol voor de evaluatie zijn omdat ze de pijnpunten goed zichtbaar maken. De wetgeving blijkt in de praktijk op sommige punten in mindere mate uitvoerbaar te zijn. De Inspectie toetst wat de wetgever in theorie bedacht heeft, terwijl het OM vanuit zijn rol meer bezig is met het rechtsvormende stuk.

- Henk Korvinus sluit af dat de Inspectie heeft geconstateerd dat in 2020 nog te weinig verbetering is gezien. In het gesprek is meegegeven dat in 2021 ook nog best een aantal punten verbeterd moet worden. Het is goed dat [redacted] in een vervolggesprek met de Inspecteurs doorspreekt over hoe het toezicht door de Inspectie zich verhoudt tot de gezagsrol van het OM.

Document 9

Aan [redacted]
Van [redacted]
Doorkiesnummer(s) 06 - [redacted]

Notitie

Datum 20 april 2022
Onderdeel Landelijk Parket – DIGIT
Onderwerp Verslag Inspectie J&V m.b.t. inzet van de hackbevoegdheid in 2021.

1 Aanleiding

Op 4 mei 2022 vindt er een bestuurlijk overleg plaats over het verslag van de Inspectie J&V m.b.t. inzet van de hackbevoegdheid (art. 126nba Sv) door de politie in 2021. Dit verslag ligt op dit moment bij het departement van J&V voor het voorbereiden van een beleidsreactie van de minister. Daarbij is de planning om de beleidsreactie en het verslag zal uiterlijk vrijdag 27 mei 2022 openbaar worden gemaakt.

Vanuit het LP (landelijk officier voor Digital Intrusion, senior adviseur en strategisch beleidsadviseur) hebben we de politie van input voorzien voor de wederhoor tabel. Deze wordt samen met het verslag openbaar gemaakt.

We zullen samen met de politie input leveren aan het departement voor de (concept) beleidsreactie.

2 Korte algemene reactie op het verslag

Het verslag van de inspectie over 2021 bevat geen onverwachte resultaten of conclusies.

Anders dan de voorgaande verslagen (over 2019 en 2020) hanteert de inspectie dit jaar een wijze van verslaglegging die een evenwichtiger beeld schetst van de manier waarop de politie uitvoering geeft aan de hackbevoegdheid. Er wordt niet enkel meer gekeken naar hetgeen niet volledig compliant is, maar er worden steeds inleidend daaraan zaken beschreven die wel al (deels) gerealiseerd zijn.

Het meest in het oog springende punt in dit verslag zijn de constateringen en opmerkingen over het gebruik van commerciële software. Het College is over (de besluitvorming rond) de inzet van deze software in 2020 al geïnformeerd.

Ik verwacht n.a.v. dit verslag voor concrete onderzoeken / strafzaken geen problemen.

3 Toezicht Inspectie vs. gezag officier van justitie

In de verslagen over 2019 en 2020 kwam naar voren dat de inspectie op een aantal punten oordelen gaf die de besluitvorming van de officier van justitie betroffen. De inspectie trad daarmee buiten haar taak / opdracht bij het houden van toezicht. In het bestuurlijk gesprek tussen de inspecteur generaal van de inspectie en de voorzitter van het College van 21 juni 2021 (over toezicht jaar 2020) is op dat punt uitgebreid stilgestaan.

De gesprekken die wij voerden met de betrokken inspecteurs hebben we na juni 2021 iets geïntensiveerd. We hebben hen nog meer meegenomen in de wijze waarop het Openbaar Ministerie functioneert en de manier waarop we als het gezag van de opsporing onze (toezichtshoudende)rol op de politie vormgeven. Daarnaast hebben we duidelijker vastgelegd welke kaders door de landelijk officier voor Digital Intrusion aan de politie zijn gesteld.

De inspectie heeft in 2021 veel werk gestoken in het opstellen / formaliseren van een toetsingskader aan de hand waarvan ze hun toezicht uitvoeren. Ze hebben (concepten) van dit kader met ons gedeeld en input gevraagd bij het opstellen om helder te krijgen hoe de afbakening tussen rollen er uit zou moeten zien. De definitieve versie van dit kader wordt op korte termijn met de politie besproken en daarna met ons gedeeld.

In het verslag over 2021 komt de afbakening tussen de rol van de inspectie en het Openbaar Ministerie duidelijker naar voren. Anders dan in het verslag over 2020 begeeft de inspectie zich nagenoeg niet meer op het terrein waarin het Openbaar Ministerie het gezag over de opsporing voert. Op twee punten waar het nog enigszins wringt (zie nrs. 11 en 17 in de wederhoortabel) heeft de inspectie hun verslag zodanig verduidelijkt of aangevuld dat het naar mijn idee acceptabel is.

4 Slotsom

Ik denk dat het wenselijk is om in het bestuurlijk gesprek tussen de inspecteur-generaal en de voorzitter van het College te benoemen dat we blij zijn met de evenwichtigere wijze van verslaglegging.

Daarnaast lijkt het me nuttig als benoemd wordt dat we tevreden zijn dat de wederzijdse inspanningen om te komen tot een heldere afbakening tussen taken/rollen, heeft geleid tot een verslag waarin nagenoeg geen conflicterende situaties bestaan.

20 april 2022

Document 11

Inspectie Justitie en Veiligheid
Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

Openbaar Ministerie Parket-Generaal
Voorzitter van het college procureurs-generaal
Mr. G.W. van der Burg
Postbus 20305
2500 EH Den Haag

Inspectie Justitie en Veiligheid
Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.inspectie-jenv.nl

Contactpersoon
[redacted]
Senior Inspecteur
M 06 [redacted]
[redacted]@inspectie-jenv.nl

Projectnaam
Toezicht hackbevoegdheid CCIII

Ons kenmerk
3966017

Bijlagen
2

Bij beantwoording de datum en ons kenmerk vermelden Wilt u slechts één zaak in uw brief behandelen

Datum 14 april 2022
Onderwerp Aanbieding Verslag toezicht wettelijke hackbevoegdheid politie 2021

Geachte heer Van der Burg,

De Inspectie Justitie en Veiligheid (de Inspectie) heeft, evenals in 2019 en 2020, ook in 2021 onderzoek gedaan naar de toepassing van de hackbevoegdheid door de politie op basis van de Wet Computercriminaliteit III. Daartoe heeft de Inspectie in 2021 onderzoek uitgevoerd en verslag gedaan.

Het Verslag is inmiddels vastgesteld. Hierbij doe ik u het Verslag toekomen. Evenals vorig jaar zal ik via uw secretariaat een afspraak maken voor een gesprek op bestuurlijk niveau omdat u nauw bij dit onderwerp betrokken bent.

Vervolgtraject
Het Verslag is samen met de wederhoortabel aangeboden aan de minister van Justitie en Veiligheid. Conform de Aanwijzingen van de minister-president inzake rijksinspecties, wordt het Verslag uiterlijk zes weken na aanbieding aan de bewindspersoon gepubliceerd op de website van de Inspectie.

Met vriendelijke groet,

H.C.D. Korvinus
Inspecteur-generaal Inspectie Justitie en Veiligheid

Document 13

Kernconclusie

7.2 Toetsing van de inzet: centrale rol Digit-OM

• Aan de inzet van de bevoegdheid gaat een uitgebreid toetsingstraject vooraf door verschillende actoren. De technische toets vindt echter plaats bij een beperkt aantal personen. De rest van de actoren vaart op die deskundigheid.

7.3 Binnendringen in een geautomatiseerd werk

• Binnendringen kan niet altijd volledig op afstand, in tegenstelling tot wat de wetgever lijkt te hebben voorzien. Digit heeft daarom behoefte aan een (heimelijke) steunbevoegdheid die er momenteel niet is.

• De meldplicht ten aanzien van onbekende kwetsbaarheden geldt ook ten aanzien van kwetsbaarheden in geautomatiseerde werken die vrijwel alleen voor criminele doeleinden worden gebruikt. Dat is een knelpunt voor de opsporingsprakrijk, omdat personen met criminele intenties uiteindelijk op de hoogte moeten worden gebracht dat in hun systeem zich een kwetsbaarheid bevindt. Het is de vraag of dat werd bedoeld met het veiliger maken van computersystemen en het internet, een belangrijke reden waarom de meldplicht er is gekomen.

• Bij het grootste deel van de inzetten is, in tegenstelling tot de verwachting van de wetgever, gebruikgemaakt van een commercieel middel. Voor de opsporingspraktijk is de inzet van dat middel noodzakelijk. Zonder de inzet ervan zou het grootste deel van de inzetten op een telefoon niet mogelijk zijn geweest.

• De verplichting, voortvloeiend uit het Regeerakkoord, om bij een commercieel middel voor elke inzet een nieuwe licentie aan te schaffen, zorgt er hoogstwaarschijnlijk voor dat voor het gebruik ervan meer geld betaald wordt dan nodig is. Het is onwaarschijnlijk dat deze regeling voorkomt dat de markt van onbekende kwetsbaarheden gestimuleerd wordt.

7.4 Technische hulpmiddelen

• Er bestaat discussie over de precieze invulling van de begrippen technisch hulpmiddel en handmatige inzet.

• Vanwege de lange ontwikkel- en keuringstijd, is slechts een klein aantal eigen technische hulpmiddelen ontwikkeld en die zijn beperkt ingezet.

• Technische hulpmiddelen zijn tot nu toe maatwerk. Digit zou graag werken met een aantal standaardcomponenten dat al gekeurd is. Dat is tot nu toe (nog) niet mogelijk gebleken.

• Digit overweegt steeds vaker een handmatige inzet. Dat betekent dat een werkwijze niet altijd volledig afgeschermd kan blijven. Dat wordt door Digit niet in alle gevallen als problematisch gezien.

7.5 Keuring van technische hulpmiddelen

• De keuring van technische hulpmiddelen moet ervoor zorgen dat gegevens die verzameld worden, betrouwbaar, integer en herleidbaar zijn. Voor Digit is het keuringsproces een groot knelpunt. Dat heeft te maken met het feit dat de twee belangrijkste actoren, Digit en de Keuringsdienst, vanuit een verschillend perspectief naar het keuringsproces kijken.

• Inzet van een vooraf goedgekeurd middel is in de praktijk nauwelijks haalbaar.

• Het grootste deel van de inzetten heeft plaatsgevonden met een commercieel hulpmiddel waarvan de Digit-officier van justitie besloten heeft dat de aard van het middel zich tot nu toe verzet tegen een keuring. Dit hulpmiddel zal hoogstwaarschijnlijk ook niet goedgekeurd kunnen worden.

• In de uitvoeringspraktijk wordt (ook) gebruikgemaakt van tactische aanvullende waarborgen. Deze maken geen onderdeel uit van het keuringsproces.

7.6 Toezicht door de Inspectie

• De Inspectie richt zich op de naleving van regels en niet op de uitvoerbaarheid van die regels. Digit ervaart dit als lastig, omdat een deel van de regels in haar ogen niet uitvoerbaar is en Digit dus nooit aan die regels zal (kunnen) voldoen.
• Het is onduidelijk wat de consequenties zijn als de Inspectie constateert dat de regels niet worden nageleefd.
• De reikwijdte van het toezicht door de Inspectie leidt tot discussie. Die discussie wordt voor een belangrijk deel veroorzaakt door het feit dat het werk van Digit-OM en Digit-politie onlosmakelijk met elkaar verbonden is.
• Het is voor de Inspectie niet goed mogelijk om systeemtoezicht uit te voeren, omdat Digit niet beschikt over een (volledig) eigen kwaliteitssysteem. In de praktijk bestaat onduidelijkheid over wat onder een kwaliteitssysteem moet worden verstaan.

7.7 Inzetten met een internationale component

• De OM-aanwijzing (Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex. artikel 126nba Sv) richt zich op inzetten van Nederland op buitenlands grondgebied. In de OM-aanwijzing is niets geregeld voor inzetten op Nederlands grondgebied door het buitenland. Daardoor moeten ingewikkelde juridische constructies worden bedacht.

7.8 Functiescheiding

• Strikte functiescheiding tussen het tactisch team en Digit-politie is wat betreft de uitvoering van de hackbevoegdheid een problematisch concept. Het technisch en het tactisch team hebben elkaar nodig om optimaal uitvoering te kunnen geven aan de hackbevoegdheid.

Hoofdpunten

3.3 keuze en aanvraag inzet hackbevoegdheid

• Het intakeproces bestaat uit twee processen die deels op elkaar aansluiten en deels simultaan plaatsvinden: een operationeel proces en een procedure rondom de toetsing van de inzet.
• Aan ruim twee derde van de verzoeken van de tactische teams wordt geen uitvoering gegeven door Digit. Daarbij spelen zowel tactische als technische argumenten een rol.
• De versleuteling van gegevens(dragers) is in elk geval bij de inzetten die nader bestudeerd zijn de belangrijkste aanleiding om de hackbevoegdheid in te zetten.

3.4 operationeel proces

• Bij het intakeproces (de allereerste beoordeling of de bevoegdheid binnen een opsporingsonderzoek überhaupt zou kunnen worden ingezet) wordt naar juridische, tactische en technische aspecten gekeken.
• Digit kan vanuit capacitair oogpunt een beperkt aantal inzetten voor haar rekening nemen. Bovendien vergt elke inzet veel voorbereidingstijd.
• Het werken met een proefopstelling, onder andere bedoeld om te kijken naar neveneffecten, wordt kritisch bekeken, omdat de omgeving waarin gehackt wordt niet volledig voorspelbaar is. Bovendien zijn er hoge kosten verbonden aan het testen vanwege de wens om een identiek toestel aan te schaffen. In de wetsgeschiedenis wordt overigens niet duidelijk in welke mate een testapparaat moet lijken op het apparaat dat zal worden binnengedrongen.

3.5 Waarborgen voor controle voorafgaand aan de inzet

• Verschillende actoren zijn betrokken bij de vraag of de bevoegdheid in een concreet opsporingsonderzoek daadwerkelijk kan en mag worden ingezet. Digit-OM speelt hierbij, als vraagbaak en adviseur, een belangrijke rol. Vooral met betrekking tot de technische aspecten van een inzet.
• Details over de exacte wijze waarop binnengedrongen wordt maken geen onderdeel uit van de toetsing door de CTC en de rechter-commissaris.
• De uitgebreide toetsingsprocedure is een arbeidsintensief traject in vergelijking met sommige andere bijzondere opsporingsbevoegdheden. Voor de opsporingspraktijk kan het lastig zijn dat in geval van spoed er geen mondelinge procedure bestaat, zoals dat wel het geval is bij een verlenging.

4.2 Misdrijven en geautomatiseerde werken

• Inzetten door Digit vinden vooral plaats in opsporingsonderzoeken naar zwaardere vormen van traditionele criminaliteit.
• Er wordt binnengedrongen op een beperkt aantal typen geautomatiseerde werken. In de afgelopen twee jaar vooral op telefoons.
• Meestal beperkt de omschrijving van een geautomatiseerd werk in bijvoorbeeld een aanvraagproces-verbaal zich tot één of twee apparaten.

4.3 Binnendringen

• Het uitvoeren van de hackbevoegdheid kan niet altijd volledig op afstand gebeuren. Daarom heeft Digit behoefte aan een (heimelijke) steunbevoegdheid.
• Om binnen te dringen op telefoons is gebruikgemaakt van een commercieel middel.

• Digit is zich bewust van het feit dat er risico's zitten aan het gebruik van zo'n middel. Het gebruik ervan wordt echter noodzakelijk geacht om op een bepaald type geautomatiseerd werk (telefoons) binnen te kunnen dringen. Op dit type geautomatiseerd werk vindt het grootste deel van de inzetten plaats.

• Het licentiemodel, dat voortvloeit uit het Regeerakkoord, maakt de aanschaf van een commercieel middel duur. Het is dan ook de vraag of dit model ertoe leidt dat de markt van onbekende kwetsbaarheden minder gestimuleerd wordt.

• De meldplicht geldt ook voor geautomatiseerde werken die vrijwel alleen voor criminele doeleinden worden gebruikt. Dat betekent dat personen met criminele intenties uiteindelijk op de hoogte moeten worden gesteld dat in hun systeem zich een kwetsbaarheid bevindt, zodat zij veiliger gebruik kunnen (blijven) maken van hun systeem.

• De meldplicht van onbekende kwetsbaarheden kent nog een ander nadeel, namelijk dat de samenwerking met binnen- en buitenlandse partijen lastiger wordt, omdat zij doorgaans geen (vergelijkbare) meldplicht kennen.

• De meldplicht, in combinatie met de wens om het gebruik van commerciele middelen te beperken, is voor Digit ingewikkeld, omdat de meldplicht ervoor zorgt dat een eventueel eigen door Digit ontwikkeld product slechts één of twee keer bruikbaar is.

• Succesvol binnendringen is afhankelijk van een mix van factoren en omstandigheden.

4.4 onderzoekshandelingen

• In de wet wordt onderscheid gemaakt tussen verschillende onderzoekshandelingen die kunnen worden verricht (de verschillende opsporingsdoelen, subA t/m E). In de uitvoeringspraktijk blijkt een onderzoekshandeling onder meerdere subs te kunnen vallen. Dat gegeven is in de uitvoeringspraktijk soms onderwerp van discussie.

• In de praktijk wordt doorgaans géén stapsgewijze aanpak gehanteerd, waarbij eerst verkennend (subA) gestart wordt.

• De ontwikkeling van eigen hulpmiddelen (en ze vooraf goedgekeurd krijgen) is nauwelijks haalbaar gebleken in de praktijk in verband met de tijd die het kost om een volledig goedgekeurd middel te ontwikkelen.

• Eigen door Digit ontwikkelde hulpmiddelen worden tot nu toe slechts voor één zaak gebruikt, omdat een nieuwe zaak doorgaans vraagt om aanpassingen van het hulpmiddel.

• Digit kan ook een handmatige inzet doen en die optie wordt (steeds) vaker overwogen.

• Het is ingewikkeld gebleken om een goed werkend systeem te implementeren waarmee monitorgegevens (logging) worden bijgehouden. In het derde Verslag van de Inspectie (Inspectie JenV, 2022, p. 31) blijkt dat het proces van logging verbeterd is.

• Digit en het tactisch team werken nauw met elkaar samen. Strikte functiescheiding blijkt in de opsporingspraktijk niet haalbaar, omdat beide teams elkaar nodig hebben bij de uitvoering van de hackbevoegdheid.

4.5 Buitenland

• Digit is betrokken geweest bij een beperkt aantal inzetten met een internationale component. Het gaat hierbij om inzetten vanuit Nederland in het buitenland en om inzetten vanuit het buitenland in Nederland.

• Wat betreft standaardinzetten is in principe de afspraak dat niet op een telefoon wordt binnengedrongen die zich in het buitenland bevindt. Voor de maatwerkinzetten is wel of niet de bevoegdheid inzetten afhankelijk van de relatie met het betreffende land.

• De OM-aanwijzing wordt gebruikt als leidraad voor inzetten in het buitenland, maar is niet altijd toereikend (indien veel verschillende geautomatiseerde werken in het spel zijn zoals bij een botnet). In het geval dat van de OM-aanwijzing wordt afgeweken, wordt de Minister van Justitie en Veiligheid geïnformeerd.

• Inzetten met een internationale component kunnen vooral politiek ingewikkeld zijn.

• Inzetten door het buitenland in Nederland zijn op dit moment niet geregeld, ook niet in de OM-aanwijzing. Buitenlandse opsporingsfunctionarissen mogen geen hack uitvoeren op Nederlands grondgebied. Daardoor moeten ingewikkelde juridische constructies worden bedacht.

5.2 De Keuringsdienst

• De Keuringsdienst keurt technische hulpmiddelen die Digit zelf ontwikkeld heeft aan de hand van een keuringsprotocol. Dit protocol is gebaseerd op een aantal artikelen uit het Besluit dat ervoor moet zorgen dat het bewijs dat wordt verzameld betrouwbaar, integer en herleidbaar is.

• De Keuringsdienst kan alleen varen op wat zij zelf ziet tijdens een keuring. Wat Digit binnen haar eigen omgeving organiseert, wordt niet meegenomen tijdens de keuring, omdat die omgeving, in lijn met het Besluit, géén onderwerp van de keuring is.

• Het ontwikkelen van een (goed-)gekeurd technisch hulpmiddel neemt veel tijd in beslag. Daardoor is de inzet van een vooraf goedgekeurd hulpmiddel nauwelijks haalbaar gebleken in de praktijk.

• Voor Digit is het lastig werkbaar dat een aangepast middel, dat nog niet was goedgekeurd, volledig opnieuw gekeurd moet worden. De Keuringsdienst keurt een aangepast middel opnieuw, omdat alleen dan uitspraken kunnen worden gedaan over de werking van het middel en over de vraag of daarmee gegevens worden verzameld die betrouwbaar, herleidbaar en integer zijn.

• Digit-OM heeft besloten dat de aard van een gebruikt commercieel middel zich verzet tegen een keuring. Het middel zal op basis van het Besluit en de geformuleerde keuringseisen (hoogstwaarschijnlijk) ook niet goedgekeurd kunnen worden.

• Digit (en het tactisch team) nemen maatregelen in het kader van aanvullende tactische en technische waarborgen bij middelen die niet (goed)gekeurd zijn. Voor de tactische waarborgen is in het Besluit geen aandacht en dus worden deze niet meegenomen tijdens de keuring.

• Voor Digit vormt de keuring een belangrijk knelpunt. Dat heeft te maken met het feit dat de twee betrokken actoren (Keuringsdienst en Digit) vanuit verschillende perspectieven naar het keuringsproces kijken. Binnen het perspectief van waaruit de Keuringsdienst kijkt, staan vooral de regels centraal: een hulpmiddel kan alleen goedgekeurd worden als aan alle eisen uit het keuringsprotocol wordt voldaan (eventueel aangevuld met vervangende waarborgen), zodat de betrouwbaarheid, integriteit en herleidbaarheid van de verzamelde gegevens gegarandeerd kunnen worden. Binnen het perspectief van waaruit Digit naar de keuring van technische hulpmiddelen kijkt wordt vooral gekeken naar de uitvoerbaarheid en de noodzakelijkheid van de regels en de daarop gebaseerde eisen. Voor Digit zijn de regels en eisen lastig uitvoerbaar, onder andere omdat ze niet goed zouden passen bij de hulpmiddelen die Digit ontwikkelt. De regels zijn vooral gebaseerd op het 'oude' Besluit. Verder worden niet alle regels noodzakelijk geacht, omdat te weinig rekening is gehouden met risicoanalyses en bewijswaardes. Het zou niet nodig dat een technisch hulpmiddel aan alle keuringseisen voldoet. Digit doet een aantal suggesties die een oplossing zouden kunnen bieden voor de knelpunten die zij tegenkomt.

5.3 De Inspectie Justitie en Veiligheid

• De Inspectie kijkt, in lijn met hoe hier in de wetsgeschiedenis over gesproken wordt, of de uitvoering verloopt volgens het wettelijk kader. Zij kijkt niet naar de uitvoerbaarheid van hetgeen in de wet geregeld is (vergelijkbaar met hoe de Keuringsdienst kijkt naar de door Digit ontwikkelde

technische hulpmiddelen). Digit ervaar dit als lastig in verband met de ontwikkelfase waarin de uitvoering van de nieuwe bevoegdheid zich bevindt.

• De reikwijdte van het toezicht van de Inspectie is op dit moment onderwerp van gesprek, vooral ten aanzien van het handelen van het Openbaar Ministerie.

• De Inspectie is van oordeel dat zij nog géén goed systeemtoezicht kan uitoefenen, omdat Digit niet beschikt over een eigen kwaliteitssysteem. In de praktijk bestaat onduidelijkheid over wat precies onder een kwaliteitssysteem moet worden verstaan.

• Digit is met een deel van de door de Inspectie geconstateerde punten aan de slag gegaan, maar zegt ook met een deel ervan niets te zullen kunnen doen, omdat het Besluit op een aantal punten niet goed uitvoerbaar zou zijn.

• De reactie van de minister op de Verslagen van de Inspectie werkt bij de Inspectie op sommige punten verbazing, omdat daaruit blijkt dat aan haar constateringen niet altijd gevolgtrekkingen worden verbonden.

5.4 Het Openbaar Ministerie

• Digit-OM vervult gedurende de inzet voor alle betrokkenen de rol van vraagbaak en kijkt mee met de inzetten aan de Digit-politiekant. Indien nodig grijpt zij in.

• De zaaksofficier van justitie wordt vooral op de hoogte gehouden of de hackbevoegdheid resultaten oplevert. Daar waar nodig gaat ze na of op basis van informatie die beschikbaar komt, gehandeld moet worden.

5.5 Verlenging inzet bevoegdheid

• Het grootste deel van de inzetten is verlengd. Vaak is aanvullende informatie in het opsporingsonderzoek benodigd. Inmiddels is binnen Digit de afspraak gemaakt dat inzetten niet voor langere tijd verlengd kunnen worden (in principe maximaal twee keer).

• Een inzet wordt niet verlengd wanneer een zaak 'geklapt' is, het geautomatiseerde werk niet in gebruik blijkt bij de verdachte, of dat het onderzoek te weinig informatie oplevert.

• Bij de beslissing of een inzet verlengd wordt, zijn dezelfde actoren betrokken die zich bezighouden met de vraag of een inzet überhaupt binnen een opsporingsonderzoek mag plaatsvinden, inclusief het daarbij behorende tijdpad.

• De CTC bouwt inmiddels in haar advies een langere periode in (bijvoorbeeld twee maanden) waarin geprobeerd kan worden een geautomatiseerd werk binnen te komen. Daartoe is besloten, omdat anders te snel weer besloten moest worden over een verlenging.

6.3 Afronding inzet

• De verwijdering van een technisch hulpmiddel gebeurt doorgaans zo goed als volledig. Indien dat niet lukt, vindt overleg met de officier van justitie plaats en wordt een proces-verbaal opgemaakt.

• Rondom de verwijdering van gegevens inclusief geheimhoudersgegevens is er geen eenduidige regelgeving (het Besluit en artikel 126aa Sv spreken elkaar tegen). Digit-OM heeft daarom voor dit moment besloten dat geheimhoudersgegevens niet definitief verwijderd worden.

• Vanuit Digit-OM is wat betreft het verbaliseren het volgende kader meegegeven: minimaal verbaliseren (en maximaal journaliseren). Dit in verband met de afscherming van opsporingsmethoden.

6.4 Opbrengst tactisch onderzoek

• De resultaten van de bevoegdheid lijken vooralsnog vooral als sturingsinformatie te worden gebruikt.

6.5 Notificatieplicht

• De notificatieplicht is de verantwoordelijkheid van de zaaksofficier van justitie. Nog niet in elke zaak heeft notificatie plaatsgevonden, vooral omdat dat een opsporingsbelang zou kunnen schaden.

6.6 Toetsing zittingsrechter

• Er is, voor zover bekend, nog geen zaak inhoudelijk behandeld door een zittingsrechter waarbij de hackbevoegdheid is ingezet. Bij een deel ervan zal dat ook nooit gebeuren.

Document 14

Wetenschappelijk Onderzoek- en Documentatiecentrum
Ministerie van Justitie en Veiligheid

Startnotitie WODC-onderzoek

Aan	MT WODC
Van afdelingshoofd	[redacted]
Concipiënt	[redacted]
Datum	11 december 2019
Projectnummer	3106B

Werkt tel van het project

Evaluatie Wet Computercriminaliteit III: de bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk

Doelstelling van het project

Het doel van het voorgestelde onderzoek is de evaluatie van de onderdelen 126nba, 126uba en 126zba Sv van de Wet Computercriminaliteit III (hierna: Wet CCIII), namelijk de bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk met het oog op de opsporing van ernstige vormen van computercriminaliteit of andere ernstige misdrijven.

Probleemstelling

Wat zijn de mogelijkheden en knelpunten in de toepassing van de bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk bij de opsporing van ernstige vormen van computercriminaliteit of andere ernstige misdrijven en in hoeverre wordt hiermee voorzien in een leemte in de reeds bestaande wettelijke bevoegdheden?

Beleidscontext

Op 1 maart 2019 is de Wet CCIII in werking getreden.[1] Met de invoering van de Wet CCIII vinden diverse wetswijzigingen plaats, zowel van materieel- als formeelrechtelijke aard. Het voorgenomen onderzoek betreft een evaluatie van een onderdeel van de Wet CCIII, namelijk de bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk (artikel 126nba Wetboek van Strafvordering, hierna: Sv).[2] 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" (art. 80sexies Sr).

De bevoegdheid van onderzoek in een geautomatiseerd werk ten behoeve van de opsporing van ernstige vormen van computercriminaliteit of andere ernstige misdrijven,[3] heeft tot doel om toegang te verkrijgen tot de gegevens die in het geautomatiseerde werk zijn of worden verwerkt.[4] Het creëren van de bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk wordt noodzakelijk geacht vanwege voortschrijdende techniek en de toenemende mate waarin gebruik wordt gemaakt van geautomatiseerde werken voor communicatie en de verwerking en opslag van gegevens. De bestaande opsporingsbevoegdheden blijken niet afdoende in de bestrijding van ernstige (computer)criminaliteit. In de

[1] *Stb.* 2019, nr. 67. De wet is op 21 september 2018 in staatsblad gepubl ceerd (*Stb.* 2018, nr. 322).

[2] Zie Regeerakkoord 2017-2021 Vertrouwen in de Toekomst, p. 3. De overige onderdelen worden op een later moment geëvalueerd.

[3] De reikwijdte hiervan is onderwerp van onderzoek, zie onder 'onderzoeksvragen en toelichting' onderdeel B onder 2 in deze startnotitie.

[4] *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 7.

Memorie van Toelichting behorende bij de Wet CCIII worden in dit kader drie ontwikkelingen benoemd die in het bijzonder kunnen leiden tot problemen in de hedendaagse opsporingspraktijk, namelijk de toenemende mate waarin gebruik wordt gemaakt van standaardversleuteling, draadloze netwerken en/of anonimiseringstechnieken en cloudcomputingdiensten.[5]

Het onderzoek in een geautomatiseerd werk kan uitsluitend plaatsvinden in het kader van de opsporing met het oog op het verrichten van bepaalde onderzoekshandelingen, namelijk 1) de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of van de gebruiker, zoals de identiteit of locatie, en de vastlegging daarvan; 2) de vastlegging van gegevens die in het geautomatiseerde werk zijn of worden opgeslagen, 3) de ontoegankelijkmaking van gegevens; 4) de uitvoering van een bevel tot het aftappen en opnemen van communicatie of opnemen van vertrouwelijke communicatie en 5) de uitvoering van een bevel tot stelselmatige observatie.[6] Het binnendringen is voorbehouden aan daartoe aangewezen opsporingsambtenaren.[7] De ambtenaren die bevoegd zijn tot het binnendringen zijn onderdeel van een technisch team dat niet betrokken is bij het operationele onderzoek (Digital Intrusion Team; hierna: DIGIT).[8]

Het binnendringen in een geautomatiseerd werk kan met behulp van verschillende methoden worden gerealiseerd.[9] Daarbij kan gebruik worden gemaakt van een technisch hulpmiddel. Indien ten behoeve van het uitoefenen van de bevoegdheid software wordt ingekocht door opsporingsdiensten, worden (strenge) eisen gesteld aan zowel de software als de leverancier daarvan. In het Regeerakkoord 2017–2021 is afgesproken dat "[...] slechts in een specifieke zaak hacksoftware [zal] worden ingekocht door opsporingsdiensten. Leveranciers van dergelijke software worden gescreend door de AIVD en verkopen niet aan dubieuze regimes."[10] Conform de afspraken in het regeerakkoord zullen opsporingsdiensten alleen tot aanschaf van software overgaan indien daar in een specifieke casus noodzaak toe bestaat, zodat afname van de markt van dergelijke software tot een minimum wordt beperkt.[11]

Het is de vraag of de gestelde eisen een effectieve toepassing van de bevoegdheid in de praktijk belemmert. In het Regeerakkoord 2017–2021 wordt daarover opgemerkt: "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."[12]

Onderzoeksvragen en toelichting

Het onderzoeksgebied bestaat uit verschillende deelgebieden die onder te verdelen zijn in A) de achtergrond van de Wet CCIII; B) de reikwijdte van de wettelijke bepaling inzake de bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk; C) de toepassing van deze bevoegdheid in de praktijk, cijfers en resultaten; D) het technisch hulpmiddel en het binnendringen; E) het aankoopproces van binnendringsoftware en

[5] *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 10-11.
[6] *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 15-28.
[7] *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 14; 31 e.v.
[8] *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 14.
[9] *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 31 e.v.
[10] Regeerakkoord 2017-2021 Vertrouwen in de Toekomst, p. 3. Zie ook *Kamerstukken II* 2017/18, 34 372, nr. G, p. 10.
[11] *Kamerstukken II* 2017/18, 34 372, nr. G, p. 11.
[12] Regeerakkoord 2017-2021 Vertrouwen in de Toekomst, p. 3.

onbekende kwetsbaarheden; F) de keuring van een technisch hulpmiddel; G) de organisatie, procedures en het toezicht op de uitoefening van de bevoegdheid; I) de grensoverschrijdende toepassing van de bevoegdheid en J) privacyaspecten. Hieronder zijn deze deelonderwerpen uitgewerkt in 39 deelvragen:

A. Achtergrond van de Wet CCIII

1. Wat is de beleidstheorie achter de Wet CCIII, meer specifiek met betrekking tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk?
2. Hoe is het wetgevingstraject verlopen en wat heeft dit betekend voor de wijze waarop de Wet CCIII vorm heeft gekregen?
3. Welke opsporingsdoelen worden beoogd met de inzet van de bevoegdheid?

B. Reikwijdte van de bevoegdheid

4. Wat is de reikwijdte van de artikelen 126nba, 126uba en 126zba Sv, in het bijzonder met betrekking tot 'het misdrijf' waarbij de bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk mag worden ingezet en welke voorwaarden gelden daarbij?

