Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

34 372 Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III)

Nr. 31 **BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 7 december 2023

In deze brief wordt een beleidsreactie gegeven op de wetsevaluatie die is uitgevoerd door het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) van de bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk, zoals opgenomen in de Wet computercriminaliteit III (Wet CCIII). Deze wet is in maart 2019 in werking is getreden.[1] Deze reactie wordt gecombineerd met de reactie op de Eindrapportage onderzoek in een geautomatiseerd werk van de procureur-generaal bij de Hoge Raad der Nederlanden (PGHR).[2] Bij deze reactie is rekening gehouden met de verslagen van de Inspectie Justitie en Veiligheid (IJenV). Op 31 augustus 2023 is het «Verslag toezicht wettelijke hackbevoegdheid politie 2022» van de IJenV naar uw Kamer toegezonden met daarbij het WODC rapport «de hackbevoegdheid in het buitenland».[3] Waar toepasselijk zijn ook deze stukken in deze reactie meegenomen.

De binnendringbevoegdheid in de praktijk

Hieronder worden enkele resultaten en karakteristieken van de binnendringbevoegdheid geschetst die ten grondslag liggen aan de aanpassingen die in deze beleidsreactie worden voorgesteld.

Resultaten

De binnendringbevoegdheid heeft in relatief korte tijd haar meerwaarde in de digitale opsporing bewezen. De binnendringbevoegdheid is bijvoorbeeld een steeds belangrijker instrument in de strijd tegen de georganiseerde criminaliteit. Door het WODC zijn ten behoeve van de wetsevaluatie in 2019–2021 25 inzetten onderzocht waarin een bevel is gegeven voor de binnendringbevoegdheid. Op basis van de uitsplitsing die wordt

[1] *Stb.* 2018, nr. 322.
[2] *Kamerstukken II 2022/23,* 29 279, nr. 744.
[3] *Kamerstukken II 2022/23, 29 628 en 34 372, nr. 1187*

kst-34372-31
ISSN 0921 - 7371
's-Gravenhage 2023

gegeven naar het type misdrijven waren 22 van deze inzetten gericht tegen ondermijnende of aan ondermijning gerelateerde criminaliteit.[4] Andere inzetten zagen op terrorisme, seksueel kindermisbruik en computervredebreuk.

In juni 2021 hebben de politie en het Openbaar Ministerie (OM) de communicatie tussen criminelen een belangrijke slag toegebracht. DoubleVPN is toen uit de lucht gehaald. Dit bedrijf leverde Virtual Private Networkdiensten (VPN). Dit zijn beveiligde en afgeschermde internetverbindingen. DoubleVPN richtte zich daarbij in hoofdzaak op cybercriminelen aan wie ze een veilige haven boden om hun slachtoffers aan te vallen.

Ook in het onderzoek naar cryptocommunicatiedienst Exclu is de binnendringbevoegdheid ingezet. Daarnaast heeft de Nederlandse politie bijgedragen aan andere internationale onderzoeken, waaronder het ontmantelen van Encrochat. Bij dit onderzoek heeft de Nederlandse politie niet zelf binnengedrongen, maar was de bijdrage in Nederland juridisch mogelijk doordat de binnendringbevoegdheid in het Wetboek van Strafvordering stond. In het onderzoek naar Encrochat zijn internationaal, na het lezen van 115 miljoen berichten, 6.500 verdachten opgepakt, en zijn 100.000 kilo cocaïne, 30 miljoen pillen en 900 miljoen euro aan crimineel vermogen in beslag genomen.

Een ander goed resultaat is dat een crimineel netwerk dat een online chatplatform en verschillende websites voor online seksueel kindermisbruik in stand hield is gefrustreerd door de aanhouding van een persoon met een vooraanstaande functie binnen dat netwerk.[5] Ook in de strijd tegen cybercriminaliteit is een succes geboekt met het uit de lucht halen van servers achter de agressieve malware Emotet. Emotet vervulde een sleutelrol binnen het cybercriminele landschap. De schatting van de schade veroorzaakt door Emotet loopt wereldwijd in de honderden miljoenen euro's. De Emotet-besmetting is niet langer actief op de computers van ruim 1 miljoen slachtoffers wereldwijd.