C. Toepassing bevoegdheid – cijfers en resultaten

5. Hoe vaak en ten behoeve van welke misdrijven is de bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk ingezet?
    a. Hoe vaak betreft dit de inzet voor de in het Besluit onderzoek in een geautomatiseerd werk aangewezen misdrijven?
    b. Voor welke in het besluit aangewezen misdrijven is de bevoegdheid ingezet en hoe vaak?
6. Wat was de aanleiding van het toepassen van de bevoegdheid (versleuteling, draadloze netwerken, cloudcomputingdiensten of een combinatie daarvan)?
7. Ten behoeve van welke onderzoekshandeling(en) is de bevoegdheid ingezet?
8. Hoe vaak en bij welke misdrijven is de onderzoekshandeling succesvol geweest (in de zin dat toegang werd verkregen)?
9. Hoe vaak was de inzet niet succesvol en waarom?
10. Op welke wijze heeft de inzet van de bevoegdheid bijgedragen aan het onderzoek (bijvoorbeeld bewijs, sturingsinformatie, ontlastende informatie etc.)?
11. Hoe verhouden deze bijdragen zich tot de beoogde oorspronkelijke doelstellingen en verwachtingen ten aanzien van de inzet van de bevoegdheid?

D. Toepassing bevoegdheid – binnendringen en technisch hulpmiddel

12. Hoe vaak is gebruik gemaakt van binnendringsoftware?
13. Hoe vaak was dit een eigen programmatuur en hoe vaak een commercieel product?
14. Hoe vaak is geen gebruik gemaakt van binnendringsoftware?
15. Hoe vaak is met en zonder software succesvol binnengedrongen?
16. Welke soorten technische hulpmiddelen (aard en functionaliteit) zijn ingezet bij de uitvoering van onderzoekshandelingen?

E. Toepassing bevoegdheid – aankoopproces binnendringsoftware/mogelijk gebruik van onbekende kwetsbaarheden

17. Hoeveel tijd is gemoeid met de screening van leveranciers van binnendringsoftware?
18. Wat zijn de consequenties van de regeling omtrent de aankoop van binnendringsoftware voor opsporingsonderzoeken?
19. Hoe verhouden zich de kosten van het aanschaffen van meerdere licenties per onderzoek tot aanschaf voor algemeen gebruik?
20. Wordt het doel van het minder stimuleren van de markt behaald met deze regeling?
21. Hoe vaak en bij welk soort zaken wordt gebruik gemaakt van onbekende kwetsbaarheden voor het binnendringen, in die gevallen waarbij geen software is gebruikt?
22. Hoe vaak zijn onbekende kwetsbaarheden gemeld?
23. Hoe vaak, in hoeverre en bij welk soort zaken wordt gebruik gemaakt van de bevoegdheid om deze onbekende kwetsbaarheden niet te melden (art. 126ffa Sv)?

F. Toepassing bevoegdheid – keuring technisch hulpmiddel

24. Hoe vaak is een keuring aangevraagd voor een technisch hulpmiddel?
25. Hoeveel tijd is ingenomen door het keuren van een technisch hulpmiddel?
26. Hoe vaak is het technisch hulpmiddel afgekeurd en waarom?
27. Hoe vaak is door de officier van justitie bepaald dat een niet gekeurd technisch middel wordt gebruikt?
28. In hoeveel gevallen is keuring achterwege gebleven omdat de aard van het technische hulpmiddel zich daartegen verzet naar het oordeel van de officier?

G. Organisatie, procedures en toezicht

29. Hoeveel tijd neemt elke stap in elke respectievelijke procedure in beslag bij reguliere aanvragen (RC, CTC, interne keuring politie, toepassing)?
30. Hoeveel tijd neemt elke stap in elke respectievelijke procedure in beslag bij spoedaanvragen (RC, CTC, interne keuring politie, toepassing?)
31. Wat zijn de administratieve lasten die gepaard gaan met de inzet van de bevoegdheid en hoe zijn deze lasten verdeeld?
32. Welke knelpunten ervaren opsporingsinstanties bij het inzetten van de bevoegdheid?
33. Hoe is de toetsing door de CTC vormgegeven?
34. Hoe is het toezicht door de Inspectie Justitie en Veiligheid vormgegeven?
35. In hoeverre is het toezicht uitvoerbaar?
36. Heeft het toezicht aanleiding gegeven tot het aanpassen van de werkwijze t.b.v. de inzet van de bevoegdheid?

I. Grensoverschrijdende toepassing

37. In hoeverre biedt de OM-aanwijzing in het kader van mogelijke grensoverschrijdende toepassing van de bevoegdheid voldoende houvast?
38. Hoe vaak is gebruik gemaakt van dit kader?

J. Privacy

39. Welke afwegingen zijn gemaakt bij het inzetten van de bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk tussen de mate van inbreuk op de persoonlijke levenssfeer en het opsporingsbelang, met het oog op het voorgenomen middel (noodzaak, proportionaliteit en subsidiariteit)?

Spelen theorieën een rol in het onderzoek?

-

Methoden en technieken (voorzien gebruik van statistische tools)

In het verkrijgen van een antwoord op de hiervoor geschetste onderzoeksvragen wordt gebruik gemaakt van vier verschillende onderzoeksmethoden, namelijk 1) een literatuurstudie; 2) een dossierstudie; 3) interviews en 4) analyse van informatie uit overige databronnen.

Met een literatuurstudie wordt achtergrondinformatie verzameld. In de eerste plaats worden hiermee de totstandkoming en de structuur van de Wet CCIII in kaart gebracht. Daarnaast levert deze informatie een bijdrage aan de beantwoording van de aan deze evaluatie ten grondslag liggende onderzoeksvragen. In het algemeen draagt de literatuurstudie eraan bij een beeld te schetsen van het nut en de noodzaak die de bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk in theorie heeft bij de opsporing van ernstige vormen van computercriminaliteit of andere ernstige misdrijven. In het bijzonder kan de literatuurstudie bijdragen aan de beantwoording van de deelvragen met betrekking tot de beoogde reikwijdte van de bevoegdheid, en de organisatie en het toezicht met het oog op toepassing van de bevoegdheid.

Daarnaast wordt met een dossierstudie een bijdrage geleverd aan de beantwoording van de onderzoeksvragen, met name waar deze zien op toepassing van de bevoegdheid in de opsporingspraktijk. Een belangrijke bron van informatie wordt gevormd door informatie afkomstig uit opsporingsdossiers waarin de bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk is toegepast. Aangezien het een bevoegdheid betreft die recentelijk is ingevoerd, is het de verwachting dat de bevoegdheid gedurende de looptijd van deze evaluatie (twee jaren) in een beperkt aantal opsporingsonderzoeken zal worden toegepast. Bij voorkeur en indien voorhanden worden minimaal 10 dossiers bestudeerd, opgemaakt in de periode na inwerkingtreding van de Wet CCIII. Deze informatie zal onder andere worden verzameld bij het DIGIT en bij de eenheid of dienst die verantwoordelijk is voor de uitvoering van het opsporingsonderzoek waarin deze bevoegdheid werd ingezet. Het eerstgenoemde team is opgericht om de bevoegdheid tot het binnendringen uit te voeren.

Tevens zal informatie worden verzameld door middel van 40 semigestructureerde interviews. De interviews worden gehouden met personen betrokken bij opsporingsonderzoeken naar cybercriminaliteit die vanwege hun rol in het opsporingsonderzoek ook betrokken kunnen zijn bij de inzet van de bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk. De gesprekken zullen worden gevoerd met leden van de politie, (cyber)officieren van justitie, rechters-commissarissen en personen verbonden aan de inspectie Justitie en Veiligheid en de CTC, belast met het toezicht. Daarnaast wordt gesproken met personen betrokken bij het wetgevingsproces. De informatie die wordt verkregen draagt bij aan het beantwoorden van de onderzoeksvragen met betrekking tot de achtergrond en totstandkoming van de Wet CCIII, de reikwijdte en toepassing van de bevoegdheid in de praktijk (inzet bevoegdheid, bijdrage aan het onderzoek,

	mogelijkheden en knelpunten), de afweging die moet worden gemaakt tussen de mate van inbreuk op de persoonlijke levenssfeer, de keuze voor het opsporingsmiddel en het opsporingsbelang, en de vragen over de organisatie van en het toezicht op de inzet van de bevoegdheid. Tot slot wordt bij het verzamelen van informatie geput uit verschillende andere databronnen. Ten eerste betreft het bevel van de officier van justitie een bron van onderzoek. Hierin staat bijvoorbeeld vermeld voor welk misdrijf een machtiging wordt aangevraagd door de politie, de van toepassing zijnde feiten en omstandigheden, het doel dat met de inzet van de bevoegdheid is beoogd, de te verrichten (onderzoeks)handelingen en een beschrijving van het betreffende geautomatiseerde werk. Deze databron kan informatie leveren ter beantwoording van de onderzoeksvragen over de rijwijdte en de toepassing van de bevoegdheid. Ten tweede vormt de machtiging van de rechter-commissaris een bron van onderzoek. Hieruit kan bijvoorbeeld worden opgemaakt hoe een afweging is gemaakt tussen de mate van inbreuk op de persoonlijke levenssfeer en het opsporingsbelang (onder D). Ten derde wordt geput uit documenten van de CTC. De CTC is belast met het toezicht op de inzet van de bevoegdheid door de officier van justitie. Uit de documenten van de CTC kan worden opgemaakt welke overwegingen ten grondslag liggen aan de beslissing al dan niet in te stemmen met de inzet van de bevoegdheid. Daarnaast geven deze documenten inzicht in de manier waarop CTC een afweging maakt met betrekking tot de effectiviteit van de bevoegdheid, het afbreukrisico en het belang van het hanteren van de bevoegdheid in een concreet geval. Deze databron kan informatie leveren ter beantwoording van de onderzoeksvragen over de reikwijdte van de bevoegdheid, het toepassen van de bevoegdheid, het toezicht daarop en privacyaspecten. Tot slot wordt bij het verzamelen van gegevens geput uit stukken van de Inspectie Justitie en Veiligheid voor zover de Inspectie deze kan delen. Ook deze databron kan informatie leveren ter beantwoording van de onderzoeksvragen over de reikwijdte van de bevoegdheid, het toepassen van de bevoegdheid, het toezicht daarop en privacyaspecten
Gebruik bron(-nen) WODC? Zo ja, welke?	Lopend WODC-onderzoek naar opsporing en verstoring van cybercrime (projectnummer: 3004).
Wijze van uitvoering	Het voorgestelde onderzoek zal worden uitgevoerd door [redacted] (projectleider en onderzoeker), [redacted] (onderzoeker), [redacted] (onderzoeker) en [redacted] (senior onderzoeker).
Gevraagde producten en/of diensten (inclusief wijze van kennisoverdracht)	Nederlandstalig onderzoeksrapport (na afloop evaluatietermijn).
Controle en hergebruik data	-
Benodigde expertise	Juridische kennis, kennis van cybercriminaliteit, kennis van sociaalwetenschappelijke onderzoeksmethoden en -technieken.
Wijze van uitvoering	Intern
Worden persoonsgegevens	Doordat gedurende het onderzoek verschillende soorten persoonsgegevens worden verwerkt, wordt een PIA uitgevoerd.

verwerkt? Zo ja: wordt er een PIA uitgevoerd	
Risico's, onzekerheden, beslispunten	Het risico bestaat dat sommige gegevens die worden verzameld in het kader van de evaluatie van de Wet Computercriminaliteit III van dusdanig gevoelige aard zijn dat zij niet in het onderzoeksrapport kunnen worden opgenomen. Ook is het mogelijk dat, vanwege de relatief korte evaluatietermijn, de bevoegdheid slechts in een beperkt aantal gevallen is ingezet waardoor bij een bespreking van de verzamelde data een risico op herleidbaarheid ontstaat. Hierdoor is het mogelijk dat niet alle onderzoeksvragen in het rapport beantwoord kunnen worden.
Begeleidingscommissie	In het voorgestelde onderzoek zal een begeleidingscommissie worden samengesteld, bij voorkeur bestaande uit twee wetenschappers en een beleidsmedewerker. Voor de samenstelling van de begeleidingscommissie wordt gedacht aan de volgende personen: - [redacted] beoogd voorzitter) - [redacted] 5.1,2e en 5.2,1 - [redacted] - [redacted] - [redacted] Met het oog op de benodigde consultering van experts die in de opsporingspraktijk betrokken kunnen zijn bij de uitvoering van de bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk, zal tevens een klankbordgroep worden samengesteld. Bij de samenstelling van de klankbordgroep wordt gedacht aan personen werkzaam bij de volgende organisatie en/of onderdelen daarvan: - Politie - Belastingdienst, FIOD, KMar - Openbaar Ministerie
Overig (o.m. relevante eerdere onderzoeken)	'De digitalisering van georganiseerde misdaad', *Justitiële Verkenningen*, 2018(44)-5 (WODC/Boom juridisch). B.J. Koops e.a., *Misdaad en opsporing in de wolken. Knelpunten en kansen van cloud computing voor de Nederlandse opsporing*, Den Haag/Tilburg: WODC/TILT 2012. R. Leukfeldt, S. Veenstra, M. Domenie & W. Stol, *De strafrechtketen in een gedigitaliseerde samenleving. Een onderzoek naar de strafrechtelijke afhandeling van cybercrime,* Programma Aanpak Cybercrime 2012. G. Odinot, M.A. Verhoeven, R.L.D. Pool, C.J. de Poot, *Organised cybercrime in the Netherlands*. Den Haag: WODC. Cahier 2017-1. J.J. Oerlemans, *Investigating cybercrime* (diss. Leiden), Amsterdam: Amsterdam University Press 2017. J.J. Oerlemans, 'De wet computercriminaliteit iii: Meer handhaving op internet', *Strafblad*, 2017(15)-4, p. 350-359.

Document 15

OPENBAAR MINISTERIE

<Parket LOCATIE> <Landelijk Parket> <Functioneel Parket>

PROCES-VERBAAL VAN BEVINDINGEN

Proces-verbaalnummer:
Documentcode:
Onderzoek:

Betreft: aanvullende waarborgen ex artikel 21 lid 4 Bogw
Parketnummer:
RC-Nummer:

PROCES-VERBAAL

<Ik/Wij>, <naam1/nummer1>, officier van justitie, en <naam2/nummer2>, officier van justitie, verklaren het volgende:

Op <datum> werd onder <mijn/onze> leiding een opsporingsonderzoek gestart onder de naam <naam onderzoek>. In dit onderzoek is/zijn (een) bevel(en) ex artikel <126nba/126uba/126zpa> Sv afgegeven.

In dit/deze bevel(en) is ex artikel 21 lid 2 van het Besluit onderzoek in een geautomatiseerd werk (Bogw) bepaald dat een niet gekeurd technisch hulpmiddel werd gebruikt.

De uitvoering van dit/deze bevel(en) is gedaan door een technisch team van politie. Dit technisch team werkt onder gezag van een andere officier van justitie. Door deze officier van justitie is - ex artikel 21 lid 4 -beslist dat de aard van het technische hulpmiddel zich verzet tegen keuring na afloop van het gebruik. Keuring is om die reden achterwege gebleven. Daarvan is een apart proces-verbaal opgemaakt.

Aangezien in de processtukken geen gegevens - die ex artikel <126nba/126uba/126zpa> Sv zijn vergaard - als bewijsmiddel zijn opgenomen, <laat ik / laten we> een vermelding van de getroffen aanvullende waarborgen achterwege.

Waarvan door <mij/ons> is opgemaakt dit proces-verbaal, dat <ik sloot / wij sloten> en <ondertekende/ondertekenden> op <datum> te <locatie LP/AP>.

<naam/nummer> op <ambtseed/ambtsbelofte>

<naam/nummer> op <ambtseed/ambtsbelofte>

Document 16

OPENBAAR MINISTERIE

Landelijk Parket

Notitie

Aan	5.1.2e
Van	5.1.2e
Datum	28 augustus 2018
Onderdeel	HTC
Onderwerp	Uitgangspunten binnendringen in een geautomatiseerd werk
Aanleiding	Wet computercriminaliteit III
Bijlage(n)	-

1 Inleiding

Naar verwachting treedt op 1 januari 2019 de Wet computercriminaliteit III in werking. Onderdeel van deze wet is de zogenaamde hackbevoegdheid. Het wordt straks mogelijk om op afstand en heimelijk een geautomatiseerd werk binnen te dringen om daar onderzoek te verrichten.

Omdat het op dit moment ook al mogelijk is om op andere bevoegdheden een geautomatiseerd werk binnen te dringen, is er behoefte aan een overzicht. In welke gevallen moet er voor 126nba Sv worden gekozen en wanneer is er een andere optie?

Hieronder wordt op basis van de verschillende bevoegdheden, relevante wetsgeschiedenis en jurisprudentie een aantal uitgangspunten geformuleerd, voorzien van een (korte) toelichting.

2 Uitgangspunten

I. De 126nba Sv wordt (in beginsel) enkel gezien als de grondslag voor het heimelijk EN op afstand binnendringen in een geautomatiseerd werk in gebruik bij de verdachte.

In de Memorie van Toelichting wordt de bevoegdheid meermalen als zodanig geduid. Hieronder volgt een voorbeeld.

"Dit wetsvoorstel introduceert een bevoegdheid voor de daartoe aangewezen opsporingsambtenaren om, onder strikte voorwaarden, een geautomatiseerd werk dat in gebruik is bij een verdachte, op afstand heimelijk binnen te dringen en onderzoek te doen met het oog op de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker, zoals de identiteit en de locatie, en de vastlegging daarvan, de vastlegging van gegevens die in het geautomatiseerde werk zijn of worden opgeslagen, de ontoegankelijkmaking van gegevens, het

opnemen van communicatie of van vertrouwelijke communicatie en de stelselmatige observatie".[1]

II. Indien er heimelijk EN op afstand kan worden binnengedrongen op grond van een ander artikel - bijvoorbeeld de 125j Sv of 94 Sv - dan zal voor de lichtste bevoegdheid worden gekozen.

De lichtste bevoegdheid is in beginsel niet 126nba Sv. Uit 125j of 94 Sv volgt niet dat de rechter-commissaris daarvoor moet worden geraadpleegd en toestemming moet verlenen. Doch gelet op de inbreuk op de privacy die veelal wordt gemaakt als de volledige inhoud van een gegevensdrager wordt gekopieerd in combinatie met de heimelijkheid, zal in de toekomst vanuit het KEC in voorkomende gevallen worden geadviseerd om rechterlijke toetsing te zoeken.

De inwerkingtreding van artikel 126nba Sv neemt de huidige mogelijkheden om een geautomatiseerd werk binnen te dringen niet weg. Naast niet-heimelijke manieren om binnen te dringen, of fysieke mogelijkheden (dus niet op-afstand) waar hieronder verder op wordt ingegaan, is er ook een aantal bevoegdheden op basis waarvan specifiek heimelijk en op afstand kan worden binnengedrongen.

Zo is het op grond van artikel 125i Sv mogelijk om op een bepaalde locatie gegevens vast te leggen en daarbij op grond van artikel 125j Sv een geautomatiseerd werk op een andere locatie – en dus op afstand - te betreden. Artikel 125m Sv maakt het mogelijk de notificatie van deze doorzoeking uit te stellen en de inzet daarmee heimelijk te houden.

III. Indien er enkel heimelijk wordt binnengedrongen, maar niet op afstand - bijvoorbeeld bij toepassing van 126l Sv - dan wordt dat artikel – de 126l in dit voorbeeld - (in beginsel) als grondslag gebruikt.

Een inbreuk op de persoonlijke levenssfeer vereist vanuit artikel 8 EVRM o.a. een kenbare wettelijke basis en een bepaalde voorzienbaarheid. Vanuit het uitgangspunt dat artikel 126nba Sv de mogelijkheid biedt om heimelijk en op afstand een geautomatiseerd werk binnen te dringen, ligt artikel 126l Sv in de rede.

Op grond van artikel 126l Sv is het mogelijk om fysiek een technisch hulpmiddel te plaatsen dat communicatie opneemt. Artikel 126l Sv geeft ook de mogelijkheid om hiervoor een woning te betreden.

IV. Indien er enkel op afstand wordt binnengedrongen, maar niet heimelijk – bijvoorbeeld bij toepassing van artikel 126ng lid 2 Sv jo

[1] Memorie van Toelichting, p. 6.

181 Sv, 125j Sv of bij 94 Sv – dan wordt dat artikel – de 126ng lid 2, 125j of 94 Sv - (in beginsel) als grondslag gebruikt.

De mailbox van een verdachte kan worden gevorderd bij een provider op grond van artikel 126ng lid 2 Sv. Met machtiging van de rechter-commissaris. Echter, dit levert op dit moment in veel gevallen of zeer veel vertraging op of is onmogelijk vanwege het ontbreken van een rechtshulprelatie of verschillen in juridische mogelijkheden. In een aantal zaken is, om deze horde te passeren, de rechter-commissaris gevraagd om een machtiging ex artikel 126ng lid 2 Sv waarbij duidelijk wordt aangegeven aan de rechter-commissaris dat in plaats van of naast te vorderen (eerst/ook) wordt ingelogd met verkregen inloggegevens. Deze toepassing is heimelijk zeer complex vanwege detectie bij de mailprovider en het afbreukrisico dat hierdoor wordt gelopen. Er wordt veelal een bericht verzonden naar diverse (andere) gegevensdragers van de gebruiker dat er met een nieuw device is ingelogd. Dit bericht kan bijna niet worden voorkomen.

Na aanhouding van een verdachte mag op dit moment worden ingelogd op zijn/haar accounts in het kader van een netwerkzoeking (artikel 125j Sv). Het geldende standpunt van het KEC houdt in dat bij clouddiensten (Dropbox, Google (mail en Drive), Instagram er door de werking van deze cloudaanbieders niet meer is na te gaan wat de datalocatie betreft van de data van de verdachte. Daarmee ligt een politieke discussie over een soevereiniteitsschending niet voor de hand, immers de bedrijven zelf weten veelal niet waar de data staat opgeslagen en wiens soevereiniteit dan zou worden geschonden.

Na inbeslagname van dat account (94 Sv) kan wel onderzoek worden gedaan welke gegevens zich op dat moment in de gegevensdrager bevinden of via dat device zichtbaar zijn, doch voorkomen moet worden dat de gegevensdrager pas later wordt bekeken om daarmee extra informatie binnen te halen. Staat op gespannen voet met briefgeheim.

Na toestemming (artikel 32 Cybercrimeverdrag) mag er worden ingelogd op servers in het buitenland, als deze zich in een land bevinden dat is aangesloten bij het verdrag. Er is dan geen soevereiniteitsschending.

Naar mijn mening blijven bovengenoemde mogelijkheden bestaan na inwerkingtreding van artikel 126nba Sv, omdat er na aanhouding geen sprake meer is van heimelijkheid.

Vanwege het ontbreken van die heimelijkheid, is – anders dan bij uitgangspunt II. – inschakelen van de rechter-commissaris bij de toepassing van artikelen 125j en 94 Sv niet nodig, tenzij een zeer ingrijpende inbreuk wordt voorzien (Smartphone-arrest).

V. Indien er enkel sprake is van binnendringen, maar er geen onderzoekshandeling als bedoeld in artikel 126nba Sv plaatsvindt,

kan dat binnendringen mogelijk worden gegrond op artikel 3 Pw ervan uitgaand dat er daarmee niet een meer dan beperkte inbreuk op de privacy wordt gemaakt. Als slechts beperkte inbreuk wordt gemaakt, ligt artikel 3 Pw ook meer voor de hand dan 126nba Sv, in het licht van het subsidiariteitsvereiste.

Het is technisch bijvoorbeeld mogelijk om heimelijk en op afstand een geautomatiseerd werk binnen te dringen enkel om kort voor een doorzoeking een tweede gebruiker toe te voegen. Na in beslagname in het kader van een doorzoeking kan de computer / laptop dan gewoon worden betreden, ondanks dat verdachte deze heeft vergrendeld.

Het binnendringen levert dan mogelijk niet meer op dan een beperkte inbreuk op de privacy. Er is hier sprake van schending van de integriteit van het geautomatiseerde werk, welke – naar mijn mening – gedekt kan worden door artikel 3 Pw. De privacy-inbreuk komt pas aan de orde bij de doorzoeking en kan worden getoetst door de OvJ en rechter-commissaris.

VI. Indien er een geautomatiseerd werk wordt binnengedrongen dat niet in gebruik is bij de verdachte, dient het binnendringen te worden gegrond op een andere bevoegdheid dan de 126nba Sv.

Artikel 126nba Sv geeft enkel de bevoegdheid om een geautomatiseerd werk in gebruik bij een verdachte binnen te dringen.

VII. Artikel 32 lid 2 Cybercrimeverdag geeft de mogelijkheid om een geautomatiseerd werk binnen te dringen en gegevens veilig te stellen indien de persoon die gerechtigd is de gegevens via dat computersysteem te verstrekken, rechtmatig en vrijwillig toestemming geeft.

Artikel 32 lid 2 Cybercrimeverdrag luidt:

> Een Partij kan, zonder de toestemming van een andere Partij:
>
> via een computersysteem dat zich op haar grondgebied bevindt, zich toegang verschaffen tot of de beschikking krijgen over opgeslagen computergegevens die zich bevinden in een andere Staat, indien de Partij de rechtmatige en vrijwillige instemming verkrijgt van de persoon die gerechtigd is de gegevens via dat computersysteem aan de Partij te verstrekken.

Bij de uitleg daarvan hebben verdragspartijen nadrukkelijk zicht gehad op een bredere groep dan de directe gebruikers (verdachten) ook beheerders en anderen komen in aanmerking en kunnen dus ook toestemming geven.

Document 19

Inzet BOB-bevoegdheden ter ondersteuning van inzet ex art. 126nba Sv

Landelijk Parket - DIGIT

Inzet BOB-bevoegdheden

BOB-bevoegdheden kunnen volgens het wetboek van strafvordering worden toegepast in het kader van een opsporingsonderzoek, waarbij sprake is van een verdenking van een misdrijf (titel IVa), verdenking van het plegen of beramen van misdrijven in georganiseerd verband (titel V) of aanwijzingen van een terroristisch misdrijf (titel VB). Onder opsporing wordt verstaan het onderzoek in verband met strafbare feiten onder gezag van de officier van justitie met als doel het nemen van strafvorderlijke beslissingen (artikel 132a Strafvordering).

Gelet hierop bestaat de mogelijkheid een BOB-bevoegdheid in te zetten ter verkrijging van informatie om een andere BOB-bevoegdheid te kunnen inzetten. Immers is die eerste inzet ook gericht op het vergaren van informatie, die uiteindelijk van belang is voor het nemen van strafvorderlijke beslissingen. In dat kader wordt hieronder uiteen gezet onder welke omstandigheden en op welke wijze ten behoeve van de inzet van de bevoegdheid om binnen te dringen in een geautomatiseerd werk ondersteunende BOB-bevoegdheden kunnen worden ingezet. Hierbij wordt specifiek ingegaan op het inzetten van BOB-bevoegdheden om informatie te vergaren of doelen te verwezenlijken die van belang zijn voor het heimelijk binnendringen van een geautomatiseerd werk (art. 126nba Sv).

Geen afscherming nodig

Als uitgangspunt geldt hierbij dat – wanneer de inzet van een BOB-bevoegdheid via het onderzoeksteam kan verlopen – dit op reguliere wijze binnen het onderzoek wordt gedaan. Daarbij kan er voor worden gekozen om de omschrijving van het gevorderde te verruimen, zodat met de formulering afgeschermd wordt welke specifieke informatie voor de verdere inzet van art. 126nba Sv noodzakelijk was. Dit moet wel passen binnen de eisen die aan een specifieke bevoegdheid zijn gesteld.

DIGIT kan waar nodig adviseren bij de formulering in het aanvraag PV. De resultaten worden door het onderzoeksteam aan DIGIT verstrekt, zodat zij hiermee aan de slag kunnen.

Afscherming gewenst

In verband met de heimelijkheid van de methodes van het binnendringen is het niet altijd mogelijk dat het onderzoeksteam in kennis wordt gesteld van de informatie die noodzakelijk is voor de uitvoering van een bevel tot binnendringen in een geautomatiseerd werk. In dat geval zal de relevante informatie door DIGIT zelf (met vordering of bevel van de DIGIT officier van justitie) verkregen dienen te worden.

Indien inzet van de BOB-bevoegdheid afgeschermd dient te worden ter afscherming van opsporingsmethodes, wordt in beginsel de zaaksofficier en/of teamleider (in hoofdlijnen) geïnformeerd over de wenselijkheid van de inzet van een BOB-bevoegdheid. Dit mede om afbreukrisico's voor het gehele onderzoek goed te kunnen inschatten (en op voorhand de rechter-commissaris te informeren) indien de BOB-bevoegdheid wordt ingezet. Waar nodig kan binnen het OM slechts afstemming plaatsvinden op niveau van rechercheofficier.

LE DIGIT zal een aanvraag PV verzorgen, LP DIGIT zorgt voor de benodigde vorderingen, machtigingen en bevelen. De BOB-bevoegdheid wordt in beginsel ingezet in het lopende onderzoek, onder parketnummer van de verdachte waarbij een geautomatiseerd werk dient te worden binnengedrongen.

Indien gedurende een opsporingsonderzoek BOB-bevoegdheden worden ingezet, is het uitgangspunt dat alle stukken die voor de ter terechtzitting door de rechter te nemen beslissingen redelijkerwijs van belang kunnen zijn, opgenomen dienen te worden in de processtukken. Hiertoe behoren dan ook de stukken van de inzet van BOB-bevoegdheden door LE DIGIT.

> *Artikel 149a Strafvordering*
> *1. De officier van justitie is tijdens het opsporingsonderzoek verantwoordelijk voor de samenstelling van de processtukken.*
> *2. Tot de processtukken behoren alle stukken die voor de ter terechtzitting door de rechter te nemen beslissingen redelijkerwijs van belang kunnen zijn, behoudens het bepaalde in **artikel 149b**.*
> *3. Van een processtuk in elektronische vorm kan de integriteit worden nagegaan doordat iedere wijziging daarvan kan worden vastgesteld.*
> *4. Bij algemene maatregel van bestuur kunnen voorschriften worden gesteld over de wijze waarop de processtukken worden samengesteld en ingericht.*

Het achterwege laten van stukken in het procesdossier kan echter op de gronden van artikel 187d Strafvordering, bijvoorbeeld wanneer een zwaarwegend opsporingsbelang wordt geschaad. Dit kan na schriftelijke machtiging van de rechter-commissaris. Van een dergelijk zwaarwegend opsporingsbelang kan sprake zijn, indien voeging van de stukken zicht kan geven op benodigde gegevens of methoden van DIGIT bij het heimelijk binnendringen van een geautomatiseerd. Indien hiervan sprake is/kan zijn, wordt gevorderd deze stukken achterwege te laten. Indien mogelijk wordt dit reeds gemotiveerd in de aanvraag tot inzet van de betreffende BOB-bevoegdheid en wordt dit (gelijktijdig) door LP DIGIT bij de rechter-commissaris gevorderd.

> *Artikel 149b Strafvordering*
> *1. De officier van justitie is bevoegd, indien hij dit met het oog op de in artikel 187d, eerste lid, vermelde belangen noodzakelijk acht, de voeging van bepaalde stukken of gedeelten daarvan bij de processtukken achterwege te laten. Hij behoeft daartoe een **schriftelijke machtiging**, op diens vordering te verlenen door de rechter-commissaris. De vordering en de beschikking worden bij de processtukken gevoegd.*
> *2. De officier van justitie doet van de toepassing van het eerste lid en, voor zover de in artikel 187d, eerste lid, vermelde belangen dat toelaten, de redenen waarom, proces-verbaal opmaken. Dit proces-verbaal wordt bij de processtukken gevoegd.*

3. Zolang de zaak niet is geëindigd, bewaart de officier van justitie de in het eerste lid bedoelde stukken.

Artikel 187d Strafvordering

1. De rechter-commissaris kan hetzij ambtshalve, hetzij op de vordering van de officier van justitie of het verzoek van de verdachte of diens raadsman of de getuige beletten dat antwoorden op vragen betreffende een bepaald gegeven ter kennis komen van de officier van justitie, de verdachte en diens raadsman, indien er gegrond vermoeden bestaat dat door de openbaarmaking van dit gegeven:

a. de getuige ernstige overlast zal ondervinden of in de uitoefening van zijn ambt of beroep ernstig zal worden belemmerd,

b. een **zwaarwegend opsporingsbelang wordt geschaad**, of

c. het belang van de staatsveiligheid wordt geschaad.

2. De rechter-commissaris maakt in zijn proces-verbaal melding van de redenen waarom het bepaalde in het eerste lid toepassing heeft gevonden.

3. De rechter-commissaris neemt de maatregelen die redelijkerwijs nodig zijn om onthulling van een gegeven als in het eerste lid bedoeld, te voorkomen. Hij is daartoe bevoegd gegevens in processtukken onvermeld te laten.

Bij bevel van de officier van justitie tot uitvoering van een BOB-bevoegdheid en machtiging van de rechter-commissaris stukken achterweg te laten, gaat LE DIGIT over tot de inzet. De resultaten hiervan worden verwoord in proces-verbaal. In het dossier over de inzet van artikel 126nba Sv wordt dit betreffende proces-verbaal, alsmede onderliggende (BOB-) stukken, niet gevoegd. Volstaan zal worden met een verwijzing naar artikel 149d Strafvordering en voeging van de stukken die zien op de beslissing tot het achterwege laten van stukken.

Werkwijze

	TAAK	Wie?
1.	LE DIGIT overlegt met LP DIGIT over inzet BOB-bevoegdheid.	LE DIGIT LP DIGIT
	2a. Indien de inzet van BOB-bevoegdheid via het onderzoeksteam kan verlopen, doet het onderzoeksteam de resultaten van de inzet van de BOB-bevoegdheid of de machtiging en/of het bevel aan LE DIGIT toekomen, zodat LE DIGIT deze BOB-bevoegdheid kan inzetten. LP DIGIT adviseert – waar nodig – bij de aanvraag van de BOB-bevoegdheid.	Onderzoeks-team
	2b. Indien BOB-bevoegdheid binnen de DIGIT-omgeving moet worden ingezet, verloopt de procedure via LP DIGIT. Zie werkproces inzet BOB-bevoegdheden vanaf taak 3.	LP DIGIT
3.	LP of LE DIGIT informeert zaaksofficier en/of teamleider over de gewenste inzet.	LE DIGIT LP DIGIT
4.	LE DIGIT maakt proces-verbaal voor die inzet op, met onderbouwing voor achterwege laten van voeging van de stukken voor het procesdossier. LE DIGIT zendt dit PV aan de secretaris DIGIT.	LE DIGIT
5.	De secretaris DIGIT zorgt voor het bevel aan LE DIGIT en/of voor vordering aan RC in het arrondissement waar de zaak loopt. LP DIGIT vordert bij de RC (tevens) op grond van 149b Sv stukken achterwege te	LP DIGIT

	laten.	
7.	LE DIGIT zet deze BOB-bevoegdheid in.	LE DIGIT
8a.	De secretaris DIGIT houdt apart BOB-dossier bij voor inzet BOB-bevoegdheden en verzoeken om de stukken achterwege te laten. Deze stukken worden in de kluis bewaard.	LP DIGIT
8b.	De dossiervormer van LE DIGIT houdt apart BOB-dossier bij voor inzet BOB-bevoegdheden en verzoeken om de stukken achterwege te laten. Deze stukken worden in de kluis bewaard.	LE DIGIT
9a.	Aan het eind van de inzet van de hackbevoegdheid archiveert LP DIGIT het BOB-dossier bij het LP.	LP DIGIT
9b.	Aan het eind van de inzet van de hackbevoegdheid archiveert LE DIGIT het BOB-dossier bij de LE.	LP DIGIT
10.	LE DIGIT voegt in de stukken van uitvoering van de hackbevoegdheid dat toepassing is gegeven aan artikel 149d Sv bij de uitvoering, alsmede de stukken die zien op de beslissing tot het achterwege laten van stukken.	LE DIGIT

16 november 2020

LP DIGIT -5.1.2e

	Toegezonden	Afgerond
LP DIGIT	25-6-2020	7-10-2020
Afgestemd LE DIGIT	25-6-2020	30-9-2020
Rechercheofficier LP	3-11-2020	12-11-2020

Document 20

Juridische kaders voor binnendringen ex art. 126nba Sv

Landelijk Parket - DIGIT

Mogelijke vormen van binnendringen ex artikel 126nba Sv

In art. 126nba Sv is onderscheid te maken tussen het binnendringen en het verrichten van onderzoekshandelingen.[1] Het binnendringen is in het artikel niet nader uitgewerkt. De onderzoekhandelingen staan beschreven in het eerste lid onder sub a tot en met e.

Wat valt onder binnendringen wordt door de wetgever op een aantal plekken in de parlementaire geschiedenis benoemd.

De wetgever benadert binnendringen vooral technisch.

> "Voor de regeling rond het binnendringen van het geautomatiseerde werk is aangesloten bij de regeling van de computervredebreuk in het Wetboek van Strafrecht. Op grond van deze regeling is van binnendringen 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 (artikel 138ab, eerste lid, Sr)."[2]

De wetgever stelt voorop dat verschillende technieken niet limitatief zijn benoemd.[3] De volgende varianten zijn o.a. in de parlementaire geschiedenis benoemd:

- Binnendringen met behulp van inloggegevens die door middel van *social engineering* zijn verkregen.[4]
- Binnendringen met behulp van inloggegevens die door het gebruik van *kunstmatige intelligentie* zijn verkregen.[5]
- Binnendringen met behulp van inloggegevens van een persoon die worden verkregen door diegene te verleiden te reageren op een e-mailbericht of een ander verzoek om contact; *phishing*.[6]
- Binnendringen door het exploiteren van *bekende kwetsbaarheden* in software.[7]
- Binnendringen door het exploiteren van *onbekende kwetsbaarheden* in software.[8]
- Binnendringen door het verkrijgen van inloggegevens door *inlichtingenwerk*.[9]
- Binnendringen door in overleg met *beheerders* toegang tot een systeem of gegevens te verkrijgen.[10]

---

[1] Zie bijvoorbeeld: Kamerstukken II, 2015/16, 34 372, nr. 6, p. 63 (NV II)
[2] Kamerstukken II, 2015/16, 34 372, nr. 3, p. 15 (MvT)
[3] Kamerstukken II, 2015/16, 34 372, nr. 3, p. 34 (MvT), Kamerstukken II, 2015/16, 34 372, nr. 6, p. 72 (NV II) en Kamerstukken II, 2015/16, 34 372, nr. 27, p. 10
[4] Kamerstukken II, 2015/16, 34 372, nr. 3, p. 34 (MvT)
[5] Kamerstukken II, 2015/16, 34 372, nr. 3, p. 34 (MvT)
[6] Kamerstukken II, 2015/16, 34 372, nr. 3, p. 34 (MvT)
[7] Kamerstukken II, 2015/16, 34 372, nr. 3, p. 34 (MvT)
[8] Kamerstukken II, 2015/16, 34 372, nr. 3, p. 34 (MvT)
[9] Kamerstukken II, 2015/16, 34 372, nr. 6, p. 64 (NV II)

- Binnendringen door *spearphishing*.[11]
- Binnendringen door *brute forcing*.[12]
- Binnendringen door *dictionary attacks*.[13]
- Binnendringen door *shoulder surfing*.[14]
- Binnendringen met behulp van een *afgevangen wachtwoord*.[15]

Deze varianten zijn bij de parlementaire behandeling in beperkte mate uitgewerkt. Alleen bij phishing en social engineering is door de wetgever iets uitgebreider beschreven wat daaronder valt.

> "De «social engineering» en het verleiden van personen om te reageren op bijvoorbeeld een emailbericht zijn methoden om de inloggegevens te verkrijgen zodat een geautomatiseerd werk op afstand heimelijk kan worden binnengedrongen."[16]

> "Social engineering kan er op gericht zijn de verdachte te bewegen handelingen te verrichten zodat software wordt geplaatst op het geautomatiseerde werk dat hij gebruikt, met behulp waarvan verbinding met een andere computer mogelijk wordt gemaakt of met behulp waarvan inloggegevens kunnen worden meegelezen. Met phishing wordt geprobeerd de verdachte ertoe te bewegen bepaalde vertrouwelijke gegevens prijs te geven, zoals identificerende gegevens of inloggegevens. Bij de toepassing van deze methoden wordt dus uitgegaan van de – veelal onwetende – medewerking van de verdachte of van een derde die het geautomatiseerde werk gebruikt waarvan de verdachte ook gebruik maakt."[17]

> "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."[18]

<u>Juridische kaders voor binnendringen ex artikel 126nba Sv</u>

Bij diverse van de benoemde varianten van binnendringen zal in meer of mindere mate inbreuk worden gemaakt op de privacy van verdachte of derden. Daarnaast zijn beschreven handelingen in een aantal te brengen onder delictsomschrijvingen van in het wetboek van Strafrecht opgenomen misdrijven (zoals bijvoorbeeld oplichting) waardoor bij uitvoering ervan de beheersbaarheid en integriteit van de opsporing in het geding kan komen. Door de wetgever is bij de parlementaire behandeling niet uitgewerkt wat de juridische kaders zijn die gelden bij het binnendringen van een geautomatiseerd werk.

Voor de kaders waarbinnen DIGIT mag binnendringen geldt daarom het algemene normkader voor strafvorderlijk optreden.

---

[10] Kamerstukken II, 2015/16, 34 372, nr. 6, p. 64 (NV II)
[11] Kamerstukken II, 2015/16, 34 372, nr. 8, 11 en 13
[12] Kamerstukken II, 2015/16, 34 372, nr. 8, 11 en 13
[13] Kamerstukken II, 2015/16, 34 372, nr. 8, 11 en 13
[14] Kamerstukken II, 2015/16, 34 372, nr. 8, 11 en 13
[15] Kamerstukken II, 2015/16, 34 372, nr. 27, p. 10
[16] Kamerstukken II, 2015/16, 34 372, nr. 6, p. 67 (NV II)
[17] Kamerstukken II, 2015/16, 34 372, nr. 6, p. 72 (NV II)
[18] Kamerstukken II, 2015/16, 34 372, nr. 8, 11 en 13

Op grond artikel 3 Politiewet mogen opsporingsmedewerkers in het kader van de daadwerkelijke handhaving van de rechtsorde handelingen verrichten die een beperkte inbreuk op grondrechten van de verdachte maken en/of die niet zeer risicovol zijn voor de integriteit en beheersbaarheid van de opsporing.

Opsporingsmedewerkers van DIGIT kunnen binnen hun taakstelling handelingen verrichten om binnen te dringen in geautomatiseerde werken. Indien bij het binnendringen een meer dan geringe inbreuk op de privacy wordt gemaakt of het binnendringen zeer risicovol is voor de beheersbaarheid en integriteit van de opsporing, zal daarbij gebruik gemaakt moeten worden van een van de bijzondere opsporingsbevoegdheden die in het wetboek van strafvordering is benoemd of waarvoor de handelingen a contrario[19] aan een strafvorderlijke bepalingen kunnen worden genormeerd.

Bij de beoordeling van de kaders voor het binnendringen zal steeds nauwgezette afstemming met DIGIT LP plaats moeten vinden.

16 november 2020

LP DIGIT [redacted]

	Toegezonden	Afgerond
LP DIGIT	22-10-2020	3-11-2020
Afgestemd LE DIGIT	22-10-2020	3-11-2020
Afgestemd rechercheovj LP	3-11-2020	12-11-2020

[19] Vgl. HR 20 december 2011, ECLI:NL:HR:2011:BP0199 en HR 5 maart 2019, ECLI:NL:HR:2019:298

Document 23

Treffen aanvullende waarborgen bij [redacted]

Landelijk Parket - DIGIT

1. Inleiding

Bij de uitvoering van art. 126nba lid 1 Sv kan gebruik worden gemaakt van een technisch hulpmiddel (TH). Deze mogelijkheid is nader uitgewerkt in het Besluit onderzoek in een geautomatiseerd werk (Bogw).[1] In het Bogw is als uitgangspunt geformuleerd wordt gewerkt met een vooraf goedgekeurd TH (art. 21 lid 1 Bogw). Indien het onderzoek het dringend vordert, kan de OvJ echter bepalen dat gewerkt wordt met een niet gekeurd TH (art. 21 lid 2 Bogw). Het niet gekeurde TH wordt na afloop van de inzet in beginsel alsnog gekeurd. De OvJ kan echter ook bevelen dat een ingezet TH, dat vooraf niet gekeurd is, überhaupt niet wordt gekeurd. Dit kan indien "de aard" van het TH zich, naar het oordeel van de OvJ, tegen keuring verzet (art. 21 lid 4 Bogw).

2. [redacted]

[redacted] voldoet naar het oordeel van de landelijk DIGIT officier van justitie in afdoende mate aan de eisen die het Bogw stelt aan technische hulpmiddelen.

[redacted] maakt onderdeel uit van een samenstel aan hard- en software. Met dat samenstel kan ook binnengedrongen worden in geautomatiseerde werken (zodat vervolgens onderzoekshandelingen kunnen worden verricht). De vereiste binnendringsoftware (voor het binnendringen) en het TH (voor het verrichten van onderzoekshandelingen) zijn binnen het samenstel aan hard- en software onlosmakelijk met elkaar verbonden.

Ten aanzien van [redacted] is door de landelijk DIGIT officier van justitie reeds een aantal maal beslist dat de aard van dit TH zich tegen keuring verzet. De verwachting is dat de aard van [redacted] in de nabije toekomst niet zal wijzigen.

Gelet op het bepaalde in art. 21 lid 4 Bogw dienen er bij de inzet van [redacted] zogeheten aanvullende waarborgen[2] te worden getroffen. Deze aanvullende waarborgen moeten in de processtukken worden vermeld.

3. Aanvullende waarborgen tactisch team

De aanvullende waarborgen kunnen worden getroffen door zowel het tactisch als het technisch team. Ten behoeve van het tactisch team en de (zaaks)officier van justitie is door LP DIGIT een handreiking opgesteld met mogelijk waarborgen.[3] Het treffen van deze

---

[1] Besluit onderzoek in een geautomatiseerd werk, *Stb.* 2018, 340.

[2] Zie voor nadere duiding van 'aanvullende waarborgen' de notitie 'Waarborgen bij 126nba' van LP DIGIT van juni 2019.

[3] Deze handreiking is een dynamisch document dat doorlopend wordt aangevuld en aangepast met nieuwe inzichten of verificatie methodes.

waarborgen en de verslaglegging daarvan in de processtukken is de verantwoordelijkheid van het tactisch team en vindt plaats onder gezag van de (zaaks)officier van justitie. De noodzaak daartoe wordt voorafgaand aan een inzet met hen besproken door DIGIT LE en DIGIT LP.

4. Aanvullende waarborgen technisch team

Naast de aanvullende waarborgen die het tactisch team treft, worden er door het technisch team aanvullende waarborgen getroffen. Dit vindt plaats onder het gezag van de landelijk DIGIT officier van justitie.

Door het technisch team worden de werking en de functionaliteiten van 5.1.2c beschreven in een proces-verbaal. Deze beschrijving is beknopt. Een verdergaande of gedetailleerdere omschrijven van het gebruikte technisch hulpmiddel is in verband met zwaarwegende opsporingsbelangen niet mogelijk.

Daarnaast wordt [redacted]n beginsel - de werking van 5.1.2c getest op een zoveel mogelijk gelijkend geautomatiseerd werk (zowel qua hard- als software) als dat in gebruik is bij de verdachte. In deze test- en verificatieopstelling wordt gekeken welke in te zetten functionaliteiten door 5.1.2c worden ondersteund en onder welke voorwaarden. In dit kader wordt ook bekeken welk type gegevens van welke apps kunnen worden geregistreerd.

De functionaliteiten van het technisch hulpmiddel die in het bevel zijn opgenomen, worden vervolgens getest in een test- en verificatieopstelling.

5. Verslaglegging in proces-verbaal door het technisch team

Door het technisch team wordt in een proces-verbaal beschreven op welke wijze invulling is gegeven aan het treffen van de onder 4. genoemde aanvullende waarborgen.

Het proces-verbaal bevat daarnaast informatie over de wijze waarop invulling wordt gegeven aan de vereisten van artikel 8 tot en met 13 Bogw.[4] Het bevat tot slot informatie over het gebruik van de technisch infrastructuur, logging, beheer en beveiliging van de technische infrastructuur door het technisch team.

Het proces-verbaal heeft tot doel om inzicht te geven in het gebruik van [redacted] zodat ter terechtzitting mede op grond daarvan kan worden beoordeeld of de met [redacted] vastgelegde gegevens in voldoende mate betrouwbaar, integer en herleidbaar zijn om te kunnen worden gebruikt als bewijsmiddel in een strafzaak.

Het format van dit proces-verbaal is afgestemd met de landelijk DIGIT officier van justitie.[5] Het door DIGIT LE opgestelde format proces-verbaal voldoet in afdoende mate voor het genoemde doel.

25 oktober 2021

LP DIGIT [redacted]

	Toegezonden	Afgerond
LP DIGIT	17-08-2021	07-09-2021
Afgestemd LE DIGIT	17-08-2021	07-09-2021
Afgestemd rechercheovj LP	07-09-2021	25-10-2021

[4] Gerichte werking, detectie en registratie (art. 8 en 9 Bogw), betrouwbaarheid en integriteit (art. 10 Bogw), herleidbaarheid (art. 11 Bogw), datum en tijd (art. 12 Bogw) en transport (art. 13 Bogw).

[5] Dit proces-verbaal is een dynamisch document dat wordt aangevuld en aangepast met nieuwe inzichten

Document 24

Juridische kaders binnendringen ex art. 138ab Sr en art. 126nba Sv

Landelijk Parket - DIGIT

Inleiding

In art. 138ab Sr is het binnendringen van een geautomatiseerd werk strafbaar gesteld. In art. 126nba Sv is de bijzondere opsporingsbevoegdheid opgenomen die het mogelijk maakt om een geautomatiseerd werk binnen te dringen (en vervolgens onderzoekshandelingen te verrichten). Beide bepalingen zijn in zekere zin elkaars spiegelbeeld. In het wetboek van strafrecht is een handeling verboden die in het wetboek van strafvordering als bevoegdheid is opgenomen. In beide gevallen wordt met binnendringen hetzelfde bedoeld. In de parlementaire behandeling bij de Wet Computercriminaliteit III schrijft de wetgever:

> "Voor de regeling rond het binnendringen van het geautomatiseerde werk is aangesloten bij de regeling van de computervredebreuk in het Wetboek van Strafrecht. Op grond van deze regeling is van binnendringen 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 (artikel 138ab, eerste lid, Sr)."[1]

In dit stuk wordt een handreiking gegeven om te bepalen of sprake is van binnendringen in een geautomatiseerd werk.

Binnendringen - art 138ab Sr

In 1993 is met de Wet computercriminaliteit het binnendringen in een geautomatiseerd werk strafbaar gesteld. Tot 2010 stond de strafbepaling in art. 138a Sr (oud) opgenomen. In 2010 is door een vernummering de strafbaarstelling opgenomen art. 138ab Sr.

Art. 138ab lid 1 Sr luidt op dit moment als volgt:

> "Met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie wordt, als schuldig aan computervredebreuk, gestraft hij die opzettelijk en wederrechtelijk binnendringt in een geautomatiseerd werk of in een deel daarvan. Van binnendringen is in ieder geval sprake indien de toegang tot het werk wordt verworven:
> a. door het doorbreken van een beveiliging,
> b. door een technische ingreep,
> c. met behulp van valse signalen of een valse sleutel, of
> d. door het aannemen van een valse hoedanigheid."

De wetgever heeft vanaf het begin van strafbaarstelling gezocht naar een definiëring van binnendringen, maar lijkt niet tot een vastomlijnde afbakening te zijn gekomen. In eerste instantie hechtte de wetgever aan het bestaan van een minimale, maar wel daadwerkelijke

[1] Kamerstukken II, 2015/16, 34 372, nr. 3, p. 15 (MvT)

beveiliging die moest worden doorbroken.[2] Daar kwam de wetgever tijdens de behandeling van het wetsvoorstel weer op terug, om ook inloggen met het gebruik van een alom bekend (gelekt) wachtwoord onder de strafbaarstelling te laten vallen.[3] De wetgever verwoordde later in de behandeling dat van binnendringen sprake was, *"indien men zich de toegang verschaft tegen de onmiskenbare wil van de rechthebbende, welke zowel uit woorden als uit daden kan blijken"*. De wetgever duidt dat nader:

> *"Allereerst wordt onder a een expliciete handeling van de rechthebbende vereist, namelijk het aanbrengen van «enige beveiliging». Er zal een kenbare drempel moeten bestaan zodat onbevoegden zich niet simpelweg de toegang kunnen verschaffen."*

en

> *"Daarnaast stelt artikel 138a, onder b, strafbaar degene die een systeem binnendringt waarbij geen sprake is van doorbreking van enige beveiliging in strikte zin."* [4]

In 2004 heeft de wetgever in de tweede nota van wijziging van de wet Computercriminaliteit II het binnendringen verder verruimd.[5] Tot de wijziging met de wet Computercriminaliteit II was sub a – d cumulatief verwoord. Dat werd met [redacted]ieuwe tekst los gelaten. Sub a-d werden ingeleid met de tekst dat van binnendringen *in ieder geval* sprake was, als het viel onder een van die subs. De wetgever schrijft:

> *"Mede met het oog op een zo krachtig mogelijke bestrijding van het verschijnsel «hacking» acht ik het daarom wenselijk geen beperking aan te brengen maar artikel 138a zodanig te herformuleren, dat in beginsel ieder opzettelijk en wederrechtelijk binnendringen in een computer(systeem) bestraft kan worden. Daarom stel ik voor de onderdelen a en b van artikel 138a, die thans nog als voorwaarde voor strafbaarheid zijn geformuleerd, te formuleren als voorbeelden van gevallen waarin sprake is van «binnendringen», door aan te geven dat in die gevallen in ieder geval sprake is van binnendringen in de zin van dit artikel. Daarmee wordt voor de jurisprudentie de nodige ruimte geschapen om ook andere methoden waarmee toegang wordt verworven, als binnendringen aan te merken."*[6]

Met die laatste zin verplaatst de wetgever de zoektocht naar een afbakening van 'binnendringen' naar de rechter (en daaraan voorafgaand naar het Openbaar Ministerie en de opsporingsdiensten). Waarmee niet direct een oplossing wordt geboden, maar het probleem vooral verschuift. Iets wat door A[redacted] Knigge wat scherp werd verwoord op 22 februari 2011.

> *"Als de wetgever er niet in slaagt om een helder omlijnd begrippenapparaat te presenteren, mag van de rechter niet verwacht worden dat hij er wél chocola van weet te maken."* [7]

Uit het voorgaande volgt dat er bij het bepalen of sprake is van binnendringen in een geautomatiseerd werk veel ruimte is voor interpretatie in de rechtspraktijk. De wetgevingsgeschiedenis biedt wel een aantal handvatten. Net als jurisprudentie en wetenschappelijke literatuur.

---

[2] Kamerstukken II, 1990/91, 21 551, nr. 3, p. 16 (MvT)
[3] Kamerstukken II, 1990/91, 21 551, nr. 6, p. 31-32 (MvA)
[4] Kamerstukken II, 1990/91, 21 551, nr. 11, p. 18 (NV). NB. In de toenmalige tekst van art. 138a Sr (oud) waren de huidige sub b, c en d samengevoegd in sub b.
[5] Kamerstukken II, 2004/05, 26 671, nr. 7 (Nota van wijziging II).
[6] Kamerstukken II, 2004/05, 26 671, nr. 7, p. 31-32 (Nota van wijziging II).
[7] PHR 22 februari 2011, ECLI:NL:PHR:2011:BN9287 (Toxbot)

De conclusie[8] van Knigge bij het arrest van de Hoge Raad van 22 februari 2011[9] in de Toxbot zaak is daarbij lezenwaardig. Knigge schets niet alleen uitvoerig de parlementaire behandeling rond de vraag wat binnendringen is, maar verwoord ook in detail wat daarbij de problemen en onduidelijkheden zijn. Hij formuleert ook een criterium dat voor de praktijk waardevol is als centrale vraag bij het bepalen of sprake is van binnendringen van een geautomatiseerd werk.

> "Art. 138a Sr vraagt om een normatieve invulling die functioneel is, die voorziet in een effectieve strafrechtelijke bescherming tegen onbevoegde kennisneming van in geautomatiseerd werken opgeslagen gegevens. Het criterium voor de vraag of onbevoegd gebruik is gemaakt van de ingeprogrammeerde toegangsmogelijkheden van een geautomatiseerd systeem, zou ik dan ook, wat de toegang door middel van telecommunicatie betreft, willen zoeken in hetgeen in het maatschappelijk (internet)verkeer algemeen geaccepteerd is. Alle methoden van toegangverschaffing die het normale, algemeen geaccepteerde gebruik van de programmatische mogelijkheden van op de telecommunicatie-infrastructuur aangesloten systemen te buiten gaan, leveren in beginsel het onbevoegd gebruik van die mogelijkheden op."[10]

Die overweging zou je kunnen vatten in de volgende vraag:

- Ging de toegang verschaffing verder dan het normale, algemeen geaccepteerde gebruik van de programmatische mogelijkheden van het geautomatiseerd werk?

Bij positieve beantwoording van die vraag zou je kunnen stellen dat sprake is van binnendringen in een geautomatiseerd werk.

Naast deze aan Knigge's conclusie ontleende vraag, kunnen de volgende vragen helpen bij het beoordelen of sprake is van binnendringen in het geautomatiseerd werk.

- Heeft men zich de toegang verschaft tot een geautomatiseerd werk tegen de onmiskenbare wil van de rechthebbende, welke wil zowel uit woorden als uit daden kan blijken?[11]
- Is er een kenbare drempel in het geautomatiseerd werk overschreden?[12]
  NB. Als louter sprake is van onbelemmerde toegang, is geen sprake van binnendringen.
- Hebben handelingen tot doel om het technisch functioneren van het geautomatiseerde werk zodanig te veranderen dat, ondanks het ontbreken van bijvoorbeeld de juiste toegangscodes of -gegevens, toegang verworven kan worden?[13]
- Is voorgewend dat sprake was van een autorisatie door de 'rechthebbende'?
- Is er gebruik gemaakt van een wachtwoord of ander (inlog)gegeven door iemand die daartoe niet gerechtigd was?

---

[8] PHR 22 februari 2011, ECLI:NL:PHR:2011:BN9287 (Toxbot)
[9] HR 22 februari 2011, ECLI:NL:HR:2011:BN9287 (Toxbot)
[10] Punt 77 in PHR 22 februari 2011, ECLI:NL:PHR:2011:BN9287 (Toxbot)
[11] Kamerstukken II, 1990/91, 21 551, nr. 11, p. 18 (NV).
[12] Kamerstukken II, 1990/91, 21 551, nr. 11, p. 18 (NV).
[13] Kamerstukken II, 2004/05, 26 671, nr. 7, p. 31-32 (Nota van wijziging II).

In het SDU Commentaar Strafrecht op artikel 138ab geven Gerritsma-Breur en Nederlof een mooie serie voorbeelden van binnendringen in een geautomatiseerd werk.[14]

- Het tegen de wil van de rechthebbende binnendringen in een computer langs een weg die de aanwezige beveiliging niet of onvoldoende afsluit, waarbij niet van belang is of die opening inherent is aan het systeem of is veroorzaakt door andere hackers.
- Het laten crashen van het inlogprogramma, zodat iedereen zonder verdere controle toegang heeft tot het geautomatiseerde werk.
- Het buiten de reguliere vragenstructuur om verleiden van een server om informatie te geven.
- Het versturen van een hyperlink naar slachtoffers die bij het openen van deze link een virus binnenhalen waarmee anderen toegang kunnen verkrijgen tot de computer.
- Een wachtwoord dat wordt gebruikt door iemand die daartoe niet gerechtigd is.
- Het inloggen op een besloten gedeelte van een site waartoe iemand vanwege wisseling van dienstverband niet meer gerechtigd was.
- Het gebruiken van een IP-[redacted]dres dat bij het te hacken systeem bekend is of als vriendelijk wordt beschouwd en daarmee mogelijk automatisch toegang verkrijgt tot het systeem.
- Het verleiden van de mens om persoonlijke gegevens zoals een wachtwoord af te geven ('social engineering') en die gegevens gebruiken om in te loggen.
- Een technische variant van social engineering, waarbij iemand via een opgemaakte nepsite wordt verleid zijn inloggegevens af te geven en die gegevens vervolgens gebruiken om in te loggen.
- Een computer de naam geven van de printserver en zo (als printer) toegang te krijgen tot de gegeven printopdrachten.
- Het zodanig manipuleren van het technisch functioneren van het geautomatiseerde werk, dat ondanks het ontbreken van het juiste wachtwoord toegang kan worden verkregen.

Tot slot wordt een voorbeeld gegeven dat mooi markeert hoe breed deze strafbepaling kan zijn:

- Indien iemand zich na een fysieke inbraak in een woning toegang verschaft tot een zich in die woning bevindende computer, is sprake van binnendringen in die computer in de zin van art. 138ab Sr.[15]

De huidige strafbaar stelling van binnendringen in een geautomatiseerd werk, heeft zijn oorsprong in het Cybercrime verdrag[16] en het Kaderbesluit over aanvallen op informatiesystemen[17]. Beide spreken echter niet over binnendringen', maar hanteren de term 'toegang' tot een computersysteem of een onderdeel daarvan, danwel een informatiesysteem.

Op 1 maart 2019 werd de Wet Computercriminaliteit III ingevoerd. Daarmee werd onder andere artikel 138c van het Wetboek van Strafrecht gewijzigd. Met die wijziging werd het

[14] C.M. Gerritsma-Breur & A.G. Nederlof in: Sdu Commentaar Strafrecht, art. 138ab Sr (online, bijgewerkt 7 mei 2019)
[15] Kamerstukken I, 2005/06, 26 671, nr. D, p. 3. (MvA I)
[16] Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, Boedapest, 23-11-2001
[17] Kaderbesluit 2005/222/JBZ van de Raad van 24 februari 2005 over aanvallen op informatiesystemen (PbL 2005/69, blz. 67).

wederrechtelijk overnemen van niet-[redacted]penbare gegevens strafbaar gesteld. In de toelichting op die wijziging schrijft de wetgever:

> *"De voorgestelde strafbepaling is, in aanvulling op de strafbaarstelling van computervredebreuk, vooral van belang voor gevallen waarin de dader rechtmatige toegang heeft tot niet-openbare gegevens van een computer, en deze gegevens wederrechtelijk overneemt."*
> en
> *"Hiermee wordt tegemoet gekomen aan situaties waarin personen gegevens van een computer waartoe zij rechtmatige toegang hebben, bijvoorbeeld vanwege hun functie bij een overheidsinstelling, zonder daartoe gerechtigd te zijn voor zichzelf of voor een ander overnemen."* [18]

Het lijkt er op dat de wetgever met deze aanvulling op de strafbaar stelling van het binnendringen van een geautomatiseerd werk, weer aansluiting zoekt bij de term 'toegang' van het eerder genoemde het Cybercrime verdrag en het Kaderbesluit. Daaruit zou kunnen worden afgeleid dat binnendringen en het opzettelijk en wederrechtelijk verwerven van toegang synoniem zijn.

<u>Binnendringen [redacted]rt 126nba Sv</u>

Over de term binnendringen in de context van art. 126nba Sv, is nog geen rechtspraak gepubliceerd. Evenmin wordt er in (wetenschappelijke) handboeken nader over geschreven.

Anders dan in de parlementaire behandeling van art. 138ab Sr en art. 138a Sr (oud), heeft de wetgever bij de behandeling van art. 126nba Sv wel concreter gemaakt wat hij ziet als binnendringen.

De wetgever stelt voorop dat verschillende technieken niet limitatief zijn benoemd.[19] De volgende varianten zijn o.a. in de parlementaire geschiedenis benoemd:

- Binnendringen met behulp van inloggegevens die door middel van *social engineering* zijn verkregen.[20]
- Binnendringen met behulp van inloggegevens die door het gebruik van *kunstmatige intelligentie* zijn verkregen.[21]
- Binnendringen met behulp van inloggegevens van een persoon die worden verkregen door diegene te verleiden te reageren op een e-[redacted]ailbericht of een ander verzoek om contact; *phishing*.[22]
- Binnendringen door het exploiteren van *bekende kwetsbaarheden* in software.[23]
- Binnendringen door het exploiteren van *onbekende kwetsbaarheden* in software.[24]
- Binnendringen door het verkrijgen van inloggegevens door *inlichtingenwerk*.[25]
- Binnendringen door in overleg met *beheerders* toegang tot een systeem of gegevens te verkrijgen.[26]

[18] Kamerstukken II, 2015/16, 34 372, nr. 3, p. 64 (MvT),
[19] Kamerstukken II, 2015/16, 34 372, nr. 3, p. 34 (MvT), Kamerstukken II, 2015/16, 34 372, nr. 6, p. 72 (NV II) en Kamerstukken II, 2015/16, 34 372, nr. 27, p. 10
[20] Kamerstukken II, 2015/16, 34 372, nr. 3, p. 34 (MvT)
[21] Kamerstukken II, 2015/16, 34 372, nr. 3, p. 34 (MvT)
[22] Kamerstukken II, 2015/16, 34 372, nr. 3, p. 34 (MvT)
[23] Kamerstukken II, 2015/16, 34 372, nr. 3, p. 34 (MvT)
[24] Kamerstukken II, 2015/16, 34 372, nr. 3, p. 34 (MvT)
[25] Kamerstukken II, 2015/16, 34 372, nr. 6, p. 64 (NV II)
[26] Kamerstukken II, 2015/16, 34 372, nr. 6, p. 64 (NV II)

- Binnendringen door *spearphishing*.[27]
- Binnendringen door *brute forcing*.[28]
- Binnendringen door *dictionary attacks*.[29]
- Binnendringen door *shoulder surfing*.[30]
- Binnendringen met behulp van een *afgevangen wachtwoord*.[31]

Deze varianten zijn bij de parlementaire behandeling in beperkte mate uitgewerkt. Alleen bij phishing en social engineering is door de wetgever iets uitgebreider beschreven wat daaronder valt.

> "De «social engineering» en het verleiden van personen om te reageren op bijvoorbeeld een emailbericht zijn methoden om de inloggegevens te verkrijgen zodat een geautomatiseerd werk op afstand heimelijk kan worden binnengedrongen."[32]

> "Social engineering kan er op gericht zijn de verdachte te bewegen handelingen te verrichten zodat software wordt geplaatst op het geautomatiseerde werk dat hij gebruikt, met behulp waarvan verbinding met een andere computer mogelijk wordt gemaakt of met behulp waarvan inloggegevens kunnen worden meegelezen. Met phishing wordt geprobeerd de verdachte ertoe te bewegen bepaalde vertrouwelijke gegevens prijs te geven, zoals identificerende gegevens of inloggegevens. Bij de toepassing van deze methoden wordt dus uitgegaan van de – veelal onwetende – medewerking van de verdachte of van een derde die het geautomatiseerde werk gebruikt waarvan de verdachte ook gebruik maakt."[33]

> "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."[34]

Hoewel deze voorbeelden enige richting geven, blijven ze behoorlijk abstract en geven ze veelal invulling aan de voor de hand liggende gevallen van binnendringen.

Conclusie

De conclusie van het voorgaande is dat er geen harde richtlijnen te geven zijn voor het beantwoorden van de vraag of sprake is van binnendringen in een geautomatiseerd werk. De wetgever heeft daarbij veel ruimte gelaten aan de zittingsrechter en daarmee (impliciet) aan het Openbaar Ministerie en de opsporingsdiensten bij de duiding van gedragingen ten aanzien van geautomatiseerde werken. Het algemene beeld daarbij is dat de wetgever gekozen heeft voor een zeer brede strafrechtelijk rechtsbescherming. De definitie van geautomatiseerd werk in art. 80sexies Sr omvat een zeer grote groep van apparaten. Vervolgens zal zeer snel sprake kunnen zijn van binnendringen in dat geautomatiseerd werk.