Daarbovenop is een van de grootste online mixers voor cryptovaluta offline gehaald. Het gaat om Bestmixer.io. Met deze actie werd het verhullen van criminele geldstromen via het mixen van cryptovaluta zoals bitcoins ernstig verstoord.

Deze uitzonderlijke resultaten bewijzen in wat voor soort zaken de binnendringbevoegdheid een verschil kan maken en welke meerwaarde het kan hebben voor de opsporing. Uit de rapporten blijkt echter dat de uitvoering vaak lastig is, onder meer omdat de wet- en regelgeving rond de bevoegdheid onvoldoende aansluit op de praktijk en de karakteristieke eigenschappen van de bevoegdheid. De wetsevaluatie van het WODC, de eindrapportage van de PGHR en de jaarverslagen van de IJenV bieden bruikbare handvatten voor verbetering. Met enkele aanpassingen kan de bevoegdheid effectiever worden uitgevoerd en meer toegevoegde waarde hebben bij de opsporing van ernstige en georganiseerde criminaliteit.

Karakteristieke eigenschappen

Binnendringen in een geautomatiseerd werk kan lastig zijn en maatwerk vereisen, de politie moet kunnen anticiperen en wendbaar zijn. Er kan meestal niet eenvoudig door middel van een kwetsbaarheid of binnendringsoftware gestandaardiseerd toegang worden verkregen. Het is

[4] WODC (2022) de Hackbevoegdheid in de praktijk, p. 86
[5] Volkskrant, 22 september 2023, *Politie op het spoor van kinderporno door nieuwe hackmethode*

bijvoorbeeld de vraag of de betrokkene daadwerkelijk gebruik blijkt te maken van een kwetsbare versie van hardware, software of dienstverlening. Meestal moet een inzet worden aangepast of uitgevoerd met diverse middelen, of moeten deze nieuw ontwikkeld worden. Soms blijkt de politie de werkwijze te moeten aanpassen wanneer al is binnengedrongen omdat de exacte samenstelling van een geautomatiseerd werk in de regel vooraf onbekend is. Vervolgens is ook het behouden van toegang geen zekerheid, bijvoorbeeld omdat de gebruiker de versie van de software update of omdat de heimelijkheid van de inzet verloren gaat.

Daarnaast is er vooral bij het binnendringen op smartphones sprake van een zekere afhankelijkheid van producten die worden aangeschaft bij externe leveranciers. Dit komt met name door de capaciteit die ontwikkelaars van smartphones inzetten op de constante innovatie van beveiliging en de vele elkaar opvolgende updates. Binnendringen is om bovenstaande redenen in het algemeen tijdrovend en kan erg arbeidsintensief zijn. Dat komt in de rapporten duidelijk naar voren. Bovendien kan de vereiste expertise schaars zijn op de arbeidsmarkt.

Er gelden strikte voorwaarden in het Wetboek van Strafvordering voor de inzet van de binnendringbevoegdheid. Ook kent de uitvoering van deze bevoegdheid een uitvoerig traject van toetsing om te bepalen of de binnendringbevoegdheid het aangewezen opsporingsmiddel is in een specifieke zaak. Uiteindelijk is hiervoor een machtiging van de rechter-commissaris noodzakelijk. Zorgvuldigheid en afbakening zijn nodig aangezien digitale opsporing plaatsvindt in een tijd waarin gegevensopslag op een geautomatiseerd werk, zoals een telefoon of een laptop, in de regel omvangrijk is. Daardoor kunnen de politie en OM via een geautomatiseerd werk een ingrijpend beeld krijgen van het privéleven van een individu.