[27] Kamerstukken II, 2015/16, 34 372, nr. 8, 11 en 13
[28] Kamerstukken II, 2015/16, 34 372, nr. 8, 11 en 13
[29] Kamerstukken II, 2015/16, 34 372, nr. 8, 11 en 13
[30] Kamerstukken II, 2015/16, 34 372, nr. 8, 11 en 13
[31] Kamerstukken II, 2015/16, 34 372, nr. 27, p. 10
[32] Kamerstukken II, 2015/16, 34 372, nr. 6, p. 67 (NV II)
[33] Kamerstukken II, 2015/16, 34 372, nr. 6, p. 72 (NV II)
[34] Kamerstukken II, 2015/16, 34 372, nr. 8, 11 en 13

Dit betekent voor de opsporingspraktijk dat voor een deel van handelingen ten aanzien van geautomatiseerde werken niet op voorhand duidelijk is of die als binnendringen van het geautomatiseerd werk moeten/kunnen worden aangemerkt. Ongeacht of dat handelingen zijn die door verdachten worden begaan bij het plegen van strafbare feiten of door opsporingsambtenaren bij het opsporen daarvan.

De beoordeling zal steeds casuïstisch zijn en resulteren in een bepleitbaar standpunt, in plaats van een vastomlijnd criterium of handvat. Het is daarom aan te bevelen om voor die beoordeling overleg te voeren met ter zake gespecialiseerde juristen, zoals cybercrime officieren van justitie en [redacted]arketsecretarissen, medewerkers van het Kennis en Expertisecentrum Cybercrime (KEC) van het Landelijk Parket en de operationeel juristen van politie die zich bezig houden met cybercrime en digitale opsporing.

21 december 2021

LP DIGIT [redacted]

	Toegezonden	Afgerond
LP DIGIT	9-6-2021	21-12-2021
Afgestemd LE DIGIT	9-6-2021	21-12-2021

Document 25

Standpunt | Opnemen communicatie of vastleggen gegevens?

Landelijk Parket - Digit

Het aftappen van communicatie

VS

Het vastleggen van (voor of na afgifte van het bevel) opgeslagen gegevens

Op 1 maart 2019 is de Wet computercriminaliteit III ("Wet CCIII") in werking getreden. Deze wet heeft onder meer een nieuwe opsporingsbevoegdheid gecreëerd, de hackbevoegdheid ex artikel 126nba Wetboek van Strafvordering ("Sv").

Een belangrijke reden voor het creëren van deze bevoegdheid is de toenemende versleuteling van gegevens.[1] Dit geldt ook voor het aftappen en opnemen van communicatie. In de Memorie van Toelichting op de Wet CCIII wordt overwogen (p. 9):

> Daarnaast wordt de effectiviteit van het aftappen en opnemen van communicatie ernstig verminderd door de encryptie van gegevens. Dit betreft de versleuteling van gegevens in transit. Het aftappen en opnemen van communicatie kan plaatsvinden door middel van een telefoon-, e-mail-, of internettap (artikelen 126m, 126t en 126zg Sv). Ook kan opgeslagen communicatie worden gevorderd van de aanbieder (artikel 126ng Sv). De inzet van deze bevoegdheden biedt echter geen resultaat in gevallen waarin gebruik wordt gemaakt van moderne versleuteling. Het aftappen en opnemen van communicatie, waarbij gebruik wordt gemaakt van de diensten van een openbare aanbieder van communicatie, levert slechts gegevens waaruit de inhoud van de communicatie niet kan worden afgeleid. Weliswaar is de aanbieder gehouden mee te werken aan het ongedaan maken van de versleuteling van de communicatie (artikel 126m, zesde lid, en 126nh, eerste lid, Sv), maar de aanbieder is hiertoe soms vaak niet in staat (bijvoorbeeld Skype), valt niet onder definitie van aanbieder (artikel 126la Sv) of is gevestigd in het buitenland. Ook kan er sprake zijn van meerdere lagen beveiliging, waarbij niet de ontsleuteling van iedere laag in handen is van een aanbieder. Dit is hierboven reeds aan de orde gekomen. Voor wat betreft het Tor-netwerk is wezenlijk dat een uitgebreid netwerk van tussenstations wordt gebruikt om de data over te dragen. Verschillende datapakketten volgen een willekeurige route langs zogeheten relaisstations, waarbij ieder station uitsluitend het IP-adres van het vorige en het eerstvolgende relaisstation in de keten kent. Hierdoor is er geen aanknopingspunt om

[1] Kamerstukken II 2015/16, 34372, 3, p. 8.

bijvoorbeeld een IP-tap in te zetten of gegevens bij een aanbieder van een communicatiedienst te vorderen.

Met als conclusie:

> De opsporing heeft dan ook dringend behoefte aan de mogelijkheid om de communicatie te kunnen onderscheppen *voordat* deze wordt versleuteld of *nadat* deze is ontsleuteld. Dit betekent dat de communicatie wordt afgetapt en opgenomen op het geautomatiseerde werk, voordat de gegevens worden verzonden of nadat deze ontvangen zijn en de communicatie door de software op het geautomatiseerde werk van de ontvanger is ontsleuteld. Daardoor verschuift de oriëntatie van het aftappen van de verbinding, door middel waarvan de communicatie tussen de deelnemers wordt overgedragen, naar het aftappen op de bron of het doel van de communicatie, te weten de computer of de mobiele telefoon met behulp waarvan de communicatie wordt gecommuniceerd («aftappen op het apparaat»).

In de nieuwe bevoegdheid is dan ook in artikel 126nba lid 1 sub b Sv het aftappen van communicatie als mogelijk onderzoek opgenomen.

Wat opvalt aan bovenstaande toelichting op het aftappen is dat met deze nieuwe wijze van aftappen (het «aftappen op het apparaat») het (ooit strikte) onderscheid tussen opgeslagen en stromende gegevens verder vervaagt. Immers, communicatie die nog niet is verzonden of reeds is ontvangen, is per definitie niet (meer) stromend.

Dat op zich is geen probleem. Het onderscheid is ook al eerder, bij de behandeling van de Wet computercriminaliteit ii (2) vanuit diverse hoeken bekritiseerd omdat het niet zou passen bij de huidige stand van de techniek.[1] Door de toenmalige minister werd er daarom ten aanzien van de tapbevoegdheid ook al gesproken van enerzijds onderzoek naar reeds bestaande gegevens en anderzijds het onderzoek gedurende een zekere tijd naar gegevens die op het moment van aanvang van het onderzoek nog niet bestaan (dat wil zeggen toekomstige gegevens).

Echter, het doet wel de vraag rijzen naar het verschil met de onderzoeksmogelijkheid van artikel 126nba lid 1 sub d Sv: het vastleggen van opgeslagen gegevens. Met name nu deze onderzoeksmogelijkheid zich ook uit kan strekken tot gegevens die worden opgeslagen na afgifte van het bevel en [redacted]blijkens de Memorie van Toelichting - ook communicatie kan betreffen.

Of, de vraag anders geformuleerd:

Wanneer kan/moet de bevoegdheid ex sub b – aftappen van communicatie – worden gebruikt en wanneer kan/moet de bevoegdheid ex sub d – het vastleggen van opgeslagen gegevens – worden gebruikt?

---

[1] Kamerstukken II, 1998/99, 26671, p. 28.

Op basis van de wetsgeschiedenis, waarin alleen in de Memorie van Toelichting wordt ingegaan op het onderscheid tussen de twee onderzoeksmogelijkheden, kom ik tot het volgende antwoord.

De tapbevoegdheid (sub b) kan worden gebruikt indien er enkel communicatie moet worden vastgelegd. Onder communicatie moet worden verstaan niet voor het publiek bestemde communicatie die plaatsvindt met gebruikmaking van de diensten van een aanbieder van een communicatiedienst. Hierbij geldt dat het vroegere onderscheid tussen opgeslagen en stromende gegevens niet meer opgaat. Er kan worden afgetapt op het apparaat. Het kan communicatie betreffen die nog niet is verzonden, of juist reeds ontvangen is. Wel moet het gaan om communicatie die op het moment van het afgeven van het bevel nog niet bestaat (toekomstige gegevens).

De bevoegdheid om gegevens vast te leggen (sub d) kan/moet worden gebruikt indien er (naast toekomstige communicatie) ook andere opgeslagen gegevens moeten worden vastgelegd. Hierbij kan worden gedacht aan historische communicatie, maar ook gegevens die niet als communicatie worden gekwalificeerd zoals inloggegevens, wachtwoorden, bestanden, afbeeldingen, persoonlijke notities, etc.

Uiteraard gelden bij beide onderzoeksmogelijkheden de eisen uit het Besluit onderzoek in een geautomatiseerd werk. Dat wil zeggen dat indien een technisch hulpmiddel wordt gebruikt, dit in beginsel gekeurd dient te zijn. Bij een dringend onderzoeksbelang kan een niet gekeurd middel worden gebruikt.

20 september 2019
LP Digit [redacted]

	Toegezonden	Afgerond
LP Digit		6 september 2019
Afgestemd LE Digit	6 september 2019	20 september 2019

Bijlage Relevante passages wetsgeschiedenis

Memorie van Toelichting

Daarnaast wordt de effectiviteit van het aftappen en opnemen van communicatie ernstig verminderd door de encryptie van gegevens. Dit betreft de versleuteling van gegevens in transit. Het aftappen en opnemen van communicatie kan plaatsvinden door middel van een telefoon-, e-mail-, of internettap (artikelen 126m, 126t en 126zg Sv). Ook kan opgeslagen communicatie worden gevorderd van de aanbieder (artikel 126ng Sv). De inzet van deze bevoegdheden biedt echter geen resultaat in gevallen waarin gebruik wordt gemaakt van moderne versleuteling. Het aftappen en opnemen van communicatie, waarbij gebruik wordt gemaakt van de diensten van een openbare aanbieder van communicatie, levert slechts gegevens waaruit de inhoud van de communicatie niet kan worden afgeleid. Weliswaar is de aanbieder gehouden mee te werken aan het ongedaan maken van de versleuteling van de communicatie (artikel 126m, zesde lid, en 126nh, eerste lid, Sv), maar de aanbieder is hiertoe soms vaak niet in staat (bijvoorbeeld Skype), valt niet onder definitie van aanbieder (artikel 126la Sv) of is gevestigd in het buitenland. Ook kan er sprake zijn van meerdere lagen beveiliging, waarbij niet de ontsleuteling van iedere laag in handen is van een aanbieder. Dit is hierboven reeds aan de orde gekomen. Voor wat betreft het Tor-netwerk is wezenlijk dat een uitgebreid netwerk van tussenstations wordt gebruikt om de data over te dragen. Verschillende datapakketten volgen een willekeurige route langs zogeheten relaisstations, waarbij ieder station uitsluitend het IP-adres van het vorige en het eerstvolgende relaisstation in de keten kent. Hierdoor is er geen aanknopingspunt om bijvoorbeeld een IP-tap in te zetten of gegevens bij een aanbieder van een communicatiedienst te vorderen. De opsporing heeft dan ook dringend behoefte aan de mogelijkheid om de communicatie te kunnen onderscheppen *voordat* deze wordt versleuteld of *nadat* deze is ontsleuteld. Dit betekent dat de communicatie wordt afgetapt en opgenomen op het geautomatiseerde werk, voordat de gegevens worden verzonden of nadat deze ontvangen zijn en de communicatie door de software op het geautomatiseerde werk van de ontvanger is ontsleuteld. Daardoor verschuift de oriëntatie van het aftappen van de verbinding, door middel waarvan de communicatie tussen de deelnemers wordt overgedragen, naar het aftappen op de bron of het doel van de communicatie, te weten de computer of de mobiele telefoon met behulp waarvan de communicatie wordt gecommuniceerd («aftappen op het apparaat»).

2.3.2 De vastlegging van gegevens die in het geautomatiseerde werk zijn of worden opgeslagen

Een belangrijke bevoegdheid betreft de vastlegging van gegevens, die in het geautomatiseerde werk zijn opgeslagen of die na het tijdstip van de afgifte van het bevel worden opgeslagen. De vastlegging heeft betrekking op gegevens die van belang zijn voor de waarheidsvinding inzake ernstige strafbare feiten. Gedacht kan worden aan het beramen of plegen van ernstige strafbare feiten waarbij de communicatie versleuteld plaatsvindt, aan strafbare afbeeldingen (kinderpornografie) of e-mailberichten die inzage geven in de communicatie met andere personen over het beramen of plegen van ernstige strafbare feiten.

Het kan gaan om zowel gegevens die reeds in het geautomatiseerde werk zijn opgeslagen als om gegevens die gedurende de looptijd van het bevel worden opgeslagen. De term «opgeslagen» wordt in neutrale zin gebruikt, en brengt tot uitdrukking dat de (vaste) gegevens in het geautomatiseerde werk aanwezig zijn. Niet vereist is een specifieke handeling van de gebruiker, gericht op het bewaren van de gegevens, zoals dat bijvoorbeeld bij programma's voor tekstverwerking aan de orde kan zijn. Het gaat hierbij om vaste gegevens, namelijk gegevens die zijn of worden opgeslagen. Daarbij kan worden gedacht aan het vastleggen van afbeeldingen van kinderpornografie of van inloggegevens van besloten «communities» of wachtwoorden waarmee de versleuteling van gegevens ongedaan kan worden gemaakt. Soms is sprake van een versleutelde harddisk. Deze gegevens kunnen ook betrekking hebben op communicatie. Mondelinge communicatie, voor zover die niet is opgeslagen, kan niet worden vastgelegd. Daarvoor dient de bevoegdheid van het aftappen van telecommunicatie. Dit komt hieronder, onder punt 4, nader aan de orde. 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.

Voorbeelden:

1.De verdachte maakt veelvuldig gebruik van cryptocontainers of complete versleuteling van de harde schijf. Nadat in het geautomatiseerde werk is binnengedrongen kan het wachtwoord worden afgevangen zodat bij latere vastlegging van de gegevens de cryptocontainer kan worden geopend.

2.De verdachte heeft zijn gegevens via het Tor-netwerk in de Cloud opgeslagen. De aanbieder kan niet worden vastgesteld of bereikt. Het veiligstellen van de gegevens is uitsluitend mogelijk als de verbinding met de Clouddienst open is. Daarvoor is het noodzakelijk om de gegevens van het geautomatiseerde werk over te nemen als de verbinding met de Clouddienst in werking is.

De vastlegging van gegevens is beperkt tot de gegevens die redelijkerwijs nodig zijn om de waarheid aan de dag te brengen. Anders dan bij het vaststellen van bepaalde kenmerken van het geautomatiseerde werk of van de gebruiker, genoemd onder punt 1, is de vastlegging van gegevens ruimer. In de eerste plaats is de vastlegging van gegevens niet beperkt tot de vaststelling van bepaalde kenmerken, maar kan het geautomatiseerde werk worden doorzocht en kunnen in het belang van het onderzoek gegevens of gegevensbestanden worden vastgelegd. Deze gegevens kunnen betrekking hebben op het internetgebruik van de gebruiker. Dit is niet beperkt tot de gegevens die zijn opgeslagen, maar kan ook betrekking hebben op gegevens die na het tijdstip van afgifte van het bevel worden opgeslagen.

2.3.4 De uitvoering van een bevel tot het aftappen en opnemen van communicatie of opnemen van vertrouwelijke communicatie

Op basis van de voorgestelde bevoegdheid kan worden overgegaan tot het heimelijk aftappen en opnemen van communicatie (hierna ook te noemen: het aftappen van communicatie) of het opnemen van vertrouwelijke communicatie (hierna ook te noemen: het direct afluisteren). Deze bevoegdheden zijn afzonderlijk geregeld in de Titels IVa en V van het Wetboek van Strafvordering («Bijzondere bevoegdheden tot opsporing» en «Bijzondere bevoegdheden tot opsporing voor het onderzoek naar het beramen of plegen van ernstige misdrijven in georganiseerd verband»). De inzet van deze bevoegdheden vereist een afzonderlijk bevel, op grond van de artikelen 126l, 126m, 126s, 126t of 126zg Sv. Het onderzoek in een geautomatiseerd werk is in dat geval beperkt tot het gebruik van het geautomatiseerde werk ten behoeve van het inzetten van de bevoegdheid van het aftappen van communicatie. Het onderzoek is niet gericht op de gegevens, anders dan die met betrekking tot de af te tappen communicatie, die in het geautomatiseerde werk worden opgeslagen.

Hierboven is, onder punt 2, de vastlegging van gegevens aan de orde gekomen. Dit kan ook gegevens met betrekking tot communicatie omvatten. Communicatie betreft de uitwisseling van informatie, in de vorm van een gesprek of een bericht dat door middel van e-mail, SMS of een social site is uitgewisseld. Als de communicatie op een geautomatiseerd werk is opgeslagen, dan kunnen de gegevens met betrekking tot die communicatie worden vastgelegd, dat wil zeggen overgenomen of gekopieerd. Als de communicatie, al dan niet met behulp van een communicatiedienst, tussen twee personen wordt uitgewisseld, dan kan gebruik worden gemaakt van de bestaande opsporingsbevoegdheden voor het aftappen en opnemen van die communicatie.

In de eerste plaats kunnen stromende gegevens met betrekking tot communicatie worden afgetapt en opgenomen op grond van het eerdergenoemde bevel tot het aftappen en opnemen van communicatie. Deze bevoegdheid kan uitsluitend worden ingezet in geval van verdenking van een ernstig misdrijf, waarvoor voorlopige hechtenis is toegelaten, en dat een ernstige inbreuk op de rechtsorde oplevert. In een dergelijk geval kan de officier van justitie, indien het onderzoek dit dringend vordert, aan een opsporingsambtenaar bevelen dat met een technisch hulpmiddel niet voor het publiek bestemde communicatie die plaatsvindt met gebruikmaking van de diensten van een aanbieder van een communicatiedienst, wordt opgenomen. Hiervoor is een schriftelijke machtiging van de rechter-commissaris vereist (artikelen 126m en 126t, vijfde lid, en 126zg, derde lid, Sv).

Het aftappen van communicatie kan zonder de medewerking van de aanbieder plaatsvinden indien dit niet mogelijk is of het belang van strafvordering zich daartegen verzet. Deze mogelijkheid is opgenomen naar aanleiding van het Cybercrime Verdrag. Dit verdrag gaat ervan uit dat de opsporingsdiensten beschikken over eigen bevoegdheden en dat daarnaast een medewerkingsplicht komt te rusten op de serviceproviders. Teneinde te voldoen aan de eisen van het verdrag is, met de Wet

computercriminaliteit II, artikel 126m Sv gewijzigd zodat het opnemen van telecommunicatie ook zonder medewerking van de aanbieder kan plaatsvinden (artikelen 126m en 126t, derde en vierde lid, en 126zg, vierde lid, Sv). Vereist is dat een technisch hulpmiddel wordt gebruikt, dat voldoet aan bij algemene maatregel van bestuur te stellen eisen (artikel 126ee, onderdeel a, Sv). Deze eisen zijn vastgelegd in het Besluit technische hulpmiddelen strafvordering. In de artikelen 126m en 126t, tweede lid, Sv zijn destijds een nieuw onderdeel e. respectievelijk f. toegevoegd, die bepalen dat in het bevel de aard van het technische hulpmiddel moet worden aangeduid waarmee de communicatie zal worden opgenomen.

De regeling van het aftappen van communicatie in het Wetboek van Strafvordering is gebaseerd op het uitgangspunt dat een bevel tot het opnemen van telecommunicatie, die plaatsvindt via een openbaar telecommunicatienetwerk of met gebruikmaking van een openbare telecommunicatiedienst, ten uitvoer wordt gelegd met medewerking van de aanbieder van het desbetreffende netwerk of de dienst. In het geval van de versleuteling van communicatie kan het belang van strafvordering zich echter verzetten tegen het opnemen van communicatie met de medewerking van de aanbieder, omdat de opgenomen communicatie dan dikwijls niet uit te lezen is. In een dergelijk geval kan de officier van justitie een bevel tot het aftappen van communicatie afgeven zonder dat daarbij een aanbieder is betrokken. De in dit artikel opgenomen vereisten voor het opnemen van communicatie zijn onverkort van toepassing wanneer in het kader van een onderzoek in een geautomatiseerd werk wordt overgegaan tot het opnemen van communicatie. Er is een afzonderlijk bevel van de officier van justitie vereist. Hiervoor is een afzonderlijke schriftelijke machtiging van de rechter-commissaris vereist (artikelen 126m, 126s en 126zg, vijfde lid, Sv). Het Besluit technische hulpmiddelen strafvordering zal worden aangepast aan het opnemen van telecommunicatie in het kader van een onderzoek in een geautomatiseerd werk. Uitsluitend de opsporingsambtenaren die door de korpschef zijn aangewezen en die ter zake deskundig zijn, zullen met de uitvoering van een dergelijk bevel kunnen worden belast. Ook zullen regels worden gesteld over het technische hulpmiddel dat hierbij kan worden gebruikt.

Het uitgangspunt van het aftappen via de aanbieder zal nauwelijks worden aangetast met de mogelijkheid van het opnemen van communicatie, waarbij op afstand heimelijk in het geautomatiseerde werk is binnengedrongen. Er zijn verschillende omstandigheden die in de weg staan aan een grootschalige toepassing van het «aftappen op het apparaat». Het is niet eenvoudig om heimelijk binnen te dringen in een geautomatiseerd werk vanwege, onder meer, de beveiliging daarvan. Deze wijze van aftappen vereist dan ook een uitgebreide voorbereiding, inclusief de voorafgaande toetsing van de voorgenomen inzet door de Centrale Toetsingscommissie van het OM. Daarnaast is de uitvoering van de bevoegdheid beperkt tot de daartoe aangewezen en ter zake deskundige opsporingsambtenaren.

In de tweede plaats kunnen stromende gegevens met betrekking tot communicatie heimelijk worden opgenomen op grond van het eerdergenoemde bevel tot het opnemen van vertrouwelijke communicatie (het direct afluisteren). Een voorbeeld betreft een gesprek dat op een openbare plaats of in een woning tussen personen

plaatsvindt. Het is ook mogelijk dat er wel sprake is van communicatie maar niet van een communicatiedienst in de zin van de Telecommunicatiewet, zoals bij communicatie via het internet (Skype). Deze bevoegdheid kan eveneens uitsluitend worden ingezet in geval van verdenking van een ernstig misdrijf, waarvoor voorlopige hechtenis is toegelaten, en dat een ernstige inbreuk op de rechtsorde oplevert. In een dergelijk geval kan de officier van justitie, indien het onderzoek dit dringend vordert, bevelen dat een ambtenaar van politie of van de Koninklijke marechaussee vertrouwelijke communicatie opneemt met een technisch hulpmiddel (artikelen 126l, 126s en 126zf, eerste lid, Sv). Hiervoor is eveneens een afzonderlijk bevel van de officier van justitie en een afzonderlijke schriftelijke machtiging van de rechter-commissaris vereist (artikelen 126l en 126s, vierde lid, en 126zf, eerste lid, Sv). Het technische hulpmiddel dat gebruikt wordt kan een keylogger zijn, die op het geautomatiseerde werk wordt aangebracht en die aanslagen op een toetsenbord vastlegt, of een richtmicrofoon, met behulp waarvan op grote afstand vertrouwelijke communicatie kan worden afgeluisterd en opgenomen. Ook kan worden gedacht aan het op afstand aanzetten van een microfoon van een computer, zodat bijvoorbeeld VOIP-gesprekken kunnen worden afgeluisterd die worden gevoerd met de betreffende computer.

De inzet van de bevoegdheden van het aftappen van communicatie en het direct afluisteren in het kader van onderzoek in een geautomatiseerd werk, biedt de mogelijkheid om communicatie op te nemen op een locatie die voor de opsporing niet goed bereikbaar is. Het is dan niet nodig een besloten plaats of een woning binnen te dringen, met alle risico's van dien. Dit kan eveneens uitkomst bieden in de gevallen waarin de locatie van de communicatie niet bekend is.

Uit het bovenstaande vloeit voort dat de bevoegdheden van het aftappen van communicatie en het direct afluisteren overlap vertonen met de handeling van het vastleggen van gegevens. Dit is aan de orde bij gegevens met betrekking tot communicatie, die in het geautomatiseerde werk zijn opgeslagen. Het traditionele aftappen heeft betrekking op spraak. Inmiddels wordt ook gebruik gemaakt van de internettap met behulp waarvan gegevens met betrekking tot communicatie, die door middel van het internet worden uitgewisseld, afgetapt kunnen worden. Zodra dergelijke gegevens in een geautomatiseerd werk worden opgeslagen, kunnen deze ook worden vastgelegd. Aldus kan communicatie worden afgetapt dan wel vastgelegd, afhankelijk van het stadium van uitwisseling.

Tijdens de consultatie heeft KPN opgemerkt dat er bij de voorgestelde bevoegdheid in het geheel geen rekening wordt gehouden met verdragsrechtelijke verplichtingen die voor vergelijkbare verplichtingen elders in het Wetboek van Strafvordering zijn opgenomen, zoals het vragen van instemming aan een ander land als de gebruiker zich in het buitenland bevindt (artikel 126ma/ta Sv). Deze verplichtingen gelden echter onverkort voor het aftappen van communicatie in het kader van een onderzoek in een geautomatiseerd werk. De inzet van deze bevoegdheden vereist immers een afzonderlijk bevel, op grond van de artikelen 126l, 126m, 126s, 126t of 126zg Sv. Dit betekent dat indien bij de afgifte van een bevel tot het aftappen van communicatie bekend is dat de gebruiker van het nummer zich op het grondgebied van een andere

staat bevindt, de instemming van die andere staat moet zijn verkregen voordat het bevel ten uitvoer wordt gelegd.

Voor de toelichting op de doelen van het onderzoek in een geautomatiseerd werk kan worden verwezen naar het algemeen deel van deze toelichting. Aanvullend kan nog worden opgemerkt dat, anders dan voor de huidige doorzoeking ter vastlegging van gegevens, de vastlegging van gegevens ook betrekking kan hebben op gegevens die na het tijdstip van afgifte van het bevel worden opgeslagen. De beperking tot de gegevens die op de plaats van de doorzoeking aanwezig zijn volgde uit het feit dat de bevoegdheid tot de doorzoeking ter vastlegging van gegevens is afgeleid van de bevoegdheid tot inbeslagneming van daarvoor vatbare voorwerpen (zoals een computer). De inbeslagnemingsbevoegdheid mag uit de aard der zaak slechts worden uitgeoefend indien redelijkerwijs kan worden vermoed dat op de te doorzoeken plaats daarvoor vatbare voorwerpen aanwezig zijn. Indien de doorzoekingsbevoegdheid wordt gebruikt om gedurende enige tijd (tijdens de doorzoeking) binnenkomende en uitgaande gegevens te onderscheppen, dan zou feitelijk sprake zijn van het opnemen of aftappen van telecommunicatie (Kamerstukken II 1998/99, 26 671, nr. 3, blz. 49). Op dit punt wordt met dit wetsvoorstel een andere afweging gemaakt. 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. Hiervoor kan ook worden verwezen naar het algemeen deel van deze toelichting. Met het gebruik van de term «vastlegging» van gegevens wordt gedoeld op het overnemen (of: kopiëren) van gegevens die zijn opgeslagen, zonder dat deze uit de beschikkingsmacht van de bezitter raken. Hiermee wordt ook het onderscheid met het aftappen van communicatie tot uitdrukking gebracht.

Document 26

Notitie 126m – tappen buiten de provider om

Landelijk Parket - DIGIT

Het verrichten van onderzoekshandelingen ex artikel 126nba Sv kan bestaan uit het geven van een bevel ex artikel 126m Sv (het tappen van een telefoon). In artikel 126m lid 3 Sv is bepaald dat het bevel om te tappen in beginsel wordt uitgevoerd met medewerking van de aanbieder van het openbare telecommunicatienetwerk / de openbare telecommunicatiedienst.

Bij een bevel ex artikel 126m Sv dat wordt gegeven nadat in een geautomatiseerd werk is binnengedrongen, zal dit echter veelal niet mogelijk zijn.

Uit de parlementaire geschiedenis van de Wet Computercriminaliteit III blijkt het volgende:

1. De bevoegdheid om na binnendringen in ene geautomatiseerd werk te kunnen tappen, is er gekomen in verband met een toenamen van encryptie. Daarom is er noodzaak ontstaan voor "aftappen op het apparaat".
2. Voor dat aftappen (en ook OVC) moet een afzonderlijke machtiging en een [redacted] worden gegeven. Dat kan wel in een gecombineerd formulier waarin de vereisten voor zowel 126nba, als 126m staan.
3. Het aftappen op deze manier is aftappen [redacted].
4. De vereisten die daarvoor gelden, staan in het [redacted] (en niet het Besluit technische hulpmiddelen Strafvordering).

16 april 2020

LP Digit - [redacted]

Tweede Kamer, vergaderjaar 2015–2016, 34 372, nr. 3
MEMORIE VAN TOELICHTING

p. 9
Daarnaast wordt de effectiviteit van het aftappen en opnemen van communicatie ernstig verminderd door de encryptie van gegevens. Dit betreft de versleuteling van gegevens in transit. Het aftappen en opnemen van communicatie kan plaatsvinden door middel van een telefoon-, e-mail-, of internettap (artikelen 126m, 126t en 126zg Sv). Ook kan opgeslagen communicatie worden gevorderd van de aanbieder (artikel 126ng Sv). De inzet van deze bevoegdheden biedt echter geen resultaat in gevallen waarin gebruik wordt gemaakt van moderne versleuteling. Het aftappen en opnemen van communicatie, waarbij gebruik wordt gemaakt van de diensten van een openbare aanbieder van communicatie, levert slechts gegevens waaruit de inhoud van de communicatie niet kan worden afgeleid. Weliswaar is de aanbieder gehouden mee te werken aan het ongedaan maken van de versleuteling van de communicatie (artikel 126m, zesde lid, en 126nh, eerste lid, Sv), maar de aanbieder is hiertoe soms vaak niet in staat (bijvoorbeeld Skype), valt niet onder definitie van aanbieder (artikel 126la Sv) of is gevestigd in het buitenland. Ook kan er sprake zijn van meerdere lagen beveiliging, waarbij niet de ontsleuteling van iedere laag in handen is van een aanbieder. Dit is hierboven reeds aan de orde gekomen. Voor wat betreft het Tor-netwerk is wezenlijk dat een uitgebreid netwerk van tussenstations wordt gebruikt om de data over te dragen. Verschillende datapakketten volgen een willekeurige route langs zogeheten relaisstations, waarbij ieder station uitsluitend het IP-adres van het vorige en het eerstvolgende relaisstation in de keten kent. Hierdoor is er geen aanknopingspunt om bijvoorbeeld een IP-tap in te zetten of gegevens bij een aanbieder van een communicatiedienst te vorderen. De opsporing heeft dan ook dringend behoefte aan de mogelijkheid om de communicatie te kunnen onderscheppen *voordat* deze wordt versleuteld of *nadat* deze is ontsleuteld. Dit betekent dat de communicatie wordt afgetapt en opgenomen op het geautomatiseerde werk, voordat de gegevens worden verzonden of nadat deze ontvangen zijn en de communicatie door de software op het geautomatiseerde werk van de ontvanger is ontsleuteld. Daardoor verschuift de oriëntatie van het aftappen van de verbinding, door middel waarvan de communicatie tussen de deelnemers wordt overgedragen, naar het aftappen op de bron of het doel van de communicatie, te weten de computer of de mobiele telefoon met behulp waarvan de communicatie wordt gecommuniceerd («aftappen op het apparaat»).

p. 23
2.3.4 De uitvoering van een bevel tot het aftappen en opnemen van communicatie of opnemen van vertrouwelijke communicatie
Op basis van de voorgestelde bevoegdheid kan worden overgegaan tot het heimelijk aftappen en opnemen van communicatie (hierna ook te noemen: het aftappen van communicatie) of het opnemen van vertrouwelijke communicatie (hierna ook te noemen: het direct afluisteren). Deze bevoegdheden zijn afzonderlijk geregeld in de Titels IVa en V van het Wetboek van Strafvordering («Bijzondere bevoegdheden tot opsporing»

en «Bijzondere bevoegdheden tot opsporing voor het onderzoek naar het beramen of plegen van ernstige misdrijven in georganiseerd verband»). [redacted] Het onderzoek in een geautomatiseerd werk is in dat geval beperkt tot het gebruik van het geautomatiseerde werk ten behoeve van het inzetten van de bevoegdheid van het aftappen van communicatie. Het onderzoek is niet gericht op de gegevens, anders dan die met betrekking tot de af te tappen communicatie, die in het geautomatiseerde werk worden opgeslagen.
(...)
[redacted] Deze mogelijkheid is opgenomen naar aanleiding van het Cybercrime Verdrag. Dit verdrag gaat ervan uit dat de opsporingsdiensten beschikken over eigen bevoegdheden en dat daarnaast een medewerkingsplicht komt te rusten op de serviceproviders. Teneinde te voldoen aan de eisen van het verdrag is, met de Wet computercriminaliteit II, artikel 126m Sv gewijzigd zodat het opnemen van telecommunicatie ook zonder medewerking van de aanbieder kan plaatsvinden (artikelen 126m en 126t, derde en vierde lid, en 126zg, vierde lid, Sv). [redacted] In de artikelen 126m en 126t, tweede lid, Sv zijn destijds een nieuw onderdeel e. respectievelijk f. toegevoegd, die bepalen dat in het bevel de aard van het technische hulpmiddel moet worden aangeduid waarmee de communicatie zal worden opgenomen.

De regeling van het aftappen van communicatie in het Wetboek van Strafvordering is gebaseerd op het uitgangspunt dat een bevel tot het opnemen van telecommunicatie, die plaatsvindt via een openbaar telecommunicatienetwerk of met gebruikmaking van een openbare telecommunicatiedienst, ten uitvoer wordt gelegd met medewerking van de aanbieder van het desbetreffende netwerk of de dienst. [redacted] Het Besluit technische hulpmiddelen strafvordering zal worden aangepast aan het opnemen van telecommunicatie in het kader van een onderzoek in een geautomatiseerd werk. Uitsluitend de opsporingsambtenaren die door de korpschef zijn aangewezen en die ter zake deskundig zijn, zullen met de uitvoering van

een dergelijk bevel kunnen worden belast. Ook zullen regels worden gesteld over het technische hulpmiddel dat hierbij kan worden gebruikt.

p. 24

Het uitgangspunt van het aftappen via de aanbieder zal nauwelijks worden aangetast met de mogelijkheid van het opnemen van communicatie, waarbij op afstand heimelijk in het geautomatiseerde werk is binnengedrongen. Er zijn verschillende omstandigheden die in de weg staan aan een grootschalige toepassing van het «aftappen op het apparaat». Het is niet eenvoudig om heimelijk binnen te dringen in een geautomatiseerd werk vanwege, onder meer, de beveiliging daarvan. Deze wijze van aftappen vereist dan ook een uitgebreide voorbereiding, inclusief de voorafgaande toetsing van de voorgenomen inzet door de Centrale Toetsingscommissie van het OM. Daarnaast is de uitvoering van de bevoegdheid beperkt tot de daartoe aangewezen en ter zake deskundige opsporingsambtenaren.

p. 55

In het kader van een onderzoek van een geautomatiseerd werk kan ook worden overgegaan tot het aftappen van communicatie of het opnemen van vertrouwelijke communicatie. Bij de toepassing van deze opsporingsbevoegdheden is evenmin sprake van communicatie die aan een derde is toevertrouwd. Het aftappen van communicatie vindt plaats zonder medewerking van de aanbieder van het openbare telecommunicatienetwerk of de openbare telecommunicatiedienst. Ook voor de toepassing van deze opsporingsbevoegdheden geldt dat materieel wordt voldaan aan de eisen van artikel 13 van de Grondwet. Er is voorzien in een wettelijke grondslag voor het aftappen van communicatie of het opnemen van vertrouwelijke communicatie in de vorm van stromende gegevens, dit betreft de eerdergenoemde artikelen 126l, 126m, 126s, 126t, 126zf en 126zg Sv. De inzet van deze bevoegdheden is eveneens gebonden aan een voorafgaande rechterlijke toetsing.

p. 103

Voor de toepassing van de bevoegdheden van het aftappen van communicatie, het opnemen van vertrouwelijke communicatie en de stelselmatige observatie is een afzonderlijk bevel vereist, op grond van de artikelen 126l, 126m en 126gSv. In het voorgestelde artikel 126nba Sv wordt telkens verwezen naar de bestaande bepalingen over de inzet van deze bijzondere opsporingsbevoegdheden. Hieruit volgt dat de wettelijke voorwaarden waaronder deze bevoegdheden kunnen worden ingezet onverminderd gelden. Bij het bevel voor onderzoek in een geautomatiseerd werk betreffende op deze bijzondere opsporingsbevoegdheden kunnen ook de gegevens worden opgenomen die in een afzonderlijk bevel tot de toepassing van een dergelijke bevoegdheid moeten worden opgenomen. Bij het bevel tot het opnemen van vertrouwelijke communicatie, bedoeld in de artikel 126l of het bevel tot het aftappen van communicatie, bedoeld in de artikelen 126m, betreft dit de gegevens, bedoeld in de artikelen 126l, en 126m Sv. Bij het bevel tot stelselmatige observatie, bedoeld in de artikelen 126gSv, betreft dit de gegevens, bedoeld in artikel 126g, vijfde lid Sv. Daardoor kan een bevel worden gecombineerd

[redacted] Hiervoor kunnen modelformulieren worden ontwikkeld.

In zijn advies merkt het College op dat de verwachting is dat een praktijk zal ontstaan waarbij gelijktijdig met het bevel tot het binnentreden van een geautomatiseerd werk een bevel tot het uitoefenen van de overige opsporingsbevoegdheden zal worden gedaan. Op deze wijze kan worden voorkomen dat de rechter-commissaris meerdere keren om een machtiging moet worden gevraagd en dat de CTC meerdere kleren moet worden gevraagd toestemming te geven. Het College adviseert om dit duidelijker in de wettelijke regeling tot uitdrukking te brengen. Aan dit advies is geen gevolg gegeven omdat uit de tekst van het voorgestelde artikel 126nba, eerste lid, Sv in combinatie met de toelichting reeds ondubbelzinnig blijkt dat de verschillende bevelen gelijktijdig gegeven kunnen worden.

Tweede Kamer, vergaderjaar 2016–2017, 34 372, nr. 6
NOTA NAAR AANLEIDING VAN HET VERSLAG
Ontvangen 8 november 2016

p. 46
Omwille van de overzichtelijkheid worden voornoemde onderwerpen uitgewerkt in een afzonderlijk besluit en niet, zoals verder in de memorie van toelichting vermeld, via een wijziging van het Besluit technische hulpmiddelen strafvordering.

Eerste Kamer, vergaderjaar 2016–2017, 34 372, D
MEMORIE VAN ANTWOORD
Ontvangen 12 juni 2017

p. 29
De bevoegdheid tot het aftappen en opnemen van communicatie (artikelen 126m/t en 126zg Sv) kan worden gebruikt om door middel van een internettap in kaart te brengen welk verkeer met het internet via een router van een thuisnetwerk of een zogenaamde openbare «hotspot» is waar te nemen. De wettelijke voorwaarden voor de toepassing van deze bevoegdheid zijn deels – voor wat betreft bijvoorbeeld de toepassing van de onderzoekshandelingen van het aftappen en opnemen van communicatie of het opnemen van vertrouwelijke communicatie – gelijk aan die voor de voorgestelde bevoegdheid van het op afstand binnendringen van een geautomatiseerd werk. Het doel van het binnendringen met het oog op het verrichten van die onderzoekshandelingen wijkt in dergelijke gevallen – het aftappen en opnemen van communicatie of het opnemen van vertrouwelijke communicatie – niet af van de bestaande bevoegdheid van het aftappen en opnemen van communicatie of het gebruik van een richtmicrofoon. De bevoegdheid van het op afstand heimelijk binnendringen van een smartphone met het oog op het aftappen en opnemen

van communicatie kan onvermijdelijk zijn om de versleuteling van de communicatie te omzeilen. Om die reden ligt een beperking van de bevoegdheid tot delicten die op een lijst zijn geplaatst, zoals door de leden van de fractie van D66 gesuggereerd, minder voor de hand. Voor de opsporing zou dat een stap terug betekenen in vergelijking met de bestaande bevoegdheden rond het aftappen en opnemen van (vertrouwelijke) communicatie.

Document 27

De omvang van de toetsing en rol van de rechter-commissaris bij art. 126nba Sv

Landelijk Parket - DIGIT

Omvang bevel 126nba Sv

In artikel 126nba Sv is bepaald dat de officier van justitie kan bevelen dat een opsporingsambtenaar binnendringt in een geautomatiseerd werk. Daartoe is wel een machtiging van de rechter-commissaris vereist. Deze machtiging vermeldt de onderdelen van het bevel.

De onderdelen van dit bevel zijn:

> 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 bekend, dat de gegevens niet in Nederland zijn opgeslagen;
> c. de feiten of omstandigheden waaruit blijkt dat de voorwaarden, bedoeld in het eerste lid, zijn vervuld;
> d. een aanduiding van de aard en functionaliteit van het technische hulpmiddel, bedoeld in het eerste lid, dat wordt gebruikt voor de uitvoering van het bevel;
> e. het onderdeel of de onderdelen, genoemd in het eerste lid, met het oog waarop het bevel wordt gegeven en, als dit het onderdeel a, d of e betreft, een duidelijke omschrijving van de te verrichten handelingen;
> f. ten aanzien van welk deel van het geautomatiseerde werk en welke categorie van gegevens aan het bevel uitvoering wordt gegeven;
> g. het tijdstip waarop, of de periode waarbinnen aan het bevel uitvoering wordt gegeven;
> h. in het geval het een bevel, bedoeld in het eerste lid, onderdeel c, betreft, een melding van het voornemen om een technisch hulpmiddel op een persoon te bevestigen.

Omvang machtiging 126nba Sv

In de systematiek van de huidige BOB-wetgeving heeft de officier van justitie een centrale rol in het opsporingsonderzoek. Voor de inzet van vergaande bijzondere opsporingsbevoegdheden machtigt de rechter-commissaris de officier van justitie om bepaalde bevelen te mogen geven. De omvang van hetgeen de officier van justitie mag bevelen, wordt ingekaderd door de wet en eventueel door de machtiging van de rc.[1]

Een vordering aan de rechter-commissaris om een bevel te mogen geven zal de nodige informatie moeten bevatten voor diens toetsing.[2]

In totstandkoming van art. 126nba Sv heeft de wetgever het volgende opgemerkt over de machtiging die de rechter-commissaris verleend:[3]

---

[1] Zie o.a. A. Beijer, R.J. Bokhorst, M. Boone, C.H. Brants en J.M.W. Lindeman, *De Wet bijzondere opsporingsbevoegdheden – eindevaluatie* (Onderzoek en beleid, deel 222), Den Haag: Boom Juridische uitgevers 2004, www.wodc.nl.

[2] Vgl. Kamerstukken II, 2015/16, 34 372, nr. 3, p. 101 (MvT)

> "De officier van justitie dient bij de rechter-commissaris een machtiging te vorderen voor het voorgenomen onderzoek in het geautomatiseerde werk. Van belang is dat het geautomatiseerde werk in voldoende mate identificeerbaar is, zodat de reikwijdte van de bevoegdheid voldoende kan worden afgegrensd. Behoudens de situatie waarin het onderzoek in een geautomatiseerd werk is gericht op het bepalen van de identiteit van het werk dat bij de verdachte in gebruik is, zal de rechter-commissaris behoefte hebben aan informatie ten behoeve van de identificering van het geautomatiseerde werk. Dit is ook van belang voor de beoordeling van de proportionaliteit van de bevoegdheid. Als bekend is dat de gegevens niet in Nederland zijn opgeslagen of vastgelegd of als de locatie niet redelijkerwijs kan worden vastgesteld dan dient dit in het bevel te worden vermeld. Daarbij geldt dat de rechter-commissaris er bij de afgifte van de machtiging vanuit mag gaan dat de officier van justitie zich houdt aan de regels op het gebied van de internationale samenwerking. Het onderzoek is uitsluitend toegestaan met het oog op het verrichten van bepaalde onderzoekshandelingen met betrekking tot het geautomatiseerde werk. In de vordering tot machtiging tot het geven van het bevel wordt vermeld voor welk doel de bevoegdheid in een concreet opsporingsonderzoek wordt ingezet. Daarnaast moeten, indien gebruik wordt gemaakt van een technisch hulpmiddel, de aard en functionaliteit van het technische hulpmiddel worden vermeld evenals ten aanzien van welk deel van het geautomatiseerde werk en welke categorie van gegevens aan het bevel uitvoering wordt gegeven. Ten slotte wordt het tijdstip vermeld waarop, of de periode waarbinnen aan het bevel uitvoering wordt gegeven. Op deze wijze wordt de rechter-commissaris in staat gesteld om de reikwijdte van het voorgenomen onderzoek in het geautomatiseerde werk te toetsen op proportionaliteit en subsidiariteit. Andere functionaliteiten dan die waarvoor de rechter-commissaris in de machtiging toestemming heeft gegeven, worden niet ingeschakeld en geïnstalleerd in het geautomatiseerde werk waarin het onderzoek plaatsvindt. Niet uitgesloten is dat meerdere onderzoekshandelingen worden verricht. Voor zover het gaat om de toepassing van de bevoegdheid van het aftappen van communicatie of het direct afluisteren is de toetsing door de rechter-commissaris reeds voorzien in de wettelijke regeling rond die bevoegdheden. Voor de bevoegdheid van de stelselmatige observatie met een technisch hulpmiddel geldt thans niet het vereiste van een voorafgaande machtiging van de rechter-commissaris. Met dit wetsvoorstel wordt in een dergelijke machtiging voorzien, als de desbetreffende bevoegdheid wordt toegepast in het kader van onderzoek in een geautomatiseerd werk en het voor de toepassing van de bevoegdheid nodig is dat op afstand heimelijk wordt binnengedrongen in het geautomatiseerde werk."

Twee aspecten bij de toetsing door de rechter-commissaris bespreek ik nader.

1. Binnendringen en toetsing door de rechter-commissaris.
2. De locatie van gegevens.

Binnendringen

In art. 126nba Sv is onderscheid te maken tussen het binnendringen en het verrichten van onderzoekshandelingen.[4] Het binnendringen is in het artikel niet nader uitgewerkt. De onderzoekhandelingen staan beschreven in het eerste lid onder sub a tot en met e.

In de Nota naar aanleiding van het verslag schrijft de wetgever:

> "In de eerste plaats is het niet de politie maar de officier van justitie die de beslissing kan nemen dat het wenselijk is dat op afstand wordt binnengedrongen in een geautomatiseerd werk. De officier kan hierover niet zelfstandig

[3] Kamerstukken II, 2015/16, 34 372, nr. 3, p. 38 (MvT)
[4] Zie bijvoorbeeld: Kamerstukken II, 2015/16, 34 372, nr. 6, p. 63 (NV II)

beslissen maar heeft een machtiging nodig van de rechter-commissaris. Er is dus een voorafgaande rechterlijke toetsing voorzien."[5]

"Voor het binnendringen van een geautomatiseerd werk zijn een bevel nodig van de officier van justitie en een machtiging van de rechter-commissaris. Ditzelfde geldt voor ieder van de afzonderlijke onderzoekshandelingen. (...) De leden van de PvdA-fractie hebben gevraagd of een computer of afstand kan worden binnengedrongen zonder een machtiging van de rechter-commissaris voor het op afstand heimelijk onderzoeken van een geautomatiseerd werk. Voor het op afstand heimelijk binnendringen van een geautomatiseerd werk is, op grond van het voorgestelde artikel 126nba Sv, altijd een machtiging van de rechter-commissaris vereist."[6]

"De leden van de D66-fractie hebben opgemerkt dat vier fasen worden beschreven die plaatsvinden bij toepassing van de bevoegdheden en hebben gevraagd of voor iedere afzonderlijke fase een bevel door de officier van justitie en een machtiging door de rechter commissaris wordt afgegeven.

In paragraaf 2.5 van de memorie van toelichting worden drie fasen beschreven rond de inzet van de voorgestelde bevoegdheid, te weten de verkennende fase (fase I), het onderzoek in een geautomatiseerd werk (fase II) en de afsluiting van een onderzoek in een geautomatiseerd werk (fase III). Zoals hierboven, naar aanleiding van vragen van de leden van de PvdA-fractie over het verschil tussen het binnendringen in een geautomatiseerd systeem en het onderzoeken van een dergelijk systeem aan de orde is gekomen (paragraaf 2.5), wordt met de term onderzoek in een geautomatiseerd werk gedoeld op het op afstand heimelijk binnendringen in een geautomatiseerd werk en het verrichten van bepaalde onderzoeks- handelingen. Het binnendringen omvat veelal het plaatsen en verwijderen van een technisch hulpmiddel met behulp waarvan gegevens kunnen worden vastgelegd. Het verrichten van onderzoekshandelingen heeft betrekking op de verschillende bevoegdheden die zijn aangeduid in het voorgestelde artikel nba/uba/zpa, eerste lid, onderdelen a. tot en met e. Voor het binnendringen van een geautomatiseerd werk is een bevel nodig van de officier van justitie en een machtiging van de rechter-commissaris. Ditzelfde geldt voor ieder van de afzonderlijke onderzoekshandelingen. In alle gevallen betreft dit fase II rond de inzet van de voorgestelde bevoegdheid."[7]

Gelet op deze opmerkingen van de wetgever moet geconcludeerd worden dat de machtiging van de rechter-commissaris het binnendringen en de te verrichten onderzoekshandelingen omvat.

Gelet op de formulering van artikel 126nba lid 2 Sv zal de rechter-commissaris actief geïnformeerd moeten worden over de te verrichten onderzoekshandelingen en de wijze waarop die worden uitgevoerd.

De methode van binnendringen maakt echter geen deel uit van het bevel en de machtiging tot het verlenen van dat bevel. In Memorie van Toelichting merkt de wetgever namelijk op:

"Niet is vereist dat in het bevel de methode(n) wordt vermeld, op grond waarvan in een geautomatiseerd werk wordt binnengedrongen. Dit zou de opsporingsdiensten nodeloos beperken in de wijze waarop uitvoering wordt gegeven aan het bevel tot het onderzoek in een geautomatiseerd werk en overigens kunnen leiden tot extra werklast voor de rechterlijke macht vanwege de mogelijke noodzaak tot aanpassing van het bevel en de daarmee samenhangende machtiging als tijdens de uitvoering van de bevoegdheid blijkt dat aanpassing van de methode voor het binnen- dringen noodzakelijk is. In de praktijk zal het veelvuldig voorkomen dat de methode aanpassing behoeft om de beveiliging van het geautomatiseerde werk te omzeilen, op dit punt dient de nodige flexibiliteit te

[5] Kamerstukken II, 2015/16, 34 372, nr. 6, p. 30 (NV II)
[6] Kamerstukken II, 2015/16, 34 372, nr. 6, p. 63 (NV II)
[7] Kamerstukken II, 2015/16, 34 372, nr. 6, p. 70 (NV II)

worden geboden. Daar komt bij de dat methode(n) voor het binnendringen in een geautomatiseerd werk niet aan de openbaarheid prijs gegeven kunnen worden, omdat deze dan niet meer kunnen worden gebruikt.[8]

De machtiging van de rechter-commissaris ziet zodoende op het geven van een bevel om binnen te dringen, maar niet op de methode van binnendringen die daarbij zal worden gebruikt.

Een actief informeren van de rechter-commissaris over de methode van binnendringen in een geautomatiseerd werk lijkt daardoor niet aangewezen. Wel kan de landelijk DIGIT officier van justitie de rechter-commissaris desgevraagd (mondeling) informeren. Daarbij zal extra aandacht uit moeten gaan naar het zwaarwegende opsporingsbelang om de methodiek van het binnendringen niet aan de openbaarheid prijs te geven.[9]

Uitzondering hierop lijkt de mate waarin schade aan het geautomatiseerd werk of derden kan optreden. Daarover schrijft de wetgever:

"De Afdeling advisering heeft opgemerkt dat de voorgestelde bevoegdheid tot binnendringen niet zonder risico is. Het door een verdachte gebruikte geautomatiseerd werk zou een vitale functie kunnen vervullen binnen bijvoorbeeld een ziekenhuis, bank of cruciaal beveiligingssysteem. Zou deze functie bekend zijn dan zou dit waarschijnlijk tot de conclusie leiden dat de risico's van binnendringen in het desbetreffende werk onaanvaardbaar groot zijn, binnendringen dus achterwege moet blijven. In reactie hierop moet worden opgemerkt dat de risico's voor het functioneren van het geautomatiseerde werk bij de voorbereiding niet altijd volledig zijn in te schatten. Wel komen de risico's soms vollediger in beeld in beeld nadat is binnengedrongen, waarbij uiteraard zoveel mogelijk wordt vermeden dat het functioneren van het betreffende werk wordt belemmerd. De technische risico's die zijn verbonden aan het onderzoek in een geautomatiseerd werk kunnen ook aan de orde komen in het kader van de toetsing van de noodzaak en de proportionaliteit van het onderzoek. Bedacht moet echter worden dat de officier van justitie en de rechter commissaris niet bij uitstek deskundig zijn om de technische risico's te beoordelen. Voor de inschatting, beheersing en beperking van deze risico's is de deskundigheid van de opsporingsambtenaren die worden belast met het binnendringen van essentieel belang."[10]

"De leden van de VVD-fractie lezen dat de risico's voor het functioneren van het geautomatiseerde werk bij de voorbereiding niet altijd volledig in te schatten zijn en dat de risico's soms volledig(er) in beeld komen nadat er is binnengedrongen. Deze leden vragen of hier nog iets tegenover wordt gesteld en of er een waarborg is die dit probleem ondervangt. Voor het op afstand binnendringen van een geautomatiseerd werk is een bevel van de officier van justitie vereist. De officier van justitie zal zich door de betrokken opsporingsambtenaren zorgvuldig laten informeren over de noodzaak van de inzet van de bevoegdheid, en de risico's die daaraan zijn verbonden. Dit is ook van belang voor de afgifte van de machtiging door de rechter-commissaris. Hierboven is reeds aangegeven dat hierbij ook gekozen kan worden voor een meer stapsgewijze aanpak, waarbij op basis van de informatie die is verkregen in het kader van de vaststelling van bepaalde kenmerken van het geautomatiseerde werk beslissingen worden genomen over de verdere aanpak. Voor de inschatting, beheersing en beperking van de risico's voor het systeem is de deskundigheid van de opsporingsambtenaren van het technische team belast met het binnendringen van essentieel belang. Op grond van het voorgestelde artikel 126nba, zevende lid, Sv worden bij of krachtens algemene maatregel van bestuur eisen gesteld aan het deskundigheids- niveau dat van deze opsporingsambtenaren mag worden verwacht." [11]

[8] Kamerstukken II, 2015/16, 34 372, nr. 3, p. 103 (MvT)
[9] Vgl. Kamerstukken II, 2015/16, 34 372, nr. 3, p. 103 (MvT)
[10] Kamerstukken II, 2015/16, 34 372, nr. 32/33, p. 102 (MvT)
[11] Vgl. Kamerstukken II, 2015/16, 34 372, nr. 6, p. 60-61 (NV II)

Over de mate waarin het binnendringen risico's met zich mee brengt voor het functioneren van het geautomatiseerde werk of derden, zal de rechter-commissaris in het kader van de proportionaliteitstoets actief geïnformeerd moeten worden. Dat geldt ook voor de risico's bij het doen van de onderzoekshandelingen.

Opmerking verdient verder dat de wetgever in de Nota naar aanleiding van het verslag heeft overwogen dat de rechter-commissaris in een concreet geval kan bepalen dat het binnendringen van een geautomatiseerd werk en/of het verrichten van bepaalde onderzoekshandelingen in zijn aanwezigheid worden verricht.[12] Hoe de wetgever dit ziet in relatie tot de rol van de officier van justitie als centraal en leidend magistraat in het opsporingsonderzoek, is door de wetgever niet uitgewerkt. Indien dit zich in de praktijk voordoet, is het van belang te onderkennen dat de uitvoering van een bijzondere opsporingsbevoegdheid een andere rol voor de rechter-commissaris kent, dan bij de uitvoering van bijvoorbeeld een doorzoeking ter inbeslagname.

<u>Buitenlandse gegevens en toetsing door de rechter-commissaris</u>

In de parlementaire behandeling van art. 126nba Sv is uitgebreid stilgestaan bij de internationale aspecten van de uitoefening van de bevoegdheid.

Conform het bepaalde in art. 126nba lid 2 sub b Sv vermeldt het bevel indien de gegevens niet in Nederland zijn opgeslagen. Ten aanzien van de toetsing door de rechter-commissaris op dit punt heeft de wetgever in de Memorie van Toelichting opgemerkt:

> "Indien bekend is dat de gegevens niet in Nederland zijn opgeslagen, dient dit in het bevel te worden vermeld. Bij de afgifte van de machtiging mag de rechter-commissaris ervan uitgaan dat de officier van justitie de regels op het gebied van de internationale samenwerking respecteert. Zoals ook in het algemeen deel aan de orde is gekomen, behoeft dit niet bij voorbaat in de weg te staan aan onverwijld optreden als de omstandigheden daartoe aanleiding geven. De uitvoering van de machtiging betreft echter vooraleerst de verantwoordelijkheid van de officier van justitie; deze functionaris dient de machtiging op zorgvuldige wijze uit te voeren en de uitvoering bij de rechter te verantwoorden."[13]

In de 'Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv' zijn de kaders beschreven waarbinnen de officier van justitie werkt indien de gegevens niet in Nederland zijn opgeslagen / het geautomatiseerde werk zich in het buitenland bevindt.

Een schending van soevereiniteit zal politieke gevolgen kunnen hebben. Dat door een eventuele schending van het volkenrecht een rechtens te respecteren belang van verdachte wordt geschonden, is niet goed denkbaar.[14]

Op welke wijze de rechter-commissaris de omstandigheid dat gegevens niet in Nederland zijn opgeslagen, moet betrekken bij zijn beoordeling van een vordering tot machtiging is door de wetgever niet nader uitgewerkt.

---

[12] Kamerstukken II, 2015/16, 34 372, nr. 6, p. 51 (NV II)
[13] Kamerstukken II, 2015/16, 34 372, nr. 3, p. 102 (MvT)
[14] Vgl. HR 17 april 2012, ECLI:NL:HR:2012:BV9070

Uitgangspunten informeren van de rechter-commissaris bij de inzet van art. 126nba Sv

Het voorgaande leidt tot een aantal uitgangspunten bij het informeren van de rechter-commissaris bij de inzet van art. 126nba Sv.

- Over het binnendringen in een geautomatiseerd werk en de wijze waarop dit gebeurt, kan de landelijk DIGIT officier van justitie de rechter-commissaris desgevraagd (mondeling) informeren. Daarbij zal extra aandacht uit moeten gaan naar het zwaarwegende opsporingsbelang om de methodiek van het binnendringen niet aan de openbaarheid prijs te geven.
- Over de te verrichten onderzoekshandelingen en de wijze waarop die worden uitgevoerd zal de rechter-commissaris actief geïnformeerd moeten worden.
- Over de mate waarin het binnendringen en/of de onderzoekshandelingen risico's met zich mee brengt voor het functioneren van het geautomatiseerde werk of derden, wordt de rechter-commissaris actief geïnformeerd. Dergelijke technische risico's komen namelijk aan de orde in het kader van de proportionaliteits- en subsidiariteitsafweging die de rechter-commissaris en de officier van justitie beide maken bij de inzet van de bevoegdheid.
- Indien de gegevens niet in Nederland zijn opgeslagen / het geautomatiseerde werk zich in het buitenland bevindt, wordt hier in de vordering tot machtiging en het bevel melding van gemaakt.

16 november 2020

LP DIGIT – b.1,2e

	Toegezonden	Afgerond
LP DIGIT	20-10-2020	03-11-2020
Afgestemd LE DIGIT	20-10-2020	03-11-2020
Afgestemd rechercheovj LP	03-11-2020	12-11-2020

Document 28

Vraag 5.1.2e

Zoals gisteren telefonisch al kort besproken, gaan we als juridische vakgroep graag met het OM in overleg over het inloggen in online omgevingen, in de hoop daarin op één lijn te komen. Een gesprek dat wij uiteraard ook graag gaan voeren met het KEC, waarmee de discussie al enige tijd loopt en we ook graag op zo kort mogelijke termijn tot een afspraak komen. We leggen nu eerst bij jou aan omdat de laatste vakgroepvergadering daar alle aanleiding toe bleek te zijn. Tijdens dat overleg kwamen we namelijk unaniem kortweg tot de conclusie dat wanneer er zonder toestemming wordt ingelogd in een online omgeving er sprake is van computervredebreuk maar dat de wederrechtelijk ervan wordt opgeheven door dit te baseren op 126nba Sv. Daarmee ligt de uitvoering van deze handeling in beginsel bij Digit, een keuze die ook werd onderschreven door de jurist van het Digit. Hiermee is ook duidelijk dat wij menen eerst bij jou te moeten aanleggen voor een gesprek hierover.

Reactie 5.1.2e

De conclusie dat wanneer er zonder toestemming wordt ingelogd in een online omgeving, er sprake is van computervredebreuk ex art. 138ab Sr onderschrijf ik. En ook deel ik de conclusie dat – als een opsporingsambtenaar dat doet in het kader van de opsporing – die wederrechtelijkheid wordt weggenomen door art. 126nba Sv. De toevoeging die ik daaraan zou willen doen, is dat die wederrechtelijkheid niet enkel door 126nba Sv kan worden weggenomen. Voor het verkrijgen van toegang tot (online) gegevens in het kader van strafvordering, biedt ons recht m.i. op dit moment een aantal juridische grondslagen.

Sommige hebben een solide basis in wetgeving of een verdrag: met toestemming van een van de rechthebbenden inloggen, het doen van een (heimelijke) netwerkzoeking ex art. 125j Sv of de inzet van de hackbevoegdheid ex art. 126nba Sv.

Anderen hebben een basis in jurisprudentie en zijn daardoor soms wat meer rechtsvormend en onzeker (of zo je wilt experimenteler): 'klassieke' beslaglegging op een account is dat aan te merken is als een 'goed'[1] of inloggen na opdracht/bevel van de rc ex art. 181 Sv jo art. 177 Sv.

Bij deze categorie vind ik van belang dat de wetgever in het Wetboek van Strafvordering nooit heeft beoogd een uitputtende lijst van bijzondere opsporingsbevoegdheden te maken.[2] Dat uitgangspunt is door de Hoge Raad bijvoorbeeld als uitgangspunt genomen bij het beoordelen van pseudoverkoop als bijzondere buitenwettelijke opsporingsbevoegdheid.[3] Belangrijker in deze context vind ik ook de uitspraken van de Hoge Raad over onderzoek aan een inbeslaggenomen gegevensdrager[4] en de lagere rechtspraak die daar uitvoering aan heeft gegeven. Naar aanleiding van die arresten is een bestendige lijn van rechtspraak ontstaan van rechters-commissaris, die na een vordering ex art. 181 Sv hebben bevolen / afgewezen dat onderzoek aan een geautomatiseerd werk werd verricht waarbij op voorhand voorzienbaar was dat daarmee een zeer ingrijpende inbreuk op de privacy van verdachte zou worden gemaakt.[5] Die specifieke bevoegdheid van de rechter-commissaris in dergelijke concrete gevallen staat / stond (nog) niet expliciet in het Wetboek van Strafvordering, maar is onder de algemene (onderzoeks)bevoegdheid van de rechter-commissaris ex art. 181 Sv geschaard.

---

[1] Recent bijvoorbeeld als grondslag voor het inloggen op een Instagram account en dat daarna ontoegankelijk maken.
[2] O.a. Kamerstukken II 1996-97, 25 403, nr. 3 (MvT), p. 9
[3] Zie o.a. HR 20 december 2011, ECLI:NL:HR:2011:BP0070 en HR 5 maart 2019, ECLI:NL:HR:2019:298
[4] De zogeheten 'smartphone arresten' HR 4 april 2017, ECLI:NL:HR:2017:584, ECLI:NL:HR:2017:588 en ECLI:NL:HR:2017:592.
[5] Zie o.a. Rechtbank Noord-Holland 29 juli 2019, ECLI:NL:RBNHO:2019:6764 en Rechtbank Limburg 8 mei 2017, ECLI:NL:RBLIM:2017:4484

Gelet op de snelheid waarmee de mogelijkheden van digitale opsporing zich ontwikkelen en voortdurend veranderen, denk ik dat we in de vorming van recht een belangrijke rol hebben. Dat leidt soms tot een (ingecalculeerd) rechterlijk oordeel dat iets niet kan, zoals bij de netwerkzoeking die op een politie bureau werd voortgezet (Hof Den Haag 22-12-2018, ECLI:NL:GHDHA:2018:3529). In andere gevallen, leidt het tot een uitbreiding van ons instrumentarium. Zoals in het geval van het inloggen na opdracht/bevel van de rc ex art. 181 Sv jo art. 177 Sv, waar inmiddels een voorzichtige lijn is te ontwaren van rechters die dergelijke vorderingen honoreren, beslissingen publiceren en publicaties daarover in vakliteratuur.[6] Die werkwijze is daarbij ook afgestemd met / goed gevonden door de vergadering van rechercheofficieren. Ook de vergadering van coördinerend rc's heeft ingestemd met deze werkwijze.

En zoals opgemerkt lijken de wetgever en rechters ons die ruimte ook te geven. Een overweging van het Hof Den Haag in het arrest over de netwerkzoeking vanaf het politie bureau vind ik daarin een mooie: "*In het onderhavige geval is het hof van oordeel dat kan worden volstaan met de constatering van het vormverzuim. Het belang van de bescherming van het recht op privéleven is weliswaar aanzienlijk, maar het hof constateert dat meer toegespitst op de concrete situatie het recht van de verdachte op een eerlijk proces zoals bedoeld in art. 6, eerste lid, van het EVRM steeds gewaarborgd is geweest, terwijl tevens sprake is geweest van rechterlijk toezicht en maximale transparantie ten aanzien van de verrichte onderzoekshandelingen. Niet gesteld of aannemelijk is geworden dat hier sprake is van een handelen door de politie dat past in een kader van een meer structureel patroon waarbij voormeld vormverzuim wordt begaan. Deze feiten en omstandigheden relativeren naar het oordeel van het hof de ernst van het verzuim in belangrijke mate. Daarenboven is niet aannemelijk geworden dat de verdachte door voormeld vormverzuim op enigerlei wijze daadwerkelijk in zijn verdediging is geschaad of dat daardoor bij hem anderszins in rechte te respecteren nadeel is geleden.*"

Zolang we oog houden voor het zwaarwegende belang van voldoende rechterlijk toezicht en we maximale transparantie ten aanzien van de verrichte onderzoekshandelingen betrachten, vind ik die rechtsvorming passen bij mijn rol als magistraat. Dat past ook in het systeem waarbij de wetgever op die manier wordt aangezet na te denken over codificatie van bepaalde opsporingsmethodieken. Dat is in dit domein recent gebeurd bij de netwerkzoeking vanaf een politie bureau en het ontgrendelen onder dwang van een gegevens dragen (beide voorgesteld in de Innovatiewet Strafvordering). En ook over het inloggen op online accounts met rechtsmatig verkregen inloggegevens, is inmiddels voorwerp van voorbereide wetgeving.

Kort en goed zijn er in mijn idee een aantal wettelijke grondslagen die maken dat bij het inloggen door een verbalisant op een online account de wederrechtelijkheid van diens handelen ontbreekt en daarmee dat handelen in het kader van de opsporing mogelijk is. De uitvoering van het inloggen in een online omgeving kan daardoor bij DIGIT liggen, maar dat is m.i. niet in beginsel het geval.

Bij de afweging of artikel 126nba Sv de aangewezen bevoegdheid is, zal een pluraliteit aan factoren mee kunnen spelen; zoals afbreukrisico voor het onderzoek, technische (on)mogelijkheden, juridische (on)mogelijkheden, afscherming van methodieken, afbreukrisico op

---

[6] Rechtbank Rotterdam 1-1-2018, ECLI:NL:RBROT:2018:8017, Rechtbank Rotterdam 22-2-2019, ECLI:NL:RBROT:2019:2712 en Rechtbank Den Haag 11-1-2019, ECLI:NL:RBDHA:2019:1329.
J.W. van den Hurk en 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 2019/37; p. 34-44.

juridisch vlak e.d. Voor de afweging of art. 126nba Sv ingezet kan worden, zal in het kader van de zware eisen die aan die bevoegdheid worden gesteld (o.a. op het gebied van proportionaliteit en subsidiariteit) veelal eerst gemotiveerd moeten worden afgewogen of enig van de andere grondslagen mogelijk is.