De binnendringbevoegdheid heeft mooie resultaten opgeleverd, maar deze eigenschappen maken de binnendringbevoegdheid (ook na de aanpassingen zoals voorgesteld in deze brief) geen panacee. Het blijft een specialistische, gerichte, streng genormeerde en gereguleerde inzet die wordt aangewend in zaken die zien op ernstige of georganiseerde criminaliteit en niet op grote schaal kan worden ingezet.

De rapporten

Wetsevaluatie WODC

Bij deze eerste evaluatie van de Wet CCIII is gekeken naar één onderdeel van de wet, namelijk de bevoegdheid tot het heimelijk en op afstand binnendringen en onderzoek doen in een geautomatiseerd werk. De hoofdvraag van het onderzoek is als volgt geformuleerd: «Op welke wijze wordt uitvoering gegeven aan de hackbevoegdheid en welke eventuele knelpunten doen zich daarbij voor in de opsporingspraktijk?»

Op basis van deze eerste evaluatie is een aantal knelpunten in de opsporingspraktijk naar voren gekomen, die de uitvoering van de bevoegdheid bemoeilijken. Deze knelpunten zijn 1) de manier waarop kan worden binnengedrongen, 2) de inzet van commerciële middelen, 3) de meldplicht die volgt uit artikel 126ffa Sv, 4) het toezicht door de Inspectie en 5) de keuring van technische hulpmiddelen.

Rapport procureur-generaal bij de Hoge Raad

De rapportage van de PGHR is opgesteld in het kader van de toezichthoudende taak die voortvloeit uit artikel 122 lid 1 van de Wet op de rechterlijke

organisatie (Wet RO). Het rapport is getiteld «Onderzoek in een geautomatiseerd werk; over de toepassing van opsporingsbevoegdheden als bedoeld in de artikelen 126nba lid 1, 126uba lid 1 en 126zpa lid 1 van het Wetboek van Strafvordering door het Openbaar Ministerie».

De centrale vraag in dit onderzoek is of de wijze waarop het OM toepassing geeft aan de bevoegdheid voldoet aan de in artikel 126nba Sv opgenomen voorschriften en de beginselen van proportionaliteit, subsidiariteit en behoorlijkheid en of het toezicht op de uitvoering daarvan toereikend is. Het rapport bevat een uitgebreide beschrijving van het juridische en normatieve kader en een bespreking van de uitvoeringspraktijk. De PGHR concludeert dat de binnendringbevoegdheid op sommige punten betrekkelijk minutieus is geregeld. Dat bergt het risico van een zekere starheid in zich, die het OM beperkt in de ruimte om in te spelen op nieuwe ontwikkelingen of om rekening te houden met de omstandigheden van het geval. De wijze waarop het OM toepassing geeft aan de bevoegdheid voldoet in het algemeen aan de wettelijke voorschriften.[6] Op onderdelen doet de PGHR acht aanbevelingen.

Rechtsvergelijkend onderzoek WODC

Dit rapport is het resultaat van de toezegging van de toenmalige Minister van Justitie en Veiligheid om te laten onderzoeken met welke waarborgen het gebruik van technische hulpmiddelen in het buitenland is omkleed.[7] Op Zweden na vindt in ieder land een vorm van keuring of toetsing plaats van het te gebruiken technisch hulpmiddel. Nederland kent de meest gedetailleerd beschreven keuring van technische hulpmiddelen. Geen enkel ander land kent een keuring door een onafhankelijke keuringsdienst waarbij deze keuringsdienst voorafgaand aan een inzet, aan de hand van een uitgebreid keuringsprotocol, de technische hulpmiddelen dient te onderzoeken.[8]

Op basis van het onderzoek heeft het WODC drie scenario's geformuleerd die een aanvulling kunnen bieden op de wijze waarop in Nederland met technische hulpmiddelen en gegevens wordt omgegaan.

Verslag toezicht wettelijke hackbevoegdheid politie 2022

De IJenV brengt jaarlijks een verslag uit over de uitvoering van de binnendringbevoegdheid door de politie. In het rapport over het jaar 2022 trekt de IJenV enkele conclusies en doet de volgende aanbeveling aan de Minister van Justitie en Veiligheid: «Neem een standpunt in over aanpassingen in het wettelijke kader om mogelijke knelpunten bij de praktische uitvoerbaarheid zoals deze door de politie worden ervaren weg te nemen.» Met deze beleidsreactie wordt invulling gegeven aan deze aanbeveling.

Opzet van de reactie op de evaluatie

Gezien de opgedane ervaring, de op punten bijzonder gedetailleerde regelgeving, en het belang van de bevoegdheid voor de opsporing van de meest ernstige vormen van criminaliteit is het verbeteren van de uitvoerbaarheid en efficiëntie van de binnendringbevoegdheid wenselijk. Tegelijkertijd blijven ook uitgebreide voorwaarden en waarborgen wenselijk gegeven de mogelijk grote inbreuk op de persoonlijke levens-

[6] PGHR (2022) Onderzoek in een geautomatiseerd werk, p. 140
[7] Kamerstukken II 2019/20, 29 628, nr. 970
[8] WODC (2023) *De hackbevoegdheid in het buitenland,* p. 10, 95

sfeer, de noodzaak voor maatwerk in de uitvoering en het risico op andere ongewenste neveneffecten.

In de afgelopen jaren is door de politie en het OM op een vakkundige, integere en rechtmatige wijze uitvoering gegeven aan de binnendringbevoegdheid. Er zijn wel enkele aandachtspunten. De conclusies van het WODC in de wetsevaluatie en de aanbevelingen van de PGHR zijn uiteenlopend en bestrijken vele aspecten van de binnendringbevoegdheid. Deze zijn gebundeld en voorzien van een reactie in de bijlage. Waar passend zijn ook de aanbevelingen van de IJenV meegenomen die zij heeft gedaan in haar verslag over het jaar 2022.

De voorgestelde aanpassingen in de uitvoering zijn opgenomen in de bijlage en gegroepeerd naar de verschillende knelpunten die het WODC in de wetsevaluatie heeft geïdentificeerd. Hier worden de aanbevelingen van de PGHR en de bevindingen van de IJenV in het jaarverslag over 2022 meegenomen. Daarnaast worden enkele wensen vanuit de opsporingsinstanties vermeld die in de periode sinds de inwerkingtreding naar voren zijn gekomen. Tenslotte worden enkele aanvullende punten behandeld. De hoofdpunten zijn:

1) de manier waarop kan worden binnengedrongen

Dit spoor bevat voornamelijk technische wijzigingen in wet- en regelgeving. Deze betreffen de verschillende organisatorische randvoorwaarden die verbonden zijn aan het binnendringen. Een voorbeeld hiervan is dat het mogelijk wordt gemaakt niet alleen op afstand binnen te dringen, maar ook op locatie. Dit kan noodzakelijk zijn indien bijvoorbeeld op een camerasysteem van een bedrijf moet worden binnengedrongen. Dan kan nodig zijn dat daarvoor eerst kortstondig een besloten plaats of erf moet worden betreden.

2) de inzet van commerciële middelen

De politie schaft op dit moment in voorkomend geval binnendringsoftware, of een licentie daarvoor, enkel aan voor een specifieke zaak. Deze regeling had tot doel om het betreden van de markt van dergelijke software tot een minimum te beperken, zodat de markt voor onbekende kwetsbaarheden zo min mogelijk wordt gestimuleerd. Met deze regeling wordt de aanschaf van binnendringsoftware sterk ingeperkt. Het WODC stelt in de wetsevaluatie dat het de vraag is of dit model er wel toe leidt dat de markt van onbekende kwetsbaarheden minder gestimuleerd wordt. De IJenV, het WODC en de PGHR signaleren dat deze werkwijze erg kostbaar is. Op basis van deze bevindingen lijkt de Nederlandse Staat met deze regeling uiteindelijk meer te betalen voor deze software dan een model waarbij niet per zaak een licentie moet worden aangeschaft.