Meer in het bijzonder toegespitst op de vraag wat relevant is in de afweging of art. 126nba Sv aangewezen is of de weg van art. 181 Sv jo art. 177 Sv. Ik denk dat daarin o.a. van belang is:

- op welke wijze de inloggegevens zijn of worden verkregen;

- wat de noodzaak en mate van afscherming van het handelen is;

- of het een geautomatiseerd werk van verdachte betreft;

- de complexiteit van detectie, registratie en transport van gegevens.

[1] Recent bijvoorbeeld als grondslag voor het inloggen op een Instagram account en dat daarna ontoegankelijk maken.
[2] O.a. Kamerstukken II 1996-97, 25 403, nr. 3 (MvT), p. 9
[3] Zie o.a. HR 20 december 2011, ECLI:NL:HR:2011:BP0070 en HR 5 maart 2019, ECLI:NL:HR:2019:298
[4] De zogeheten 'smartphone arresten' HR 4 april 2017, ECLI:NL:HR:2017:584, ECLI:NL:HR:2017:588 en ECLI:NL:HR:2017:592.
[5] Zie o.a. Rechtbank Noord-Holland 29 juli 2019, ECLI:NL:RBNHO:2019:6764 en Rechtbank Limburg 8 mei 2017, ECLI:NL:RBLIM:2017:4484
[6] Rechtbank Rotterdam 1-1-2018, ECLI:NL:RBROT:2018:8017, Rechtbank Rotterdam 22-2-2019, ECLI:NL:RBROT:2019:2712 en Rechtbank Den Haag 11-1-2019, ECLI:NL:RBDHA:2019:1329.
J.W. van den Hurk en 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 2019/37; p. 34-44.

23 december 2020 5.1.2e

Document 38

Juridische kaders binnendringen ex art. 138ab Sr en art. 126nba Sv

Landelijk Parket - DIGIT

Inleiding

In art. 138ab Sr is het binnendringen van een geautomatiseerd werk strafbaar gesteld. In art. 126nba Sv is de bijzondere opsporingsbevoegdheid opgenomen die het mogelijk maakt om een geautomatiseerd werk binnen te dringen (en vervolgens onderzoekshandelingen te verrichten). Beide bepalingen zijn in zekere zin elkaars spiegelbeeld. In het wetboek van strafrecht is een handeling verboden die in het wetboek van strafvordering als bevoegdheid is opgenomen. In beide gevallen wordt met binnendringen hetzelfde bedoeld. In de parlementaire behandeling bij de Wet Computercriminaliteit III schrijft de wetgever:

> "Voor de regeling rond het binnendringen van het geautomatiseerde werk is aangesloten bij de regeling van de computervredebreuk in het Wetboek van Strafrecht. Op grond van deze regeling is van binnendringen 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 (artikel 138ab, eerste lid, Sr)."[1]

In dit stuk wordt een handreiking gegeven om te bepalen of sprake is van binnendringen in een geautomatiseerd werk.

Binnendringen – art 138ab Sr

In 1993 is met de Wet computercriminaliteit het binnendringen in een geautomatiseerd werk strafbaar gesteld. Tot 2010 stond de strafbepaling in art. 138a Sr (oud) opgenomen. In 2010 is door een vernummering de strafbaarstelling opgenomen art. 138ab Sr.

Art. 138ab lid 1 Sr luidt op dit moment als volgt:

> "Met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie wordt, als schuldig aan computervredebreuk, gestraft hij die opzettelijk en wederrechtelijk binnendringt in een geautomatiseerd werk of in een deel daarvan. Van binnendringen is in ieder geval sprake indien de toegang tot het werk wordt verworven:
> a. door het doorbreken van een beveiliging,
> b. door een technische ingreep,
> c. met behulp van valse signalen of een valse sleutel, of
> d. door het aannemen van een valse hoedanigheid."

De wetgever heeft vanaf het begin van strafbaarstelling gezocht naar een definiëring van binnendringen, maar lijkt niet tot een vastomlijnde afbakening te zijn gekomen. In eerste instantie hechtte de wetgever aan het bestaan van een minimale, maar wel daadwerkelijke

[1] Kamerstukken II, 2015/16, 34 372, nr. 3, p. 15 (MvT)

beveiliging die moest worden doorbroken.[1] Daar kwam de wetgever tijdens de behandeling van het wetsvoorstel weer op terug, om ook inloggen met het gebruik van een alom bekend (gelekt) wachtwoord onder de strafbaarstelling te laten vallen.[2] De wetgever verwoordde later in de behandeling dat van binnendringen sprake was, *"indien men zich de toegang verschaft tegen de onmiskenbare wil van de rechthebbende, welke zowel uit woorden als uit daden kan blijken"*. De wetgever duidt dat nader:

> *"Allereerst wordt onder a een expliciete handeling van de rechthebbende vereist, namelijk het aanbrengen van «enige beveiliging». Er zal een kenbare drempel moeten bestaan zodat onbevoegden zich niet simpelweg de toegang kunnen verschaffen."*

en

> *"Daarnaast stelt artikel 138a, onder b, strafbaar degene die een systeem binnendringt waarbij geen sprake is van doorbreking van enige beveiliging in strikte zin."*[4]

In 2004 heeft de wetgever in de tweede nota van wijziging van de wet Computercriminaliteit II het binnendringen verder verruimd.[5] Tot de wijziging met de wet Computercriminaliteit II was sub a – d cumulatief verwoord. Dat werd met de nieuwe tekst los gelaten. Sub a-d werden ingeleid met de tekst dat van binnendringen *in ieder geval* sprake was, als het viel onder een van die subs. De wetgever schrijft:

> *"Mede met het oog op een zo krachtig mogelijke bestrijding van het verschijnsel «hacking» acht ik het daarom wenselijk geen beperking aan te brengen maar artikel 138a zodanig te herformuleren, dat in beginsel ieder opzettelijk en wederrechtelijk binnendringen in een computer(systeem) bestraft kan worden. Daarom stel ik voor de onderdelen a en b van artikel 138a, die thans nog als voorwaarde voor strafbaarheid zijn geformuleerd, te formuleren als voorbeelden van gevallen waarin sprake is van «binnendringen», door aan te geven dat in die gevallen in ieder geval sprake is van binnendringen in de zin van dit artikel. Daarmee wordt voor de jurisprudentie de nodige ruimte geschapen om ook andere methoden waarmee toegang wordt verworven, als binnendringen aan te merken."*[6]

Met die laatste zin verplaatst de wetgever de zoektocht naar een afbakening van 'binnendringen' naar de rechter (en daaraan voorafgaand naar het Openbaar Ministerie en de opsporingsdiensten). Waarmee niet direct een oplossing wordt geboden, maar het probleem vooral verschuift. Iets wat door A-G Knigge wat scherp werd verwoord op 22 februari 2011.

> *"Als de wetgever er niet in slaagt om een helder omlijnd begrippenapparaat te presenteren, mag van de rechter niet verwacht worden dat hij er wél chocola van weet te maken."*[7]

Uit het voorgaande volgt dat er bij het bepalen of sprake is van binnendringen in een geautomatiseerd werk veel ruimte is voor interpretatie in de rechtspraktijk. De wetgevingsgeschiedenis biedt wel een aantal handvatten. Net als jurisprudentie en wetenschappelijke literatuur.

---

[1] Kamerstukken II, 1990/91, 21 551, nr. 3, p. 16 (MvT)
[2] Kamerstukken II, 1990/91, 21 551, nr. 6, p. 31-32 (MvA)
[4] Kamerstukken II, 1990/91, 21 551, nr. 11, p. 18 (NV). NB. In de toenmalige tekst van art. 138a Sr (oud) waren de huidige sub b, c en d samengevoegd in sub b.
[5] Kamerstukken II, 2004/05, 26 671, nr. 7 (Nota van wijziging II).
[6] Kamerstukken II, 2004/05, 26 671, nr. 7, p. 31-32 (Nota van wijziging II).
[7] PHR 22 februari 2011, ECLI:NL:PHR:2011:BN9287 (Toxbot)

De conclusie[8] van Knigge bij het arrest van de Hoge Raad van 22 februari 2011[9] in de Toxbot zaak is daarbij lezenwaardig. Knigge schets niet alleen uitvoerig de parlementaire behandeling rond de vraag wat binnendringen is, maar verwoord ook in detail wat daarbij de problemen en onduidelijkheden zijn. Hij formuleert ook een criterium dat voor de praktijk waardevol is als centrale vraag bij het bepalen of sprake is van binnendringen van een geautomatiseerd werk.

> "Art. 138a Sr vraagt om een normatieve invulling die functioneel is, die voorziet in een effectieve strafrechtelijke bescherming tegen onbevoegde kennisneming van in geautomatiseerd werken opgeslagen gegevens. Het criterium voor de vraag of onbevoegd gebruik is gemaakt van de ingeprogrammeerde toegangsmogelijkheden van een geautomatiseerd systeem, zou ik dan ook, wat de toegang door middel van telecommunicatie betreft, willen zoeken in hetgeen in het maatschappelijk (internet)verkeer algemeen geaccepteerd is. Alle methoden van toegangverschaffing die het normale, algemeen geaccepteerde gebruik van de programmatische mogelijkheden van op de telecommunicatie-infrastructuur aangesloten systemen te buiten gaan, leveren in beginsel het onbevoegd gebruik van die mogelijkheden op."[10]

Die overweging zou je kunnen vatten in de volgende vraag:

- Ging de toegang verschaffing verder dan het normale, algemeen geaccepteerde gebruik van de programmatische mogelijkheden van het geautomatiseerd werk?

Bij positieve beantwoording van die vraag zou je kunnen stellen dat sprake is van binnendringen in een geautomatiseerd werk.

Naast deze aan Knigge's conclusie ontleende vraag, kunnen de volgende vragen helpen bij het beoordelen of sprake is van binnendringen in het geautomatiseerd werk.

- Heeft men zich de toegang verschaft tot een geautomatiseerd werk tegen de onmiskenbare wil van de rechthebbende, welke wil zowel uit woorden als uit daden kan blijken?[11]
- Is er een kenbare drempel in het geautomatiseerd werk overschreden?[12]
  NB. Als louter sprake is van onbelemmerde toegang, is geen sprake van binnendringen.
- Hebben handelingen tot doel om het technisch functioneren van het geautomatiseerde werk zodanig te veranderen dat, ondanks het ontbreken van bijvoorbeeld de juiste toegangscodes of -gegevens, toegang verworven kan worden?[13]
- Is voorgewend dat sprake was van een autorisatie door de 'rechthebbende'?
- Is er gebruik gemaakt van een wachtwoord of ander (inlog)gegeven door iemand die daartoe niet gerechtigd was?

---

[8] PHR 22 februari 2011, ECLI:NL:PHR:2011:BN9287 (Toxbot)
[9] HR 22 februari 2011, ECLI:NL:HR:2011:BN9287 (Toxbot)
[10] Punt 77 in PHR 22 februari 2011, ECLI:NL:PHR:2011:BN9287 (Toxbot)
[11] Kamerstukken II, 1990/91, 21 551, nr. 11, p. 18 (NV).
[12] Kamerstukken II, 1990/91, 21 551, nr. 11, p. 18 (NV).
[13] Kamerstukken II, 2004/05, 26 671, nr. 7, p. 31-32 (Nota van wijziging II).

In het SDU Commentaar Strafrecht op artikel 138ab geven Gerritsma-Breur en Nederlof een mooie serie voorbeelden van binnendringen in een geautomatiseerd werk.[14]

- Het tegen de wil van de rechthebbende binnendringen in een computer langs een weg die de aanwezige beveiliging niet of onvoldoende afsluit, waarbij niet van belang is of die opening inherent is aan het systeem of is veroorzaakt door andere hackers.
- Het laten crashen van het inlogprogramma, zodat iedereen zonder verdere controle toegang heeft tot het geautomatiseerde werk.
- Het buiten de reguliere vragenstructuur om verleiden van een server om informatie te geven.
- Het versturen van een hyperlink naar slachtoffers die bij het openen van deze link een virus binnenhalen waarmee anderen toegang kunnen verkrijgen tot de computer.
- Een wachtwoord dat wordt gebruikt door iemand die daartoe niet gerechtigd is.
- Het inloggen op een besloten gedeelte van een site waartoe iemand vanwege wisseling van dienstverband niet meer gerechtigd was.
- Het gebruiken van een IP-adres dat bij het te hacken systeem bekend is of als vriendelijk wordt beschouwd en daarmee mogelijk automatisch toegang verkrijgt tot het systeem.
- Het verleiden van de mens om persoonlijke gegevens zoals een wachtwoord af te geven ('social engineering') en die gegevens gebruiken om in te loggen.
- Een technische variant van social engineering, waarbij iemand via een opgemaakte nepsite wordt verleid zijn inloggegevens af te geven en die gegevens vervolgens gebruiken om in te loggen.
- Een computer de naam geven van de printserver en zo (als printer) toegang te krijgen tot de gegeven printopdrachten.
- Het zodanig manipuleren van het technisch functioneren van het geautomatiseerde werk, dat ondanks het ontbreken van het juiste wachtwoord toegang kan worden verkregen.

Tot slot wordt een voorbeeld gegeven dat mooi markeert hoe breed deze strafbepaling kan zijn:

- Indien iemand zich na een fysieke inbraak in een woning toegang verschaft tot een zich in die woning bevindende computer, is sprake van binnendringen in die computer in de zin van art. 138ab Sr.[15]

De huidige strafbaar stelling van binnendringen in een geautomatiseerd werk, heeft zijn oorsprong in het Cybercrime verdrag[16] en het Kaderbesluit over aanvallen op informatiesystemen[17]. Beide spreken echter niet over binnendringen', maar hanteren de term 'toegang' tot een computersysteem of een onderdeel daarvan, danwel een informatiesysteem.

Op 1 maart 2019 werd de Wet Computercriminaliteit III ingevoerd. Daarmee werd onder andere artikel 138c van het Wetboek van Strafrecht gewijzigd. Met die wijziging werd het

[14] C.M. Gerritsma-Breur & A.G. Nederlof in: Sdu Commentaar Strafrecht, art. 138ab Sr (online, bijgewerkt 7 mei 2019)
[15] Kamerstukken I, 2005/06, 26 671, nr. D, p. 3. (MvA I)
[16] Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, Boedapest, 23-11-2001
[17] Kaderbesluit 2005/222/IBZ van de Raad van 24 februari 2005 over aanvallen op informatiesystemen (PbL 2005/69, blz. 67).

wederrechtelijk overnemen van niet-openbare gegevens strafbaar gesteld. In de toelichting op die wijziging schrijft de wetgever:

> *"De voorgestelde strafbepaling is, in aanvulling op de strafbaarstelling van computervredebreuk, vooral van belang voor gevallen waarin de dader rechtmatige toegang heeft tot niet-openbare gegevens van een computer, en deze gegevens wederrechtelijk overneemt."*
> en
> *"Hiermee wordt tegemoet gekomen aan situaties waarin personen gegevens van een computer waartoe zij rechtmatige toegang hebben, bijvoorbeeld vanwege hun functie bij een overheidsinstelling, zonder daartoe gerechtigd te zijn voor zichzelf of voor een ander overnemen."* [18]

Het lijkt er op dat de wetgever met deze aanvulling op de strafbaar stelling van het binnendringen van een geautomatiseerd werk, weer aansluiting zoekt bij de term 'toegang' van het eerder genoemde het Cybercrime verdrag en het Kaderbesluit. Daaruit zou kunnen worden afgeleid dat binnendringen en het opzettelijk en wederrechtelijk verwerven van toegang synoniem zijn.

Binnendringen – art 126nba Sv

Over de term binnendringen in de context van art. 126nba Sv, is nog geen rechtspraak gepubliceerd. Evenmin wordt er in (wetenschappelijke) handboeken nader over geschreven.

Anders dan in de parlementaire behandeling van art. 138ab Sr en art. 138a Sr (oud), heeft de wetgever bij de behandeling van art. 126nba Sv wel concreter gemaakt wat hij ziet als binnendringen.

De wetgever stelt voorop dat verschillende technieken niet limitatief zijn benoemd.[19] De volgende varianten zijn o.a. in de parlementaire geschiedenis benoemd:

- Binnendringen met behulp van inloggegevens die door middel van *social engineering* zijn verkregen. [20]
- Binnendringen met behulp van inloggegevens die door het gebruik van *kunstmatige intelligentie* zijn verkregen. [21]
- Binnendringen met behulp van inloggegevens van een persoon die worden verkregen door diegene te verleiden te reageren op een e-mailbericht of een ander verzoek om contact; *phishing*.[22]
- Binnendringen door het exploiteren van *bekende kwetsbaarheden* in software.[23]
- Binnendringen door het exploiteren van *onbekende kwetsbaarheden* in software. [24]
- Binnendringen door het verkrijgen van inloggegevens door *inlichtingenwerk*.[25]
- Binnendringen door in overleg met *beheerders* toegang tot een systeem of gegevens te verkrijgen.[26]

[18] Kamerstukken II, 2015/16, 34 372, nr. 3, p. 64 (MvT),
[19] Kamerstukken II, 2015/16, 34 372, nr. 3, p. 34 (MvT), Kamerstukken II, 2015/16, 34 372, nr. 6, p. 72 (NV II) en Kamerstukken II, 2015/16, 34 372, nr. 27, p. 10
[20] Kamerstukken II, 2015/16, 34 372, nr. 3, p. 34 (MvT)
[21] Kamerstukken II, 2015/16, 34 372, nr. 3, p. 34 (MvT)
[22] Kamerstukken II, 2015/16, 34 372, nr. 3, p. 34 (MvT)
[23] Kamerstukken II, 2015/16, 34 372, nr. 3, p. 34 (MvT)
[24] Kamerstukken II, 2015/16, 34 372, nr. 3, p. 34 (MvT)
[25] Kamerstukken II, 2015/16, 34 372, nr. 6, p. 64 (NV II)
[26] Kamerstukken II, 2015/16, 34 372, nr. 6, p. 64 (NV II)

- Binnendringen door *spearphishing*.[27]
- Binnendringen door *brute forcing*.[28]
- Binnendringen door *dictionary attacks*.[29]
- Binnendringen door *shoulder surfing*.[30]
- Binnendringen met behulp van een *afgevangen wachtwoord*.[31]

Deze varianten zijn bij de parlementaire behandeling in beperkte mate uitgewerkt. Alleen bij phishing en social engineering is door de wetgever iets uitgebreider beschreven wat daaronder valt.

> "De «social engineering» en het verleiden van personen om te reageren op bijvoorbeeld een emailbericht zijn methoden om de inloggegevens te verkrijgen zodat een geautomatiseerd werk op afstand heimelijk kan worden binnengedrongen."[32]

> "Social engineering kan er op gericht zijn de verdachte te bewegen handelingen te verrichten zodat software wordt geplaatst op het geautomatiseerde werk dat hij gebruikt, met behulp waarvan verbinding met een andere computer mogelijk wordt gemaakt of met behulp waarvan inloggegevens kunnen worden meegelezen. Met phishing wordt geprobeerd de verdachte ertoe te bewegen bepaalde vertrouwelijke gegevens prijs te geven, zoals identificerende gegevens of inloggegevens. Bij de toepassing van deze methoden wordt dus uitgegaan van de – veelal onwetende – medewerking van de verdachte of van een derde die het geautomatiseerde werk gebruikt waarvan de verdachte ook gebruik maakt."[33]

> "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."[34]

Hoewel deze voorbeelden enige richting geven, blijven ze behoorlijk abstract en geven ze veelal invulling aan de voor de hand liggende gevallen van binnendringen.

Conclusie

De conclusie van het voorgaande is dat er geen harde richtlijnen te geven zijn voor het beantwoorden van de vraag of sprake is van binnendringen in een geautomatiseerd werk. De wetgever heeft daarbij veel ruimte gelaten aan de zittingsrechter en daarmee (impliciet) aan het Openbaar Ministerie en de opsporingsdiensten bij de duiding van gedragingen ten aanzien van geautomatiseerde werken. Het algemene beeld daarbij is dat de wetgever gekozen heeft voor een zeer brede strafrechtelijk rechtsbescherming. De definitie van geautomatiseerd werk in art. 80sexies Sr omvat een zeer grote groep van apparaten. Vervolgens zal zeer snel sprake kunnen zijn van binnendringen in dat geautomatiseerd werk.

[27] Kamerstukken II, 2015/16, 34 372, nr. 8, 11 en 13
[28] Kamerstukken II, 2015/16, 34 372, nr. 8, 11 en 13
[29] Kamerstukken II, 2015/16, 34 372, nr. 8, 11 en 13
[30] Kamerstukken II, 2015/16, 34 372, nr. 8, 11 en 13
[31] Kamerstukken II, 2015/16, 34 372, nr. 27, p. 10
[32] Kamerstukken II, 2015/16, 34 372, nr. 6, p. 67 (NV II)
[33] Kamerstukken II, 2015/16, 34 372, nr. 6, p. 72 (NV II)
[34] Kamerstukken II, 2015/16, 34 372, nr. 8, 11 en 13

Dit betekent voor de opsporingspraktijk dat voor een deel van handelingen ten aanzien van geautomatiseerde werken niet op voorhand duidelijk is of die als binnendringen van het geautomatiseerd werk moeten/kunnen worden aangemerkt. Ongeacht of dat handelingen zijn die door verdachten worden begaan bij het plegen van strafbare feiten of door opsporingsambtenaren bij het opsporen daarvan.

De beoordeling zal steeds casuïstisch zijn en resulteren in een bepleitbaar standpunt, in plaats van een vastomlijnd criterium of handvat. Het is daarom aan te bevelen om voor die beoordeling overleg te voeren met ter zake gespecialiseerde juristen, zoals cybercrime officieren van justitie en -parketsecretarissen, medewerkers van het Kennis en Expertisecentrum Cybercrime (KEC) van het Landelijk Parket en de operationeel juristen van politie die zich bezig houden met cybercrime en digitale opsporing.

21 december 2021

LP DIGIT – 5.1.2e

	Toegezonden	Afgerond
LP DIGIT	9-6-2021	21-12-2021
Afgestemd LE DIGIT	9-6-2021	21-12-2021

Document 39

Notitie | waarborgen bij 126nba

Landelijk Parket - Digit

Aanvullende en procedurele waarborgen betrouwbaarheid, integriteit en herleidbaarheid

Wettelijke verplichting

> "De bevoegdheid van art. 126nba Sv maakt het mogelijk om op afstand en heimelijk binnen te dringen in een geautomatiseerd werk dat in gebruik is bij de verdachte. Het technisch team verricht na binnendringen onderzoekshandelingen in een geautomatiseerd werk waarmee gegevens worden vastgelegd op een technische infrastructuur. Het onderzoek wordt uitgevoerd aan de hand van de in het bevel omschreven onderzoekhandelingen. Uitgangspunt is hierbij dat de onderzoekshandelingen die door het technisch team worden verricht bij de uitvoering van een bevel, worden verricht met een technisch hulpmiddel. Wanneer het onderzoeksbelang dit dringend vordert kan de officier van justitie bepalen dat een niet gekeurd technisch hulpmiddel wordt gebruikt. Een niet gekeurd technisch hulpmiddel dient achteraf gekeurd te worden, tenzij naar het oordeel van de officier de aard van het technisch hulpmiddel zich tegen keuring verzet. Ook kunnen op bevel van de officier onderzoekshandelingen worden verricht zonder de inzet van een technisch hulpmiddel waarbij gegevens handmatig worden veiliggesteld. Van het verrichten van onderzoekshandelingen zonder technisch hulpmiddel is sprake als geen gebruik wordt gemaakt van software die gegevens "detecteert, registreert en transporteert"."[1]

Op grond van artikel 21 lid 4 Besluit onderzoek in een geautomatiseerd werk ("Besluit") dienen er, in het geval er met een technisch hulpmiddel dat naar zijn aard niet kan worden gekeurd gegevens worden vastgelegd, aanvullende waarborgen te worden getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van die vastgelegde gegevens te garanderen.

Op grond van artikel 21 lid 5 van het Besluit dienen er, in het geval er zonder een technisch hulpmiddel (dus handmatig) gegevens worden vastgelegd, procedurele waarborgen te worden getroffen om de betrouwbaarheid, integriteit en herleidbaarheid te garanderen van de tijdens het onderzoek vast te leggen gegevens te garanderen.

---

[1] Nota van Toelichting bij het Besluit, p. 32.

In het navolgende zal worden ingegaan op het verschil tussen de aanvullende en procedurele waarborgen en wat dit betekent voor de toepassing in het kader van de hackbevoegdheid.

Aanvullende of procedurele waarborgen

Invulling van de waarborgen bij inzet TH
Het Besluit geeft onder artikel 21 lid 4 aan dat aanvullende waarborgen getroffen dienen te worden in het geval er met een technisch hulpmiddel dat naar zijn aard niet kan worden gekeurd gegevens worden vastgelegd. Het betreft een aanvulling op de eisen die als basisvoorwaarden gesteld worden bij de inzet van een technisch hulpmiddel, onder artikel 8-13 van het Besluit. Dit zijn eisen voor een herleidbare, betrouwbare en integere vastlegging van gegevens:

- Gerichte werking, detectie en registratie (artikel 8 en 9)
- Registratie op een wijze dat de gegevens identiek zijn aan de inhoud van de gedetecteerde gegevens (artikel 10)
- Registratie met uniek gegeven (artikel 11)
- Registratie met datum en tijd (artikel 12)
- Beveiliging tegen wijziging van gegevens (artikel 10 en 13)

Voor de inzet van een technisch hulpmiddel dient als uitgangspunt voldaan te worden aan deze gestelde eisen. Dit nog los van de vraag of een technisch hulpmiddel wel of niet gekeurd kan worden. Indien een technisch hulpmiddel goed gekeurd is, wordt geacht dat hiermee voldoende waarborgen zijn getroffen voor een herleidbare, betrouwbare en integere vastlegging van gegevens.

Indien reeds op voorhand bekend is dat keuring van een technisch hulpmiddel niet mogelijk zal zijn, dienen bij de inzet van dit hulpmiddel reeds aanvullende waarborgen getroffen te worden. Onder omstandigheden kan het eveneens aanbeveling verdienen aanvullende waarborgen te treffen indien voor de inzet geen voorafgaande goedkeuring heeft plaatsgevonden.

In de Nota van Toelichting bij het Besluit wordt opgemerkt dat er bij aanvullende waarborgen gedacht kan worden aan[2]:

- Een uitgebreide omschrijving van de functionele specificaties van op maakt 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
- Het audiovisueel vastleggen van de uitvoering van de onderzoekshandelingen

Dit betreft uitdrukkelijk geen limitatieve lijst met (verplicht te treffen) waarborgen.

De aanvullende waarborgen kunnen – bovenop de basiseisen van de artikelen 8-13 van het Besluit – de rechtmatigheid van de inzet waarborgen en voorkomen dat er twijfel

[2] Stb. 2018, 340, p. 45.

ontstaat over de betrouwbaarheid, integriteit en herleidbaarheid van de vastgelegde gegevens.

Invulling van de waarborgen bij inzet zonder TH
Indien bij het onderzoek in een geautomatiseerd werk geen technisch hulpmiddel wordt ingezet, dienen waarborgen getroffen zodat er op geen enkel moment twijfel ontstaat over de betrouwbaarheid, integriteit en herleidbaarheid van de vastgelegde gegevens. Artikel 21 lid 5 van het Besluit benoemt dit als procedurele waarborgen.

De inzet van een technisch hulpmiddel geeft met de voorwaarden in de artikelen 8-13 van het Besluit een zeker minimum aan waarborgen voor de inzet. Bij handmatige inzet ontbreken dergelijke basisvoorwaarden.

Handmatige inzet brengt automatisch met zich mee dat de concrete inzet door en voor het oog van een opsporingsambtenaar wordt verricht. Van alle handelingen en verrichtingen kan op ambtseed of ambtsbelofte proces-verbaal worden opgemaakt.

Bovendien worden – zoals reeds naar voren kwam in het antwoord van de minister op vragen van de VVD en D66 – onderzoekshandelingen die verricht worden zonder technisch hulpmiddel standaard gelogd[1]. Hierbij valt te denken aan het monitoren en loggen van systeemhandelingen, schermopnames en toetsenbordaanslagen, met een exacte logging van datum en tijd. Dit zorgt ervoor dat achteraf verifieerbaar is welke handelingen op welke momenten zijn verricht.
Deze onafhankelijke logging van de onderzoekshandelingen kan de bevindingen van de opsporingsambtenaar derhalve ondersteunen.

Daarnaast kunnen ook op andere wijze waarborgen getroffen worden. Bij handmatige inzet zal altijd maatwerk geleverd moeten worden. Bij het treffen van concrete waarborgen zal onder andere rekening gehouden worden met de risico's op ontdekking van de inzet en de risico's voor het geautomatiseerde werk.
Ter illustratie kan bijvoorbeeld gedacht worden aan de volgende waarborgen:
- Meekijken door een andere opsporingsambtenaar uit het technisch team
- Het vooraf en achteraf maken van een kopie
- Het vooraf en achteraf hashen van de veilig te stellen gegevens
- Beveiliging van gegevenstransport door middel van het gebruik van end-to-end versleuteling
- Het audiovisueel vastleggen van de uitvoering van de onderzoekshandelingen
- Het synchroon laten lopen van een (IP)tap

<u>Verantwoording in processen-verbaal</u>

Verder kan worden opgemerkt dat er een verschil bestaat tussen artikel 21 lid 4 en lid 5 Sv. aangaande het voegen van deze waarborgen bij de processtukken. Dit wordt wel voorgeschreven bij toepassing van lid 4, niet bij lid 5. In de Nota van Toelichting op het

[1] Kamerstukken I 2017/18, G, p. 18.

Besluit worden de leden echter gezamenlijk besproken. Dit levert onder andere de volgende overwegingen op:

> "In uitzonderingsgevallen kan de keuring van een technisch hulpmiddel geheel achterwege blijven, namelijk indien de aard van het technische hulpmiddel zich naar het oordeel van de officier van justitie daartegen verzet (artikel 21, vierde lid). 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 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. Indien de officier van justitie beveelt dat onderzoekshandelingen worden verricht zonder technisch hulpmiddel dan worden ter uitvoering van het bevel de onderzoekshandelingen verricht die omschreven zijn in het bevel (artikel 21, vijfde lid).
> 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, vierde en vijfde lid). Hierbij kan worden gedacht aan een uitgebreide omschrijving van de functionele specificaties van op maat gemaakt technische 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."[4]

Nu het onduidelijk is of lid 5 een omissie bevat of dat er onterecht in de toelichting vanuit is gegaan dat lid 4 en lid 5 allebei die voeging voorschrijven, wordt er vooralsnog voor gekozen om artikel 21 lid 5 Besluit grammaticaal te interpreteren. De waarborgen worden getroffen en afgestemd met de DIGIT officier, maar niet (direct) bij de processtukken worden gevoegd. Er wordt wel rekening gehouden met een rechterlijke oordeel waardoor voeging uiteindelijk wel wordt verzocht. Een duidelijk overzicht van de getroffen waarborgen is derhalve beschikbaar.

Conclusie

Het treffen van waarborgen bij de uitvoering van artikel 126nba Strafvordering heeft als doel de betrouwbaarheid, integriteit en herleidbaarheid van de in het kader van die bevoegdheid vastgelegde gegevens te bewaken. Artikel 21 lid 4 van het Besluit – bij de inzet van een technisch hulpmiddel dat niet gekeurd kan worden – spreekt over het

[4] Stb. 2018, 340, p. 15

treffen van aanvullende waarborgen. Op grond van artikel 21 lid 5 van het Besluit dienen bij een handmatige inzet procedurele waarborgen getroffen te worden.

De uitgangspunten van het Besluit bij de inzet met en zonder technisch hulpmiddelen verschillen van dusdanige aard dat niet gesteld kan worden dat de aanvullende waarborgen onder lid 4 eenzelfde waarborgen betreffen als de procedurele van lid 5.

Schematisch kan dit als volgt worden ingetekend:

<table>
<tr><th>Goedgekeurd technisch hulpmiddel</th><th>Niet goedgekeurd technisch hulpmiddel</th><th>Handmatige inzet</th></tr>
<tr><td rowspan="2">Eisen van artikel 8-13 Besluit</td><td>Eisen van artikel 8-13 Besluit</td><td rowspan="2">Procedurele waarborgen (artikel 21 lid 5 Besluit)</td></tr>
<tr><td>Aanvullende waarborgen (artikel 21 lid 4 Besluit)</td></tr>
</table>

Waar bij de handmatige inzet in het besluit geen concrete (basis)waarborgen of eisen genoemd worden, is dit bij de inzet van een technisch hulpmiddel wel het geval. Slechts indien een technisch hulpmiddel niet gekeurd kan worden, dienen aanvullende waarborgen getroffen te worden. Dit, terwijl bij een handmatige inzet altijd procedurele waarborgen getroffen dienen te worden.