Daarnaast blijkt uit de wetsevaluatie van het WODC dat er een zekere mate van afhankelijkheid van deze producten bestaat voor een effectieve uitvoering van de bevoegdheid. Zoals recentelijk gemeld in het verslag van de IJenV over 2022 is in 25 van de 31 zaken gebruik gemaakt van binnendringsoftware van een externe leverancier.[9] Dit maakt deze software een cruciaal middel in de strijd tegen ondermijning en andere ernstige misdrijven.

Om deze redenen bevat dit spoor een beleidswijziging op de aanschaf van binnendringsoftware van een externe leverancier. Het wordt mogelijk om

[9] *Kamerstukken II 2022/23, 29 628 en 34 372, nr. 1187*

binnendringsoftware aan te schaffen en te hergebruiken in andere zaken. Het gebruik blijft wel een uiterste middel bij het binnendringen. Indien een andere methode met succes kan worden ingezet, dan wordt daarvoor gekozen. Minder ingrijpende methoden zoals social engineering, handmatig binnendringen of gebruik van rechtmatig verkregen inloggegevens worden eerst overwogen. In het Jaarverslag van het Ministerie van Justitie en Veiligheid wordt ook de komende jaren gerapporteerd over de hoeveelheid opsporingsonderzoeken waarin de binnendringbevoegdheid is ingezet alsook het gebruik van binnendringsoftware van een externe leverancier in die onderzoeken. De specifieke regelingen inzake de naslag, toets en contractuele clausules voor leveranciers van binnendringsoftware blijven bestaan.

3) de meldplicht van onbekende kwetsbaarheden die volgt uit artikel 126ffa Sv

Op dit moment kan op grond van art. 126ffa Sv het bekend maken aan de producent van een onbekende kwetsbaarheid voor het binnendringen in een geautomatiseerd werk, bedoeld in de artikelen 126nba, 126uba en 126zpa, worden uitgesteld indien een zwaarwegend opsporingsbelang bestaat.[10] In dit spoor wordt een aanpassing van de regeling van het melden van onbekende kwetsbaarheden verkend. In de praktijk is gebleken dat de georganiseerde criminaliteit gebruik maakt van specifiek voor en door hen ontwikkelde software. Het is denkbaar dat dit soort software kwetsbaarheden bevat die onder de reikwijdte van artikel 126ffa Sv kunnen vallen. Het WODC benoemt dit als knelpunt. Melding van deze kwetsbaarheden door opsporingsinstanties aan producenten van deze software zou criminaliteit kunnen faciliteren doordat de software gemaakt voor criminelen daardoor veiliger wordt. Op dit moment is de praktijk zo dat langdurig uitstel van het melden van de kwetsbaarheid mogelijk is in deze gevallen, maar dat de uitstelverzoeken wel periodiek moeten worden herhaald. De komende periode wordt bezien of het melden van onbekende kwetsbaarheden in software voor en door criminelen uitgesloten kan worden van het bereik van artikel 126ffa Sv na een machtiging daartoe van de rechter-commissaris.