Niet uitgesloten is echter dat bij een concrete inzet een waarborg zowel in de situatie van lid 4 of lid 5 getroffen kan worden in verband met de betrouwbaarheid, integriteit en herleidbaarheid van de in het kader van artikel 126nba Strafvordering vastgelegde gegevens

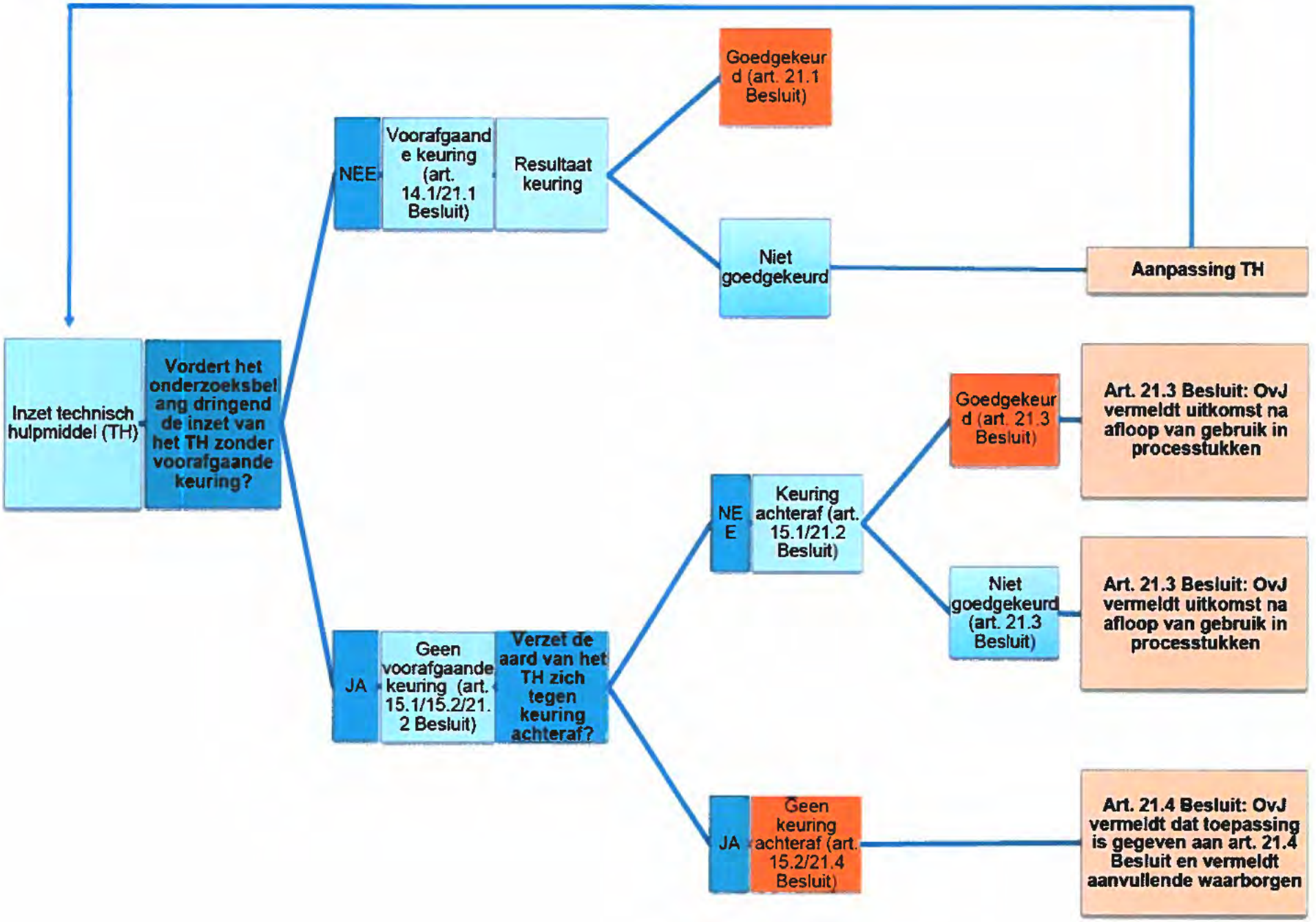
Voorts dient ten aanzien van de verantwoording van een aanvullende of procedurele waarborg een in beginsel een onderscheid gemaakt te worden in het kader van de verantwoordinging. Bij het treffen van aanvullende waarborgen dient dat op grond van het Besluit bij de processtukken gevoegd te worden. De procedurele waarborgen die op grond van artikel 12 lid 5 van het Besluit worden getroffen, hoeven echter niet direct bij de processtukken gevoegd te worden.

Juni 2019
LP Digit

	Toegezonden	Afgerond
LP Digit		*Juni 2019*
Afgestemd LE Digit	Juni 2019	*Juli 2019*

Afgestemd 5.1.2e	Juni 2019	Juli 2019
Afgestemd 5.1.2	Juli 2019	Juli 2019

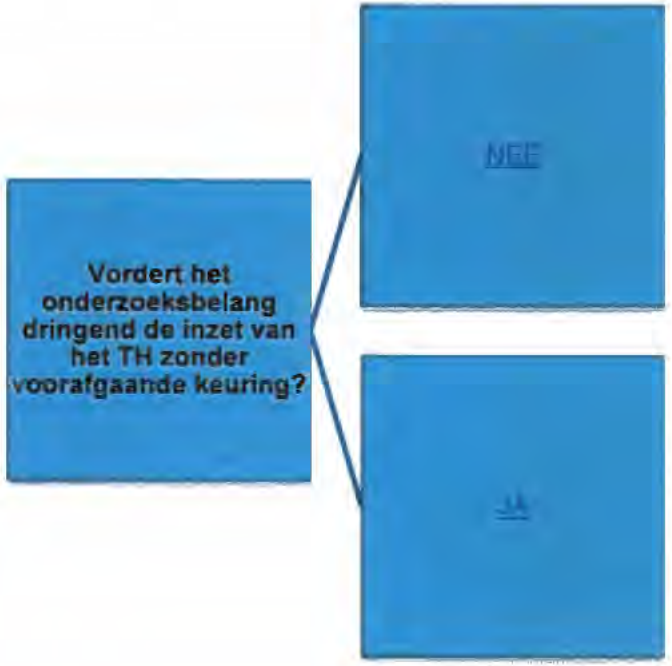
Document 40


Inzet technisch hulpmiddel (TH)
Vordert het onderzoeksbelang dringend de inzet van het TH zonder voorafgaande keuring?
NEE
Voorafgaande keuring (art. 14.1/21.1 Besluit)
Resultaat keuring
Goedgekeurd (art. 21.1 Besluit)
Niet goedgekeurd
Aanpassing TH
JA
Geen voorafgaande keuring (art. 15.1/15.2/21.2 Besluit)
Verzet de aard van het TH zich tegen keuring achteraf?
NEE
Keuring achteraf (art. 15.1/21.2 Besluit)
Goedgekeurd (art. 21.3 Besluit)
Art. 21.3 Besluit: OvJ vermeldt uitkomst na afloop van gebruik in processtukken
Niet goedgekeurd (art. 21.3 Besluit)
Art. 21.3 Besluit: OvJ vermeldt uitkomst na afloop van gebruik in processtukken
JA
Geen keuring achteraf (art. 15.2/21.4 Besluit)
Art. 21.4 Besluit: OvJ vermeldt dat toepassing is gegeven aan art. 21.4 Besluit en vermeldt aanvullende waarborgen

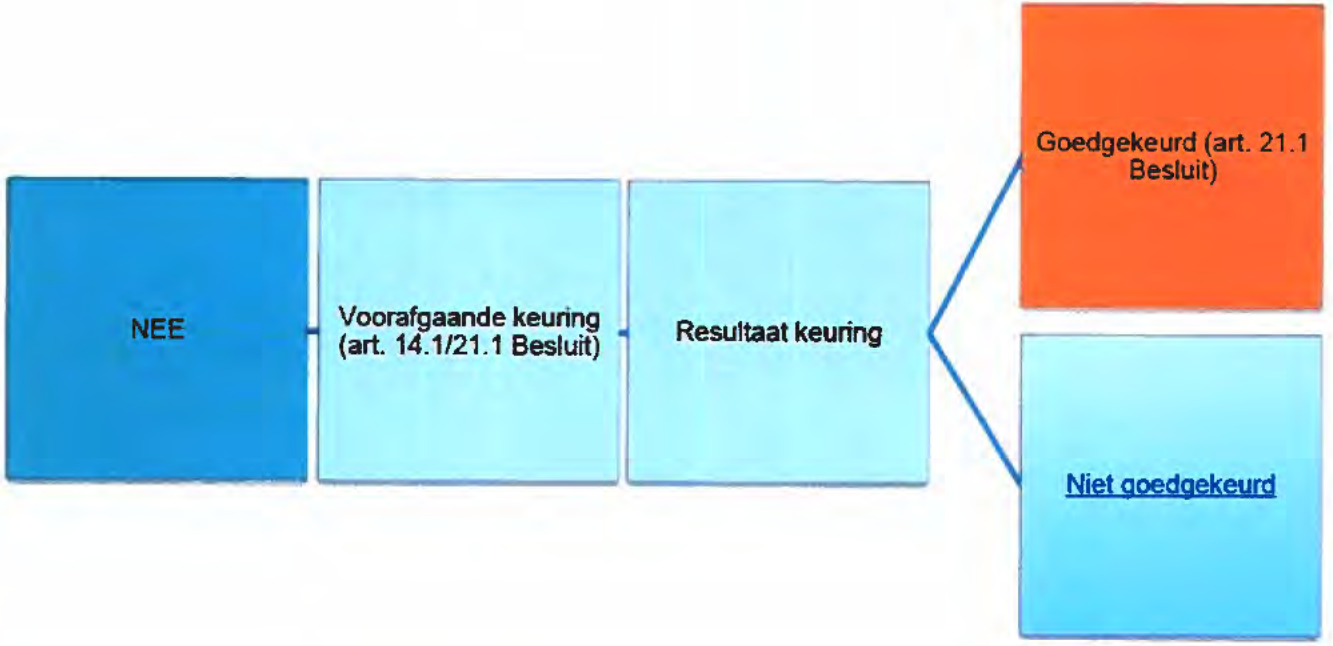
Vordert het onderzoeksbelang dringend inzet zonder keuring vooraf?

Daarbij kan gedacht worden aan de navolgende (niet-limitatieve lijst met) omstandigheden:

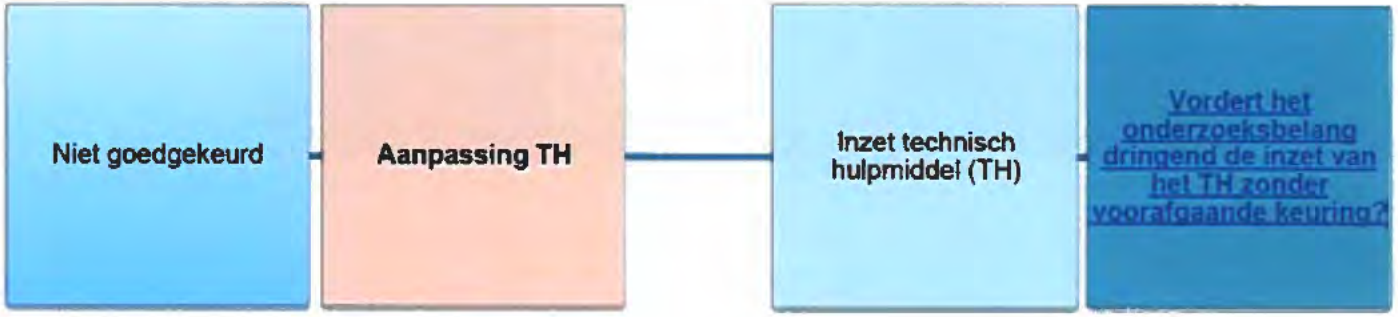
- Het gebruik van speciaal op maat gemaakte software (*NvT Besluit*)
- ...



Het onderzoeksbelang vordert niet dringend inzet zonder keuring vooraf:



Het TH wordt bij voorafgaande keuring niet goedgekeurd:

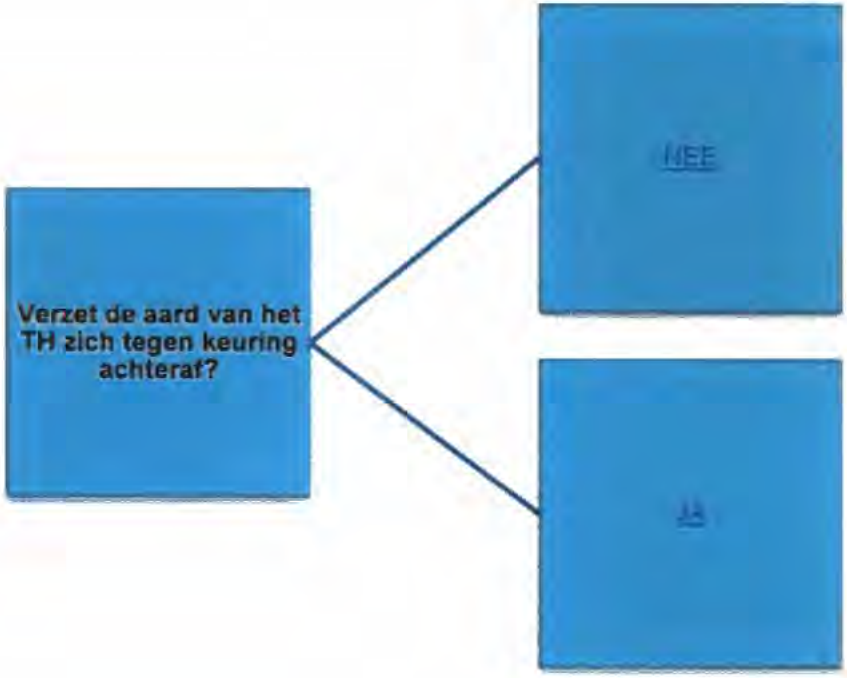


Het onderzoeksbelang vordert dringend inzet zonder keuring vooraf:

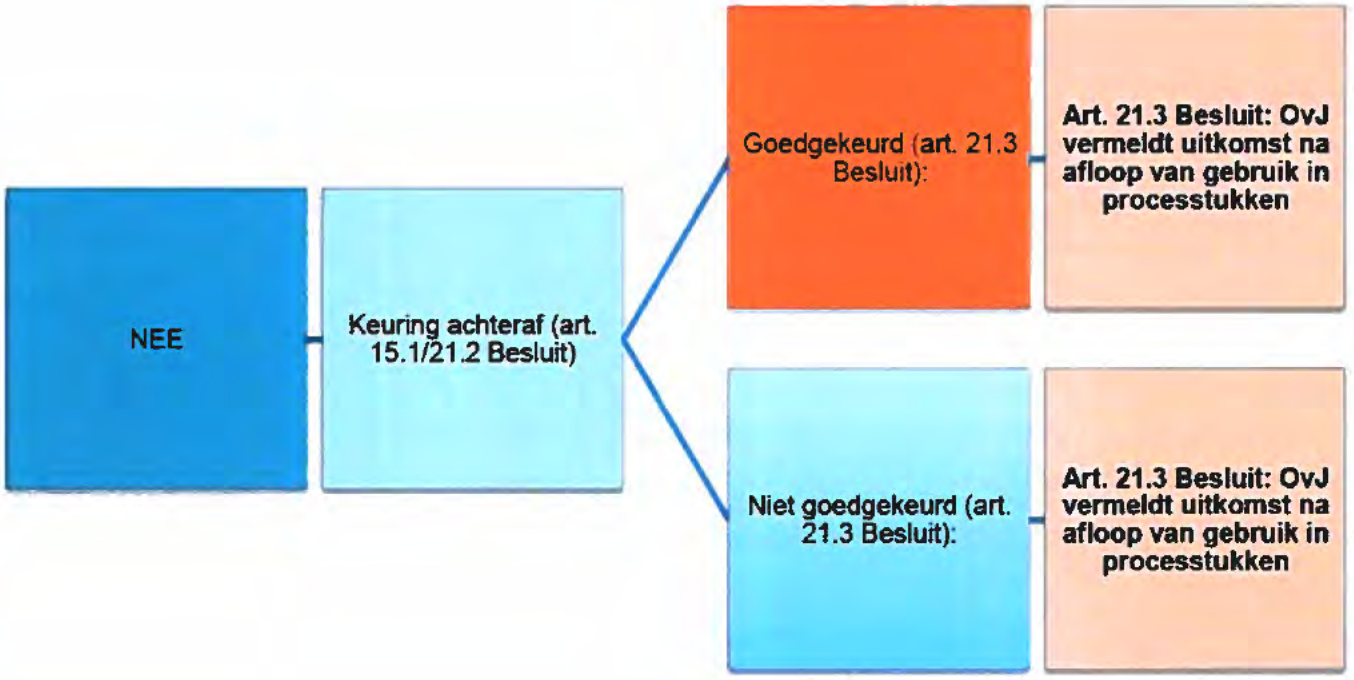
Aard van het TH verzet zich tegen keuring achteraf:

Daarbij kan gedacht worden aan de navolgende (niet-limitatieve lijst met) omstandigheden:

- Het gebruik van speciaal op maat gemaakte software (*NvT Besluit*)
- ...



Keuring achteraf:

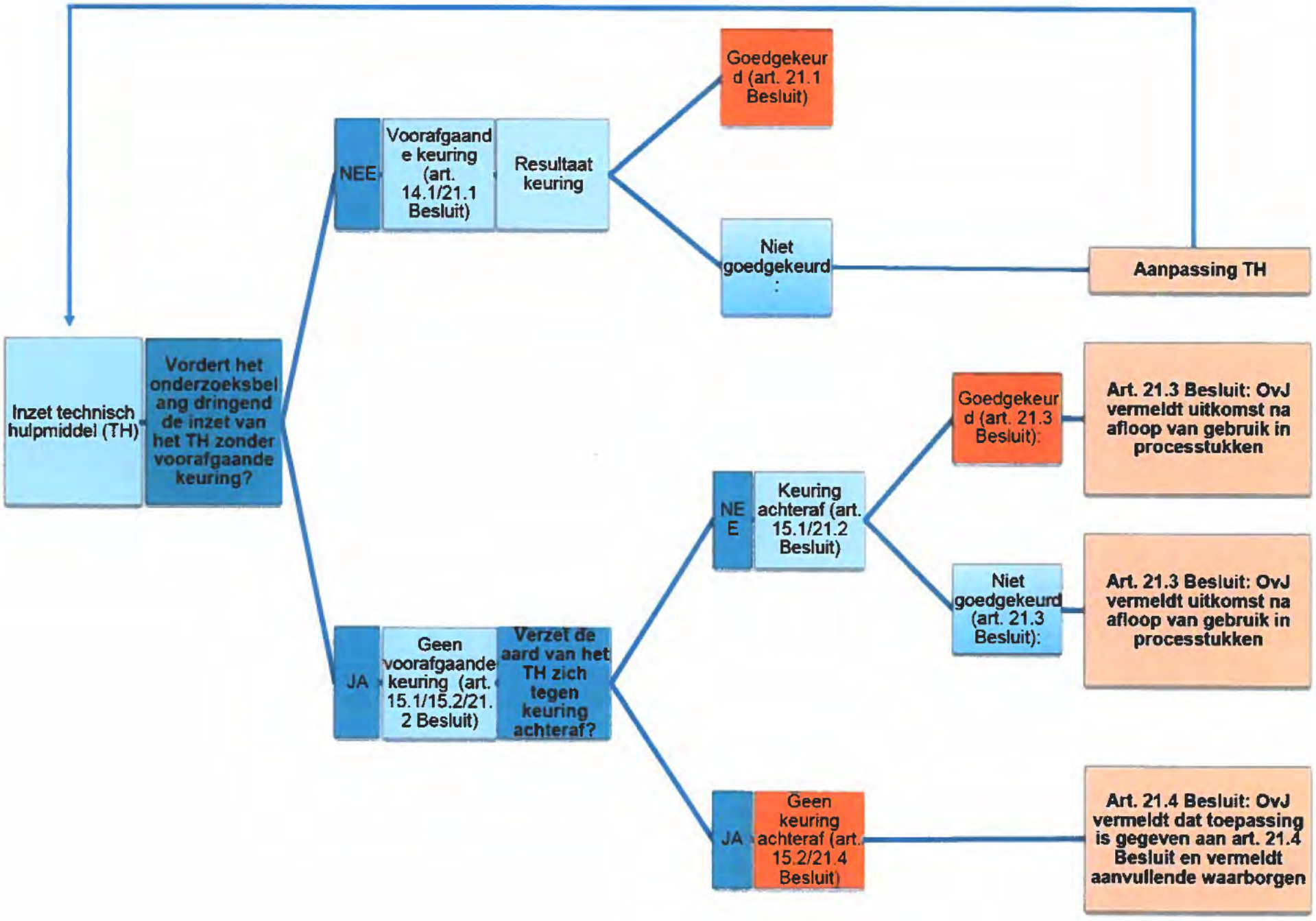


Geen keuring achteraf:

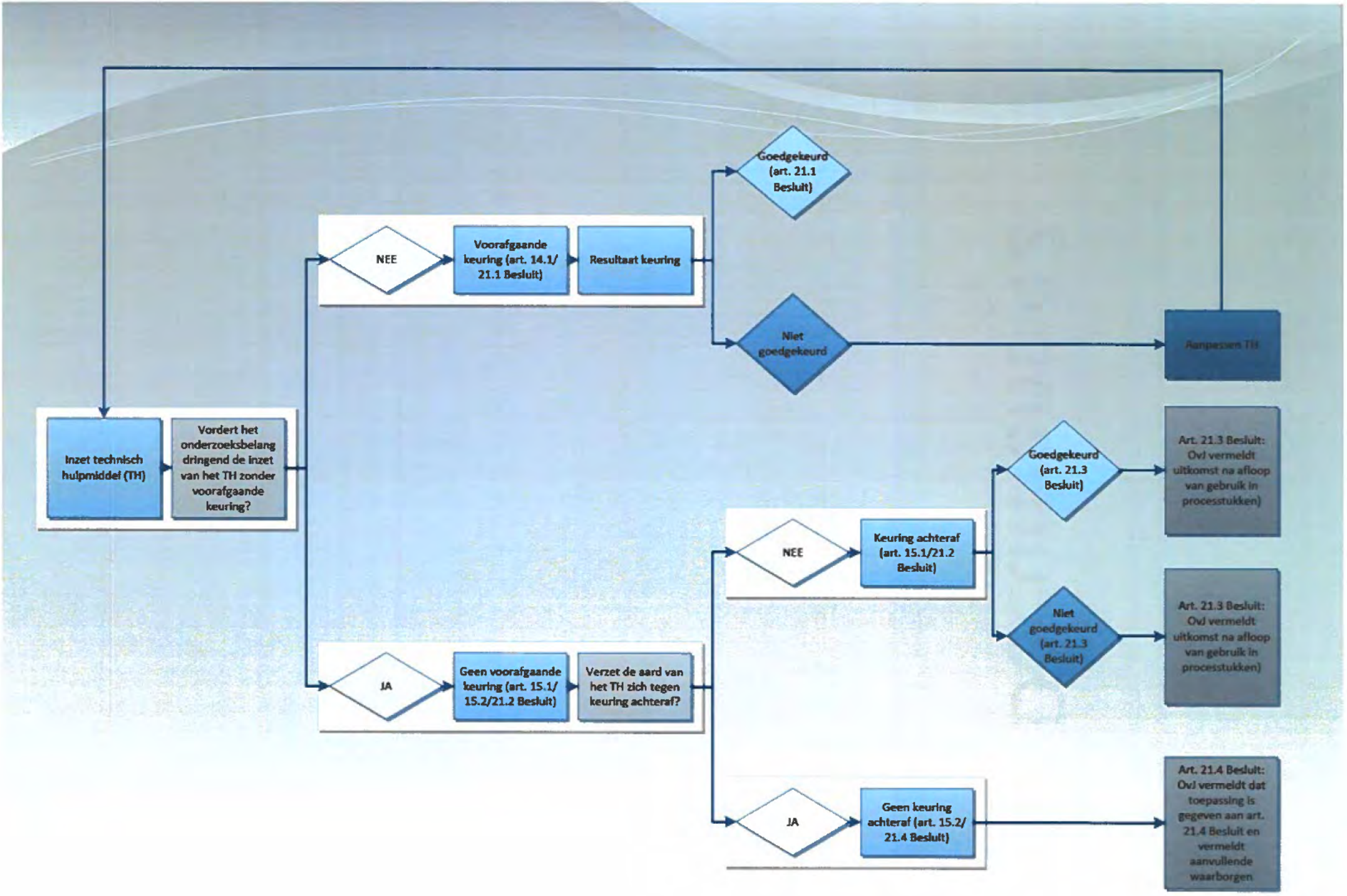
Aanvullende waarborgen:

Daarbij kan gedacht worden aan de navolgende (niet-limitatieve lijst met) aanvullende waarborgen:

- Een uitgebreide omschrijving van de functionele specificaties van op maakt gemaakt technisch hulpmiddel (*NvT Besluit*)
- Het voegen van een digitale kopie van de software en de broncode bij het proces-verbaal (*NvT Besluit*)
- Het vooraf en achteraf maken van een forensische kopie (*NvT Besluit*)
- Het audiovisueel vastleggen van de uitvoering van de onderzoekshandelingen (*NvT Besluit*)
- …


Inzet technisch hulpmiddel (TH)
Vordert het onderzoeksbelang dringend de inzet van het TH zonder voorafgaande keuring?
NEE
Voorafgaande keuring (art. 14.1/21.1 Besluit)
Resultaat keuring
Goedgekeurd (art. 21.1 Besluit)
Niet goedgekeurd:
Aanpassing TH
JA
Geen voorafgaande keuring (art. 15.1/15.2/21.2 Besluit)
Verzet de aard van het TH zich tegen keuring achteraf?
NEE
Keuring achteraf (art. 15.1/21.2 Besluit)
Goedgekeurd (art. 21.3 Besluit):
Art. 21.3 Besluit: OvJ vermeldt uitkomst na afloop van gebruik in processtukken
Niet goedgekeurd (art. 21.3 Besluit):
Art. 21.3 Besluit: OvJ vermeldt uitkomst na afloop van gebruik in processtukken
JA
Geen keuring achteraf (art. 15.2/21.4 Besluit)
Art. 21.4 Besluit: OvJ vermeldt dat toepassing is gegeven aan art. 21.4 Besluit en vermeldt aanvullende waarborgen

Document 41


Inzet technisch hulpmiddel (TH)
Vordert het onderzoeksbelang dringend de inzet van het TH zonder voorafgaande keuring?
NEE
Voorafgaande keuring (art. 14.1/ 21.1 Besluit)
Resultaat keuring
Goedgekeurd (art. 21.1 Besluit)
Niet goedgekeurd
Aanpassen TH
JA
Geen voorafgaande keuring (art. 15.1/ 15.2/21.2 Besluit)
Verzet de aard van het TH zich tegen keuring achteraf?
NEE
Keuring achteraf (art. 15.1/21.2 Besluit)
Goedgekeurd (art. 21.3 Besluit)
Art. 21.3 Besluit: OvJ vermeldt uitkomst na afloop van gebruik in processtukken)
Niet goedgekeurd (art. 21.3 Besluit)
Art. 21.3 Besluit: OvJ vermeldt uitkomst na afloop van gebruik in processtukken)
JA
Geen keuring achteraf (art. 15.2/ 21.4 Besluit)
Art. 21.4 Besluit: OvJ vermeldt dat toepassing is gegeven aan art. 21.4 Besluit en vermeldt aanvullende waarborgen

Document 42

Prioritering technisch hulpmiddel

Landelijk Parket - Digit

Inleiding

Sinds ongeveer een maand heeft Digit (het technisch team dat de hackbevoegdheid mag uitvoeren) de beschikking over een (niet gekeurd) technisch hulpmiddel. Door het College is inmiddels al enkele malen toestemming gegeven voor het gebruik van dit middel.

5.1,2i en 5.2,1

Prioritering Digit

5.1,2i en 5.2,1

Bij de prioritering / toewijzing van een verzoek door Digit wordt er rekening gehouden met het volgende:

5.1,2i en 5.2,1

5.1,2i en 5.2,1

5.1.2i
en 5.2.1

[redacted]

Bovenstaande geldt tav min of meer gelijkwaardige onderzoeken. Uiteraard is er jaarlijks ook een aantal onderzoeken van de buitencategorie waarin zoveel mogelijk (technische beperkingen daargelaten) geleverd wordt.

De beslissing over de inzet zal door de Landelijk Digit OvJ worden teruggekoppeld aan de zaaksovj.

	Toegezonden	Afgerond
Afgestemd Evert		X
Afgestemd Recherche OvJ's		X

Document 43

Notitie | DIGIT LP/LE

Onderzoek al dan niet met een technisch hulpmiddel

[redacted]

Inleiding

A.

Artikel 126nba lid 1 Sv bepaalt, voor zover relevant:

> [de officier van justitie kan] bevelen dat een daartoe aangewezen opsporingsambtenaar binnendringt in een geautomatiseerd werk dat bij de verdachte in gebruik is en, **al dan niet met een technisch hulpmiddel**, onderzoek doet [...]

De vraag rijst wat moet worden verstaan onder een technisch hulpmiddel en wat dan valt onder "al dan niet"; de andere categorie van middelen waarmee onderzoek kan worden gedaan. En of er een bepaalde (dwingende) voorkeur voor een middel bestaat.

Hieronder wordt in onderdeel A – technisch hulpmiddel of handmatig? - antwoord gegeven op deze vraag.

B.

Artikel 126nba lid 8 Sv bepaalt, voor zover relevant:

> Bij of krachtens algemene maatregel van bestuur worden regels gesteld omtrent:
>
> a. [...]
> b. de geautomatiseerde vastlegging van gegevens over de uitvoering van het bevel

Deze algemene maatregel van bestuur is ingevoerd als het Besluit onderzoek in een geautomatiseerd werk. Dit Besluit geeft onder andere de definitie van een technisch hulpmiddel en stelt bepaalde voorwaarden aan het gebruik van een technisch hulpmiddel. Deze keuringseisen, of indien er niet (vooraf) gekeurd kan worden waarborgen, worden hieronder in onderdeel B – inzet technisch hulpmiddel – verder uitgewerkt.

A. Technisch hulpmiddel of handmatig?

1. Technisch hulpmiddel

Artikel 126nba lid 8 sub b Sv bepaalt:

> Bij of krachtens algemene maatregel van bestuur worden regels gesteld omtrent:
> a. [...]
> b. de geautomatiseerde vastlegging van gegevens over de uitvoering van het bevel, bedoeld in het eerste lid.

Deze algemene maatregel van bestuur is ingevoerd als het Besluit onderzoek in een geautomatiseerd werk.

In **artikel 1 sub f Besluit** wordt een definitie gegeven van een technisch hulpmiddel:

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

Hieronder wordt de interpretatie van deze definitie nader onderzocht.

a. Detectie, registratie en transport

Wat moet worden verstaan onder detectie en registratie vermelden het Besluit en de Nota van Toelichting daarop niet.

In het Keuringsprotocol CCIII wordt *detectie* gedefinieerd als:

> het vinden van gegevens waar naar gezocht wordt.

Onder *registratie* wordt in het Keuringsprotocol CCIII verstaan:

> het maken van een kopie van gedetecteerde gegevens om deze later te kunnen vastleggen in een technische infrastructuur.

Uit het Besluit en de Nota van Toelichting valt wel op te maken wat er moet worden verstaan onder *transport*.

In **artikel 13 (transport)** wordt bepaald:

1. Een technisch hulpmiddel transporteert de geregistreerde gegevens automatisch naar een technische infrastructuur.
2. Een technisch hulpmiddel beveiligt de geregistreerde gegevens tijdens het transport naar een technische infrastructuur tegen wijziging van de geregistreerde gegevens en kennisneming van de geregistreerde gegevens door onbevoegden.

Artikel 26 lid 1 Besluit bepaalt:

1. Indien een technisch hulpmiddel niet of niet volledig kan worden verwijderd uit een geautomatiseerd werk, beëindigt de met verwijdering belaste opsporingsambtenaar het

transport van de door het technische hulpmiddel geregistreerde gegevens naar de technische infrastructuur.

In paragraaf 3.5 van de Nota van Toelichting op het Besluit wordt het volgende toegelicht op het transport:

> Het transport van de geregistreerde gegevens vindt plaats naar een technische infrastructuur, een opslaglocatie in beheer van de politie, waarop de gegevens worden vastgelegd.

In de artikelsgewijze toelichting, onder artikelen 10, 11 en 12 wordt opgemerkt:

> Een technisch hulpmiddel detecteert gegevens in het geautomatiseerde werk, registreert de gedetecteerde gegevens en transporteert de gegevens naar de technische infrastructuur van het technisch team.

Onder artikel 13 wordt opgemerkt:

> Op grond van artikel 13, eerste lid, van het besluit dient een technisch hulpmiddel zodanig te zijn ingericht dat geregistreerde gegevens automatisch worden getransporteerd naar een technische infrastructuur, die in beheer is bij een technisch team. Deze eis wordt gesteld om onbevoegde toegang van derden tot de met een technisch hulpmiddel geregistreerde gegevens te voorkomen. De keuring van een technisch hulpmiddel strekt zich uit tot het transport naar de opslaglocatie. De technische infrastructuur waarop de vastlegging van met een technisch hulpmiddel geregistreerde gegevens plaatsvindt wordt niet gekeurd.

Kortom, onder transport kan worden verstaan:

> het automatische transport van geregistreerde gegevens naar een technische infrastructuur van het technisch team.

Het Keuringsprotocol CCIII hanteert (overigens) de volgende definitie:

> het transport van geregistreerde gegevens vanaf de locatie waar registratie plaatsvindt tot aan een technische infrastructuur.

b. Technische infrastructuur

Ten behoeve van een volledige definitie dient nader te worden bekeken wat wordt bedoeld met "een technische infrastructuur".

Artikel 1 lid sub g bepaalt:

> g. *technische infrastructuur:* technische voorziening van een technisch team bedoeld voor de vastlegging van gegevens ter uitvoering van een bevel;

De vraag hierbij rijst wat moet worden verstaan onder een technische voorziening. Kan dit bijvoorbeeld ook de computer / laptop / NAS zijn van de aangewezen opsporingsambtenaar die de onderzoekshandelingen verricht?

Ter verduidelijking van deze definitie kan allereerst worden opgemerkt dat er (kennelijk) meerdere technische voorzieningen bij het technisch team in gebruik kunnen zijn.

Op pagina 14 van de Nota van Toelichting wordt (namelijk) opgemerkt dat gelet op de bijzondere expertise en de technische *voorzieningen* die nodig zijn voor het uitvoeren van onderzoek in een geautomatiseerd werk, in iedergeval gedurende de beginfase, de organisatie van de technische teams centraal wordt belegd bij de politieorganisatie.

Op pagina 33 wordt de definitie van technische infrastructuur nader toegelicht:

> Uit deze definitie, in combinatie met de definitie van 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 integriteit van het verkregen bewijsmateriaal te borgen en onbevoegde wijziging of kennisneming hiervan te voorkomen.

Op pagina 47 wordt eveneens de technische infrastructuur verduidelijkt:

> Dit betreft een technische voorziening van een technisch team, die is bedoeld voor de vastlegging van de tijdens het verrichten van onderzoekshandelingen geregistreerde gegevens. De technische infrastructuur moet in staat zijn om het unieke gegeven dat door het technisch hulpmiddel aan de geregistreerde gegevens is toegevoegd te herkennen. Zo kan de herkomst van de vastgelegde gegevens worden vastgesteld.

In het Besluit en de Nota van Toelichting daarop komt de term "technische infrastructuur" in totaal 62 keer voor. Hieronder volgen de relevante passages, in aanvulling op de passages die hierboven reeds zijn geciteerd.

Artikel 5 (logbestanden)

1. Gedurende de uitvoering van een bevel worden doorlopend en automatisch gegevens in logbestanden vastgelegd over:
   a. [...]
   b. [...]
   c. de gegevens die al dan niet met een technisch hulpmiddel op de technische infrastructuur worden vastgelegd ter uitvoering van een bevel.

Artikel 27 (vastlegging van gegevens op een technische infrastructuur)

1. De vastlegging van de tijdens het onderzoek al dan niet door een technisch hulpmiddel geregistreerde gegevens vindt plaats op een technische infrastructuur.
2. Een technische infrastructuur is zodanig ingericht dat bij de vastlegging van gegevens het door een technisch hulpmiddel geregistreerde unieke gegeven wordt herkend.
3. Een technische infrastructuur is zodanig ingericht dat bij de vastlegging van gegevens de datum en tijd van de vastlegging worden geregistreerd.

Artikel 28 (betrouwbaarheid en integriteit van een technische infrastructuur)

1. De inhoud van de op een technische infrastructuur vastgelegde gegevens wordt niet gewijzigd.
2. De vastgelegde gegevens zijn uitsluitend toegankelijk voor door de korpschef aangewezen ambtenaren.

Pagina 17:

Ook het functioneren van de technische infrastructuur wordt gelogd.

Pagina 21:

De technische infrastructuur is beveiligd tegen wijziging van de vastgelegde gegevens en kennisneming hiervan door onbevoegden.

[...]

Ook als onderzoekshandelingen zonder goedgekeurd hulpmiddel worden verricht, dienen de verkregen gegevens te worden vastgelegd op een technische infrastructuur.

Kortom, onder technische infrastructuur lijkt te moeten worden verstaan een specifieke omgeving binnen de politieorganisatie waar een aantal eisen aan worden gesteld. Zo moet de technische infrastructuur in staat zijn om kenmerken te herkennen, moet er bij vastlegging van gegevens datum en tijd worden geregistreerd, is de infrastructuur beveiligd, zijn de vastgelegde gegevens uitsluitend toegankelijk voor aangewezen opsporingsambtenaren en wordt het functioneren van de technische infrastructuur gelogd.

Het door een opsporingsambtenaar belast met de uitvoering van de onderzoekshandelingen gebruikte component (computer, laptop, NAS, etc) lijkt derhalve niet te kunnen worden gelijkgesteld met de technische infrastructuur in de zin van artikel 1 sub g Besluit.

Dit kan overigens ook worden afgeleid uit het Keuringsprotocol CCIII waarin het voorbeeld wordt gegeven van cloud-extractie (een voorbeeld dat overigens ook wordt genoemd in het Besluit, op pagina 39). In dat geval vindt er met behulp van een technisch hulpmiddel in een lokaal component registratie en detectie plaats waarna er transport plaatsvindt naar de technische infrastructuur waar de gegevens worden vastgelegd.

c. *Conclusie definitie technisch hulpmiddel*

Samenvattend kan de volgende allesomvattende definitie worden gehanteerd voor een technisch hulpmiddel.

Een technisch hulpmiddel is een softwareapplicatie waarmee onderzoekshandelingen worden verricht ter uitvoering van een bevel die gegevens detecteert, registreert en automatisch transporteert naar een technische infrastructuur van het technisch team.

2. "Al dan niet": handmatig onderzoek

Zoals aangegeven geeft artikel 126nba Sv de mogelijkheid om onderzoekshandelingen 'al dan niet' met een technisch hulpmiddel te verrichten. Naast de categorie technisch

hulpmiddel is er dus nog een tweede categorie.

In de Memorie van Toelichting wordt deze tweede categorie beperkt tot handmatig onderzoek:

> [...] onderzoekshandelingen kunnen handmatig dan wel met behulp van een technisch hulpmiddel worden verricht, in de vorm van een softwareapplicatie.

Dit doet de vraag rijzen wanneer onderzoekshandelingen kunnen worden aangemerkt als handmatig. In de Memorie van Toelichting wordt hier niet verder over uitgeweid. Ook in de overige kamerstukken wordt verder niet gesproken over handmatig onderzoek. Behalve in de Nota van Toelichting op het Besluit waarin de term tweemaal in dit verband voorkomt.

Pagina 16:

> Het gebruik van een technisch hulpmiddel is echter niet strikt noodzakelijk: onderzoekshandelingen kunnen ook ad hoc en handmatig worden verricht.

Pagina 21:

> In bepaalde gevallen kunnen onderzoekshandelingen beter handmatig worden verricht, zodat het gebruik van een technisch hulpmiddel achterwege kan blijven. Hierbij 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 een geautomatiseerd werk. 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.

Uit bovenstaande passage kan worden afgeleid dat handmatig niet noodzakelijkerwijs met zich hoeft te brengen dat de gegevens door de opsporingsambtenaar visueel op het scherm 'gedetecteerd' worden. Er kan volgens het gegeven voorbeeld immers worden gedacht aan direct inzien *of* (direct) overnemen. Vanwege dit alternatieve karakter, kan worden geconcludeerd dat er bij overnemen niet (enkel) hoeft te worden gedacht aan iets op een geautomatiseerd werk zien en dat vervolgens overtypen. Dat zou zijn inzien *en* (vervolgens) overnemen. Vanwege de technische / digitale aard van het onderzoek en deze voorbeelden, kan er bij handmatig ook worden gedacht aan een technische handeling waarbij er op dat moment (nog) geen sprake is van visuele detectie.

Wel lijkt het begrip handmatig en het gegeven voorbeeld de situatie op te roepen waarin niet sprake is van een afstandelijk, geautomatiseerd proces over een langere periode, maar van een directe uitvoering door de opsporingsambtenaar die het onderzoek uitvoert, met direct resultaat, directe vastlegging van de gegevens, waarbij onregelmatigheden ook direct kunnen worden geconstateerd.

De ruimte voor technisch handelen doet in het licht van de definitie van een technisch hulpmiddel de denkrichting ontstaan dat het handmatig handelen zich zou kunnen beperken tot één (of twee) van de drie criteria van een technisch hulpmiddel; detectie, registratie en/of transport.

Ter illustratie:

Voorbeeld 1
Stel DIGIT is een mailbox van een verdachte binnengedrongen. Vervolgens kan DIGIT handmatig mailtjes van een bepaalde afzender (visueel) detecteren. Het registreren en transport vindt vervolgens automatisch plaats.

Vanwege de handmatige detectie is er geen sprake van een technisch hulpmiddel. Vanwege de directe betrokkenheid door de handmatige detectie kan er wel worden gesproken van handmatig onderzoek in de zin van artikel 126nba Sv lid 1 Sv.

Voorbeeld 2
DIGIT kan in een grote database met behulp van een technische voorziening (analysetool) de juiste gegevens detecteren. En wellicht ook registreren. Echter, het transport naar de technische infrastructuur (safe store) van DIGIT dient zelf, handmatig, te worden uitgevoerd.

Nu de technische voorziening (tool) enkel detecteert en registreert kan er gezien de definitie uit artikel 1 sub f Besluit niet worden gesproken van een technisch hulpmiddel. Vanwege de directe betrokkenheid bij het handmatige transport kan er wel worden gesproken van handmatig onderzoek in de zin van artikel 126nba Sv lid 1 Sv.

Voorbeeld 3
DIGIT gebruikt een software applicatie die automatisch gegevens detecteert en registreert en een script die automatisch de geregistreerde gegevens transporteert naar de technische infrastructuur.

Er wordt niet handmatig gehandeld, er is geen sprake van directe betrokkenheid. Hier kan niet worden gesproken van handmatig onderzoek in de zin van artikel 126nba Sv. De applicatie en het script moeten dusdanig worden samengesteld om te functioneren als één applicatie en als technisch hulpmiddel in de zin van artikel 1 sub f Besluit.

Uiteraard geldt dat waar een van de fases technisch wordt uitgevoerd (zoveel mogelijk) voldaan zal moeten worden aan de keuringseisen uit het Besluit die gelden voor die specifieke fases. Of, waar niet mogelijk, aanvullende/procedurele waarborgen zullen moeten worden gesteld.

Samenvattend, lijkt de volgende definitie van handmatig mogelijk.

> **Handmatig onderzoek is onderzoek verricht door de volgens het Besluit aangewezen opsporingsambtenaar waarbij één of meerdere van de fases – registratie, detectie en/of transport - zonder gebruik van een technische tool, met directe betrokkenheid van eerstgenoemde opsporingsambtenaar wordt uitgevoerd.**

3. De keuze: technisch hulpmiddel of handmatig onderzoek

Hoofdregel is dat bij de uitvoering van een bevel gebruik wordt gemaakt van een vooraf

goedgekeurd technisch hulpmiddel. [1]

De wetgever biedt ruimte om van dit uitgangspunt af te wijken. Zoals hierboven reeds werd vermeld is handmatig onderzoek in sommige gevallen (zelfs) de betere optie.

Pagina 21:

> In bepaalde gevallen kunnen onderzoekshandelingen beter handmatig worden verricht, zodat het gebruik van een technisch hulpmiddel achterwege kan blijven.

Er moet dan uiteraard wel in de eerste plaats worden bekeken of handmatig onderzoek technisch mogelijk is. Is het mogelijk om voldoende directe betrokkenheid van de uitvoerende opsporingsambtenaar te realiseren?

Zo ja, dan moet worden bekeken of niet toch de inzet van een technisch hulpmiddel is vereist. Hierbij dient onder meer te worden gekeken naar:

a. de aard van de inzet;
b. de aard van het geautomatiseerde werk; en
c. de vraag of de gegevens zonder gebruik van een technisch hulpmiddel als rechtmatig bewijs kunnen worden aangemerkt.

Wat wordt bedoeld met die laatste factor is onduidelijk. Naast het gebruik van een technisch hulpmiddel geeft artikel 126nba Sv een andere manier van het verrichten van onderzoekshandelingen, die – indien wordt voldaan de voorwaarden – evenzeer rechtmatig is. Wellicht dat hier de betrouwbaarheid van het bewijs wordt bedoeld.

Ten aanzien van (onder meer) de betrouwbaarheid van vast te leggen gegevens is in het Besluit (art. 21 lid 5) bepaald dat wanneer onderzoekshandelingen in een geautomatiseerd werk handmatig worden uitgevoerd, de onderzoekshandelingen worden verricht die zijn omschreven in het bevel en er procedurele waarborgen worden getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de tijdens het onderzoek vast te leggen gegevens te garanderen.

Indien er onvoldoende directe betrokkenheid van de uitvoerend opsporingsambtenaar kan worden gerealiseerd en/of (ook) (de genoemde) factoren zich verzetten tegen het passeren van het gebruik van een technisch hulpmiddel, dient een technisch hulpmiddel te worden ingezet.

[1] Nota van toelichting p. 44.

B. Inzet technisch hulpmiddel

Op grond van het Besluit zijn er ten aanzien van de inzet van een technisch hulpmiddel drie opties:

1. de regel: er wordt gebruik gemaakt van een vooraf goedgekeurd technisch hulpmiddel;
2. de uitzondering I: er wordt gebruik gemaakt van een niet gekeurd technisch hulpmiddel, dat achteraf wordt gekeurd; of
3. de uitzondering II: het technisch hulpmiddel wordt in zijn geheel niet gekeurd.

1. De regel: er wordt gebruik gemaakt van een vooraf goedgekeurd technisch hulpmiddel

In **artikel 14 (voorafgaande keuring en herkeuring)** wordt bepaald

> 1. Een technisch hulpmiddel wordt voorafgaand aan het gebruik ervan gekeurd door een keuringsdienst.

In **artikel 21 (uitvoering van een bevel)** wordt bepaald

> 1. Indien de officier van justitie beveelt dat het verrichten van onderzoekshandelingen in een geautomatiseerd werk plaatsvindt met een technisch hulpmiddel wordt ter uitvoering van het bevel gebruik gemaakt van een goedgekeurd technisch hulpmiddel.

In de toelichting op het Besluit wordt de hoofdregel nogmaals benoemd: Ter uitvoering van een bevel van de officier van justitie wordt in beginsel steeds gebruik gemaakt van een vooraf goedgekeurd technisch hulpmiddel[2]. (pag 21)

Bij de keuring wordt getoetst of het hulpmiddel voldoet aan de in hoofdstuk 5 gestelde technische eisen. (pag. 19)

Het is mogelijk om te voldoen aan een of meer in het besluit gestelde technische eisen via vervangende procedurele waarborgen (artikel 18 derde lid, onderdeel e). De huidige keuringspraktijk heeft uitgewezen dat hieraan behoefte bestaat. (pag. 43)

Van de keuring wordt een rapport opgemaakt, waarin de bevindingen van de keuringsdienst worden vastgelegd (artikel 18 tweede lid).

Als bij het verrichten van onderzoekshandelingen gebruik wordt gemaakt van een goedgekeurd hulpmiddel mag er vanuit worden gegaan dat aan de wettelijke eisen omtrent de betrouwbaarheid, integriteit en herleidbaarheid van de gegevens is voldaan. (pag. 19)

[2] Onder goedgekeurd technisch hulpmiddel wordt een technisch hulpmiddel verstaan dat voldoet aan de eisen van artikelen 8-13 van het Besluit en waartoe door de Keuringdienst overeenkomstig artikel 18 lid 3 van het Besluit een keuringsrapport is opgemaakt.

2. De uitzondering I: er wordt gebruik gemaakt van een niet gekeurd technisch hulpmiddel, dat achteraf wordt gekeurd

In **artikel 15 (uitzonderingen op voorafgaande keuring en herkeuring)** wordt bepaald

> 1. In afwijking van artikel 14, eerste en derde lid, kan een technisch hulpmiddel na afloop van het gebruik ervan worden gekeurd of kan na afloop van het gebruik herkeuring plaatsvinden indien de officier van justitie dit heeft bepaald overeenkomstig artikel 21, tweede lid.
> 2. In afwijking van het eerste lid kan keuring of herkeuring achteraf achterwege blijven, indien de officier van justitie dit heeft bepaald overeenkomstig artikel 21, vierde lid.

In **artikel 21 (uitvoering van een bevel)** wordt bepaald

> 2. In afwijking van het eerste lid kan de officier van justitie bepalen dat, indien het onderzoeksbelang dit dringend vordert, een niet gekeurd technisch hulpmiddel wordt gebruikt. In dat geval vermeldt de officier van justitie in het bevel dat toepassing is gegeven aan artikel 21, tweede lid.
> 3. 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.

Een uitzondering op deze hoofdregel (dat een niet vooraf goedgekeurd technisch hulpmiddel wordt ingezet[3]) 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. In dat geval vermeldt de officier van justitie in het bevel dat gebruik wordt gemaakt van een niet gekeurd hulpmiddel. Na afloop vindt alsnog keuring plaats, tenzij de aard van het hulpmiddel zich naar het oordeel van de officier hiertegen verzet. (pag 21)

En in toelichting op artikel 21 lid 2: Hierbij kan worden gedacht aan de situatie dat (her)keuring voorafgaand aan de inzet teveel tijd zou vergen. Het moet dan gaan om situaties waarin het belang van het onderzoek de inzet van het desbetreffende technische hulpmiddel dringend vordert. Bij deze afweging zal de officier van justitie in overleg met de keuringsinstantie (in het verslag van een schriftelijk overleg, nr. 29: "de politie") nagaan of het beoogde technische hulpmiddel naar verwachting zal voldoen aan de in de artikel 8 tot en met 13 gestelde technische eisen. (pag. 44)

Dat bewust ruimte is gelaten voor het inzetten van niet vooraf goed gekeurde technische hulpmiddelen, blijkt ook uit de navolgende overweging in het Besluit:

> Het advies van BoF om de uitzonderingen omtrent het gebruik van niet dan wel achteraf goedgekeurde technische hulpmiddelen te beperken is niet overgenomen. Dit zou te belemmerend zijn voor de opsporingspraktijk. (pag. 29)

In de toelichting bij artikel 14 wordt verder opgemerkt dat in de praktijk niet lichtzinnig van het gebruik van een goedgekeurd hulpmiddel zal worden afgezien. Bij deze

[3] Onder een *niet gekeurd technisch hulpmiddel* worden alle technische hulpmiddelen verstaan die niet voorafgaande aan de inzet zijn goedgekeurd door de Keuringsdienst.

afweging zal de officier van justitie in overleg met de keuringsinstantie nagaan of het beoogde technische hulpmiddel naar verwachting zal voldoen aan de in het besluit gestelde technische eisen. (pag. 42)

3. De uitzondering II: het technisch hulpmiddel wordt in zijn geheel niet gekeurd

In **artikel 15 (uitzonderingen op voorafgaande keuring en herkeuring)** wordt bepaald:

> 2. In afwijking van het eerste lid kan keuring of herkeuring achteraf achterwege blijven, indien de officier van justitie dit heeft bepaald overeenkomstig artikel 21, vierde lid.

In **artikel 21 (uitvoering van een bevel)** wordt bepaald:

> 4. In afwijking van het derde lid kan keuring of herkeuring na afloop van het gebruik achterwege blijven, indien de aard van het technische hulpmiddel zich naar het oordeel van de officier van justitie daartegen verzet. In dat geval vermeldt de officier van justitie in de processtukken dat toepassing is gegeven aan artikel 21, vierde lid, en vermeldt hij welke aanvullende waarborgen zijn getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de met het technisch hulpmiddel vastgelegde gegevens te garanderen.

Na afloop vindt alsnog keuring plaats, *tenzij de aard van het hulpmiddel zich naar het oordeel van de officier hiertegen verzet*. In dat geval vermeldt de officier van justitie in de processtukken dat is afgezien van keuring en vermeldt hij welke aanvullende waarborgen zijn getroffen om de betrouwbaarheid, integriteit en de herleidbaarheid van de vastgelegde gegevens te garanderen. (pag. 21)

In uitzonderingsgevallen kan de keuring van een technisch hulpmiddel geheel achterwege blijven, namelijk indien de aard van het technische hulpmiddel zich naar het oordeel van de officier van justitie daartegen verzet (artikel 21, vierde lid). 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 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.

In het advies over het ontwerp-besluit heeft de NP opgemerkt dat het bij de gevallen waarin keuring geheel achterwege blijft naar verwachting om uitzonderlijke gevallen gaat. (pag. 45)

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, vierde en vijfde lid).

Document 44

Toelichting art. 21 lid 4 Bogw
Landelijk Parket - DIGIT

1. Aanleiding

In het onderzoek dat je leidt, is gebruik gemaakt van de bevoegdheid ex artikel 126nba Sv. Daarbij is een niet gekeurd technisch hulpmiddel ingezet. Door de landelijk DIGIT officier is beslist dat de aard van het gebruikte technische hulmiddel zich verzet tegen keuring achteraf. Dat heeft tot gevolg dat op grond van het Besluit onderzoek in een geautomatiseerd werk (verder: Bogw) door de officier van justitie in de processtukken moet worden vermeld welke aanvullende waarborgen zijn getroffen. In deze toelichting staat achtergrond informatie over het kader rond keuring van technisch hulpmiddelen ex art. 126nba Sv.

2. Binnendringen vs. onderzoekshandelingen

In artikel 126nba Sv is de bevoegdheid opgenomen om heimelijk en op afstand binnen te dringen in een geautomatiseerd werk en daar onderzoekshandelingen te verrichten.

Voor de uitvoering van artikel 126nba Sv wordt gebruik gemaakt van ondersteunende middelen waarmee *binnengedrongen* kan worden in geautomatiseerde werken. In dit kader wordt soms gesproken over binnendringsoftware. De binnendringsoftware of andere hulpmiddelen voor het binnen dringen zijn geen onderdeel van het keuringsproces.[1]

Nadat is binnengedrongen worden op grond van artikel 126nba Sv *onderzoekshandelingen* verricht in een geautomatiseerd werk dat in gebruik is bij een verdachte. De *onderzoekshandelingen* die worden benoemd in art. 126nba Sv zijn:

- sub a: het vast stellen van kenmerken van het geautomatiseerde werk of de gebruiker
- sub b: het uitvoeren van een bevel tap of OVC
- sub c: het uitvoeren van een bevel stelselmatige observatie
- sub d: het vastleggen van gegevens die op het geautomatiseerde werk zijn opgeslagen
- sub e: het ontoegankelijk maken van gegevens

Bij het verrichten van onderzoekshandelingen kan gebruik gemaakt worden van een technisch hulpmiddel (TH). In het Bogw worden nadere regels gesteld omtrent het gebruik van een TH en de keuring daarvan.

Kortgezegd: De middelen die worden gebruikt om binnen te dringen, zijn dus niet aan keuring onderworpen. Een TH waarmee onderzoekhandelingen worden verricht, moet in beginsel wel worden gekeurd.

3. Besluit onderzoek in een geautomatiseerd werk (Bogw)

Bij de uitvoering van art. 126nba lid 1 Sv kan dus gebruik worden gemaakt van een TH. Deze mogelijkheid is nader uitgewerkt in het Besluit onderzoek in een geautomatiseerd werk (Bogw).[2] In het Bogw wordt een TH omschreven als "softwareapplicatie die gegevens detecteert, registreert en transporteert en waarmee onderzoekshandelingen worden verricht ter uitvoering van een bevel".[3]

Het in het Bogw geformuleerde uitgangspunt voor het gebruik van TH's is dat wordt gewerkt met een vooraf goedgekeurd TH (art. 14 en 21 lid 1 Bogw).

---

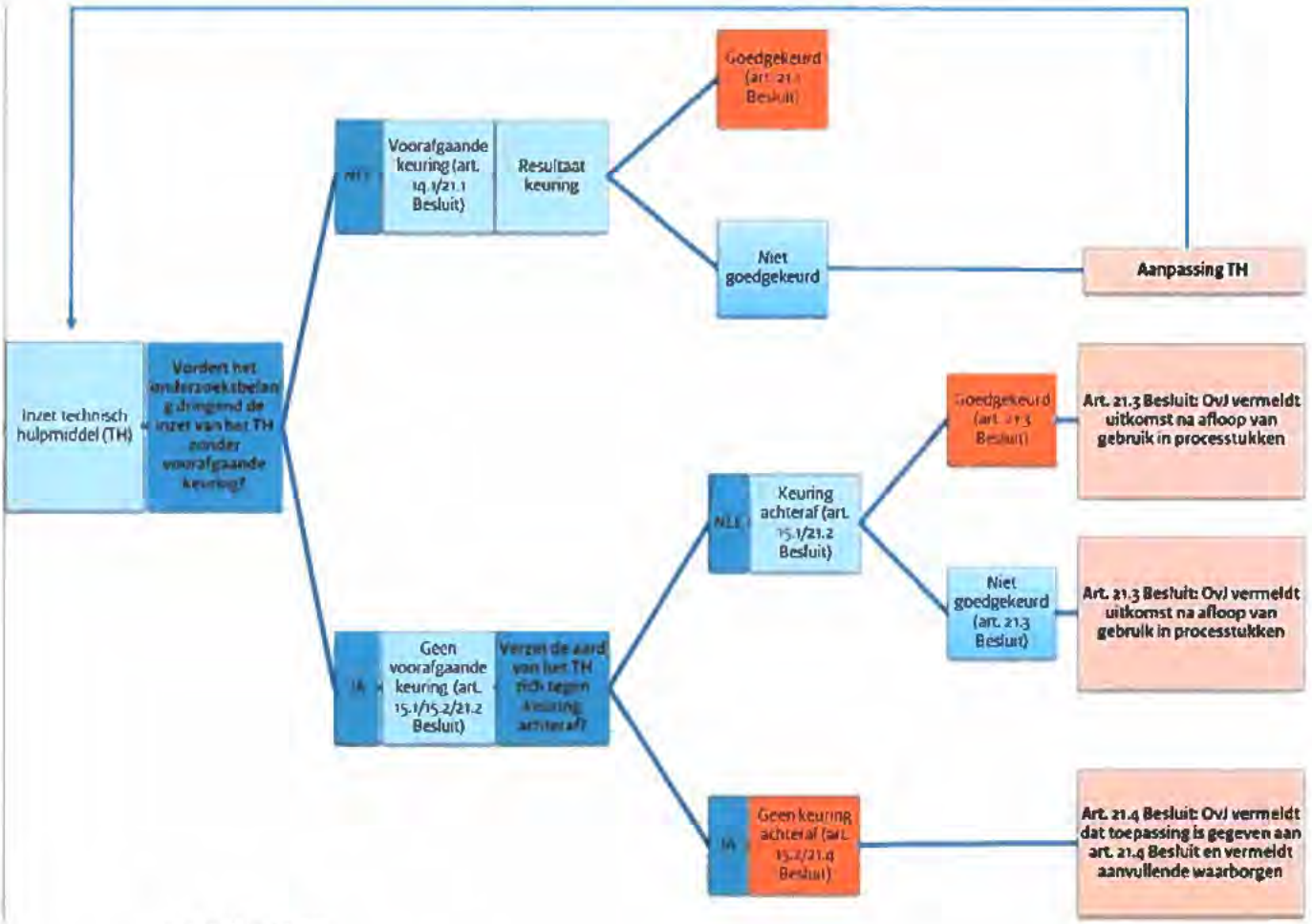
[1] Bogw, p. 20.
[2] Besluit onderzoek in een geautomatiseerd werk, *Stb.* 2018, 340.
[3] Artikel 1 sub f Bogw.

Indien het onderzoek het dringend vordert, kan de OvJ bepalen dat gewerkt wordt met een niet gekeurd TH (art. 21 lid 2 Bogw). Die beslissing wordt ook opgenomen in het bevel. Het niet gekeurde TH wordt na afloop van de inzet alsnog gekeurd. De resultaten daarvan worden aan het procesdossier toegevoegd (art. 21 lid 3 Bogw).

De OvJ kan echter ook bevelen dat een ingezet TH, dat vooraf niet gekeurd is, überhaupt niet wordt gekeurd. Dit kan indien "de aard" van het TH zich, naar het oordeel van de OvJ, tegen keuring verzet (art. 21 lid 4 Bogw). In de toelichting op het Bogw is hierover het volgende opgemerkt:

> "In uitzonderingsgevallen kan de keuring van een technisch hulpmiddel geheel achterwege blijven, namelijk indien de aard van het technische hulpmiddel zich naar het oordeel van de officier van justitie daartegen verzet (artikel 21, vierde lid). 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 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."[4]

4. Stroomschema art. 21 Bogw



7 oktober 2020

LP Digit – [redacted]

[4] Bogw, p. 45.

Document 45

Handelingskader inzet technisch hulpmiddel en handmatige uitvoering van onderzoekshandelingen ex art. 126nba Sv

Landelijk Parket - DIGIT

Inleiding

Artikel 126nba lid 1 Sv bepaalt, voor zover relevant:

> *[de officier van justitie kan] bevelen dat een daartoe aangewezen opsporingsambtenaar binnendringt in een geautomatiseerd werk dat bij de verdachte in gebruik is en, **al dan niet met een technisch hulpmiddel**, onderzoek doet [...]*

In artikel 1 sub f Besluit onderzoek in een geautomatiseerd werk (Bogw)[1] wordt een definitie gegeven van een technisch hulpmiddel:

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

Het begrip 'technisch hulpmiddel' laat zich niet eenduidig afbakenen ten opzichte van het 'handmatig' verrichten van onderzoekshandelingen in een geautomatiseerd werk.[2] In dit stuk zijn daarom de handelingskaders geschetst die DIGIT LP heeft gesteld aan DIGIT LE bij het verricht van onderzoekshandelingen "al dan niet" met gebruik van een technisch hulpmiddel.

Onderzoekshandelingen met een technisch hulpmiddel of handmatig?

De vraag rijst wat moet worden verstaan onder een technisch hulpmiddel en wat dan valt onder "al dan niet"; de andere categorie van middelen waarmee onderzoek kan worden gedaan. En of er een bepaalde (dwingende) voorkeur voor een middel bestaat?

Hoofdregel is dat bij de uitvoering van een bevel gebruik wordt gemaakt van een (vooraf goedgekeurd) technisch hulpmiddel.[3] De wetgever biedt ruimte om van het uitgangspunt dat bij de uitvoering van een bevel gebruik wordt gemaakt van een technisch hulpmiddel af te wijken:

> *Het gebruik van een technisch hulpmiddel is echter niet strikt noodzakelijk: onderzoekshandelingen kunnen ook ad hoc en handmatig worden verricht.*[4]

Sterker, door de wetgever is nadrukkelijk aangegeven dat handmatig onderzoek in sommige gevallen (zelfs) de betere optie is:

> *In bepaalde gevallen kunnen onderzoekshandelingen beter handmatig worden verricht, zodat het gebruik van een technisch hulpmiddel achterwege kan blijven. Hierbij kan worden gedacht aan de*

---

[1] Besluit onderzoek in een geautomatiseerd werk, Stb. 2018, 340.
[2] Vgl. Nota van toelichting (NvT), p. 21.
[3] NvT p. 44.
[4] NvT, p. 16.

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. De vraag of het gebruik van een technische 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.[5]

De vraag of het gebruik van een technisch hulpmiddel noodzakelijk is, wordt volgens de nota van toelichting dus onder meer afhankelijk gesteld van verschillende aspecten die ruimte bieden voor een operationele, technische en/of juridische afweging per geval.

Invulling definitie technisch hulpmiddel

Een *technisch hulpmiddel* is een softwareapplicatie waarmee onderzoekshandelingen worden verricht ter uitvoering van een bevel die gegevens detecteert, registreert en transporteert naar een technische infrastructuur van het technisch team. 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.[6]

Bij de invulling van de definitie van een technisch hulpmiddel wordt uitgegaan van het volgende:

Bij de inzet van een technisch hulpmiddel is er sprake van een zelfstandig functionerend middel dat buiten de invloedssfeer van de uitvoerder de drie componenten (detectie, registratie en transport) uitvoert waarmee onderzoekshandelingen ter uitvoering van een bevel worden verricht. Er kan sprake zijn van één softwareapplicatie, maar ook van meerdere softwareapplicaties die in samenhang worden ingezet en die tezamen de drie componenten uit de definitie van een technisch hulpmiddel uitvoeren.[7]

"Al dan niet": handmatig onderzoek

Zoals aangegeven geeft artikel 126nba Sv de mogelijkheid om onderzoekshandelingen 'al dan niet' met een technisch hulpmiddel te verrichten. Naast de categorie technisch hulpmiddel is er dus nog een tweede categorie.

In de Memorie van Toelichting wordt deze tweede categorie beperkt tot handmatig onderzoek:

[...] onderzoekshandelingen kunnen handmatig dan wel met behulp van een technisch hulpmiddel worden verricht, in de vorm van een softwareapplicatie.

Dit doet de vraag rijzen wanneer onderzoekshandelingen kunnen worden aangemerkt als handmatig. In de Memorie van Toelichting wordt hier niet verder over uitgeweid. Ook in de overige kamerstukken wordt verder niet gesproken over handmatig onderzoek. Behalve in de Nota van Toelichting op het Bogw waarin de term tweemaal in dit verband voorkomt.

---

[5] NvT, p. 21.
[6] NvT, p. 20.
[7] Dit sluit niet uit dat binnen de genoemde componenten van het technisch hulpmiddel onderdelen samenvallen of moeilijk te onderscheiden zijn. Bv. binnen de architectuur van een TH zijn detectie en registratie niet los van elkaar aanwijsbaar bij een TH dat geautomatiseerd e-mail gegevens vanuit een mail-account in de cloud downloadt en registreert. Er is dan (ook) sprake van een technisch hulpmiddel.

Pagina 16:

> *Het gebruik van een technisch hulpmiddel is echter niet strikt noodzakelijk: onderzoekshandelingen kunnen ook ad hoc en handmatig worden verricht.*

Pagina 21:

> *In bepaalde gevallen kunnen onderzoekshandelingen beter handmatig worden verricht, zodat het gebruik van een technisch hulpmiddel achterwege kan blijven. Hierbij 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 een geautomatiseerd werk. 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.*

Uit bovenstaande passage kan worden afgeleid dat handmatig niet noodzakelijkerwijs met zich hoeft te brengen dat de gegevens door de opsporingsambtenaar direct visueel op het scherm 'gedetecteerd' worden. Er kan volgens het gegeven voorbeeld immers worden gedacht aan direct inzien of (direct) overnemen. Vanwege dit alternatieve karakter, kan worden geconcludeerd dat er bij overnemen niet (enkel) hoeft te worden gedacht aan iets op een geautomatiseerd werk zien en dat vervolgens overtypen. Dat zou zijn inzien *en* (vervolgens) overnemen. Vanwege de technische / digitale aard van het onderzoek en deze voorbeelden, kan er bij handmatig ook worden gedacht aan een technische handeling waarbij er op dat moment (nog) geen sprake is van visuele detectie. Wel lijkt het begrip handmatig en het gegeven voorbeeld de situatie op te roepen waarin niet sprake is van een afstandelijk, proces over een langere periode, maar van een noodzakelijke uitvoering door de opsporingsambtenaar die het onderzoek uitvoert, met een directe noodzakelijke reactie vanuit het geautomatiseerd werk waarbij bv. onregelmatigheden door de uitvoerder kunnen worden geconstateerd of er een beslismoment is zoals welk bestand veilig moet worden gesteld. Voor de uitvoering kan het noodzakelijk zijn om ook bij de handmatige uitvoering een of meer delen van het proces met behulp van (een) softwareapplicatie(s) uit te voeren.

Bij de handmatige uitvoering wordt er daarom vanuit gegaan dat dit de uitvoering betreft waarbij op een of meerdere componenten (detectie, registratie en/of transport) een noodzakelijke betrokkenheid wordt vereist van de uitvoerder.

2 september 2020

28 juni 2021 (aangevuld)

LP DIGIT

	Toegezonden	Afgerond
LP DIGIT	09-04-2020	28-06-2021
Afgestemd LE DIGIT	09-04-2020	28-06-2021
Afgestemd rechercheovj LP	29-05-2020	21-08-2020