4) het toezicht door de Inspectie Justitie en Veiligheid

Het toezicht op de binnendringbevoegdheid is relatief zwaar en intensief vergeleken met andere bijzondere opsporingsmiddelen. De wetgever heeft voorafgaand aan de inwerkingtreding de IJenV gevraagd om nalevingstoezicht. Nalevingstoezicht wil in het kort zeggen dat wordt gekeken naar de rechtmatigheid van de inzet. Op dit moment wordt dit per inzet gecontroleerd, bijvoorbeeld op basis van de verschillende typen logging die worden bijgehouden. In de opstartfase van deze bevoegdheid is dit intensieve toezicht nuttig gebleken aangezien bij de politie ervaring moest worden opgedaan. Door de politie en het OM is de afgelopen jaren de nodige ervaring opgedaan met de binnendringbevoegdheid. In het algemeen kan worden gesteld dat de binnendringbevoegdheid op een vakkundige, integere en rechtmatige wijze wordt ingezet. De wens bestaat dat wordt toegewerkt naar systeemtoezicht op de naleving van de wet- en regelgeving die geldt voor de binnendringbevoegdheid. Dit bestaat veelal uit een audit gericht op de uitvoeringspraktijk, waarbij gebruik wordt gemaakt van de politie-interne borgingssystemen. Hiervoor is het nodig dat het Digital Intrusion Team (DIGIT) van de politie dat de binnendringbevoegdheid uitvoert beschikt over een eigen kwaliteitssysteem. Onder dit spoor wordt door de politie een visie opgesteld waarin concrete acties en verbeteractiviteiten worden beschreven die nodig zijn om het kwaliteits-

[10] ECLI:NL:RBDHA:2013:19764

systeem van DIGIT zodanig in te richten dat systeemtoezicht door de IJenV de norm kan worden. De IJenV wordt hierbij geconsulteerd. Totdat het kwaliteitssysteem op orde is zal sprake zijn van nalevingstoezicht door de IJenV zoals dat nu wordt ingevuld.

De wettelijke mogelijkheid (artikel 65 Politiewet 2012) van de IJenV om risico gestuurd verdiepend onderzoek uit te voeren blijft vanzelfsprekend van toepassing.

5) de keuring van technische hulpmiddelen.

In de WODC-wetsevaluatie wordt geconstateerd dat het ontwikkel- en keuringsproces van een technisch hulpmiddel als een groot knelpunt wordt ervaren. Het technisch hulpmiddel detecteert, registreert en transporteert gegevens die relevant zijn voor het opsporingsonderzoek. De keuring blijkt voor DIGIT niet goed uitvoerbaar in de praktijk. Het WODC schrijft bijvoorbeeld: »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.»[11] Vanuit DIGIT is meer behoefte aan een vorm van risicoanalyse in plaats van een starre goed- of afkeuring. De WODC-wetsevaluatie beschrijft dat bij een risicoanalyse «veel meer uitgegaan zou moeten worden van de vraag wat het risico is als niet aan een bepaalde eis wordt voldaan, in plaats van dat het hulpmiddel voor goedkeuring aan die eis moet voldoen.»[12]

In het rechtsvergelijkend onderzoek van het WODC van 2023 staat vermeld dat op Zweden na in ieder land een vorm van keuring of toetsing van het te gebruiken technisch hulpmiddel plaatsvindt. Nederland kent de meest gedetailleerd beschreven keuring van technische hulpmiddelen. Geen enkel ander land kent een keuring door een onafhankelijke keuringsdienst waarbij deze keuringsdienst voorafgaand aan een inzet, aan de hand van een uitgebreid keuringsprotocol, de technische hulpmiddelen dient te onderzoeken.[13] Op basis van de wetsevaluatie en het rechtsvergelijkend onderzoeksrapport van het WODC worden de politie en het OM gevraagd om uit te werken dat alle technische hulpmiddelen die gegevens automatisch detecteren, registreren en transporteren ter keuring worden aangeboden bij een keuringsdienst. Op deze manier wordt inzicht verkregen in de mate waarin dit hulpmiddel aan de eisen van het Besluit onderzoek in geautomatiseerd werk voldoet en kan de officier van justitie bepalen of aanvullende verificatiemaatregelen moeten worden genomen als aan een eis niet, of niet volledig, wordt voldaan. Op die manier krijgen de rechter, verdediging en officier van justitie inzicht in de bewijswaarde in de rechtszaal van de verkregen informatie. Hiermee zou het uitgangspunt dat alleen goedgekeurde hulpmiddelen worden ingezet worden gewijzigd. De door het WODC beschreven elementen zoals voldoende technische deskundigheid in de rechtbank en gevolgen voor de afscherming van de opsporingsmethode worden hierin meegenomen. Deze aanpassing vereist een wijziging in het Besluit onderzoek in geautomatiseerd werk. Hierbij wordt het gebruikelijke traject van het betrekken van de relevante actoren in acht genomen. Uit dit overleg is het mogelijk dat alternatieve effectieve oplossingen voortkomen.

[11] WODC (2022) De hackbevoegdheid in de praktijk, p. 147
[12] WODC (2022) De hackbevoegdheid in de praktijk, p. 175 ev
[13] WODC (2023) De hackbevoegdheid in het buitenland, p. 95.

6) Procedurele of aanvullende waarborgen, vernietigen van gegevens en overige punten

Dit spoor bevat voornamelijk conclusies en aanbevelingen van de PGHR die niet onder één van de vijf andere sporen kunnen worden geschaard en aanvullende punten die vanuit de praktijk onder de aandacht van het departement zijn gebracht. Voorbeelden hiervan zijn de vastlegging van procedurele en aanvullende waarborgen in de procesdossiers, aandacht voor het opstellen van de processen-verbaal en de rol van de rechter-commissaris in de omgang met geheimhoudersgegevens. De IJenV heeft hier in haar verslag over het jaar 2022 eveneens opmerkingen over gemaakt.

Ondanks bovengenoemde aanpassingen blijft de bevoegdheid gepaard gaan met passende voorwaarden en waarborgen. Er blijft bijvoorbeeld sprake van een uitvoerig besluitvormingstraject voorafgaand aan de inzet van de binnendringbevoegdheid, waaronder een machtiging van de rechter-commissaris. Ook blijft er sprake van controle op de uitvoering van de bevoegdheid door een speciaal aangewezen officier van justitie en vindt toezicht plaats door de IJenV. Tevens blijven er verschillende test- en keuringsvoorschriften gelden en blijven aanvullende regels voor aanschaf van binnendringsoftware van externe leveranciers en transparantie over de inzet daarvan.

Echter, met bovengenoemde aanpassingen wordt de effectiviteit van de binnendringbevoegdheid vergroot door de nodige flexibiliteit en maatwerk te introduceren en starheid in de regelgeving te verhelpen. Op sommige onderdelen is meer onderzoek nodig, omdat het vaak om complexe vraagstukken gaat. Uiteindelijk is het doel dat de binnendring-bevoegdheid een effectiever instrument wordt. Dat is van belang in de strijd tegen ernstige en georganiseerde criminaliteit, maar ook in opsporingsonderzoeken naar moord, cybercrime, terrorisme en seksueel kindermisbruik.

De Minister van Justitie en Veiligheid,
D. Yeşilgöz-Zegerius

Bijlage

In deze bijlage worden de veranderingen, of het voornemen daartoe, nader geschetst. Eerst worden in de tabellen de conclusies van het WODC uit de wetsevaluatie, de aanbevelingen en daarbij horende conclusies van de PGHR vermeld en waar relevant de bevindingen van de IJenV in haar verslag over het jaar 2022 of het rechtsvergelijkend onderzoek van het WODC. In een aantal gevallen wordt voorts ingegaan op voornemens uit de praktijk van de opsporingsinstanties. Na de weergave van de bevinden in de tabellen wordt daaronder een reactie gegeven en de (voorgenomen) acties benoemd.

Spoor 1 de manier waarop kan worden binnengedrongen

Introductie

Aan het binnendringen zijn verschillende organisatorische randvoorwaarden verbonden, zoals het plan van aanpak in een haalbaarheidsonderzoek, de kwalificaties van het personeel en het gegeven dat een inzet «heimelijk en op afstand» moet gebeuren. In dit spoor worden voorstellen tot wijziging gedaan over de randvoorwaarden waaronder de inzet plaatsvindt of worden enkele verduidelijkingen gegeven bij het bestaand wettelijk kader. In deze introductie kan ook worden gewezen op het advies van de Cybersecurityraad. Zij stelt voor de mogelijkheid uit te werken van een transparante wettelijke regeling voor versterkte toegang bij telecomproviders, teneinde een betere uitgangspositie te hebben om specifieke mobiele telefoons te kunnen binnendringen.[14] Dit wordt nader onderzocht.

I. Steunbevoegdheid voor inzet op een locatie nabij het geautomatiseerde werk
WODC
• 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 nog niet is.
PGHR
• Geen aanbevelingen.

Reactie: in de praktijk blijkt een behoefte te bestaan voor de mogelijkheid om weliswaar heimelijk een inzet te plegen, maar niet louter op afstand. Op afstand kan namelijk niet altijd worden binnengedrongen. Indien bijvoorbeeld op een camerasysteem van een loods moet worden binnengedrongen, kan het nodig zijn dat daarvoor eerst kortstondig een besloten plaats of erf moet worden betreden. Deze betredingsbevoegdheid is vergelijkbaar met de wijze waarop het betreden van besloten plaatsen is geregeld voor het opnemen van vertrouwelijke communicatie (artikel 126l, tweede lid, Sv) of het stelselmatig observeren (artikel 126g, tweede lid, Sv). Een wetsvoorstel om dit ook voor de binnendringbevoegdheid in de wet op te nemen, zal worden voorbereid.

[14] CSR, 23 augustus 2022, Adviesbrief inzake reële alternatieven voor rechtmatige toegang tot end-to-end versleutelde communicatie, anders dan inperking van encryptie.

II. Verduidelijking functiescheiding tussen het technisch team dat de inzet uitvoert (DIGIT) en het tactisch team van het opsporingsonderzoek

WODC

- 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.

PGHR

- Geen aanbevelingen

Reactie: uit de praktijk is gebleken dat behoefte is aan verduidelijking van de functiescheiding tussen het technisch team en het tactisch team. Deze verduidelijking wordt hier gegeven, dit betreft geen beleidswijziging. Bij de inzet van de bevoegdheid wordt onderscheid gemaakt tussen het technisch team dat de inzet uitvoert en het tactisch team dat het opsporingsonderzoek uitvoert in het kader waarvan de inzet nodig is. Deze scheiding is gemaakt om te voorkomen dat het technisch team (het Digital Intrusion Team, of DIGIT) wordt beïnvloed ten aanzien van de haalbaarheid van de inzet en de uitvoering daarvan. Deze scheiding betekent echter niet dat er geen communicatie kan plaatsvinden tussen DIGIT en het tactisch team. In de Nota naar aanleiding van het verslag staat reeds vermeld: «Deze scheiding van functies behoeft de communicatie tussen de teams niet te belemmeren. «[15] Artikel 4 van het Besluit onderzoek in een Geautomatiseerd werk (Bogw) geeft de korpschef daarnaast de bevoegdheid om een lid van het tactisch team als deelnemer van het DIGIT aan te wijzen. Hierbij kan worden gedacht aan de situatie dat een opsporingsambtenaar van een bijzondere opsporingsdienst met specifieke kennis op het gebied van digitale fraude tijdelijk wordt toegevoegd aan DIGIT in verband met gewenste ICT-expertise op dit gebied in een specifiek onderzoek. Het WODC stelt in de wetsevaluatie dat er belangrijke informatie bij het tactisch team aanwezig kan zijn dat kan bijdragen aan een zorgvuldige voorbereiding of uitvoering van het bevel. Het Bogw verzet zich niet tegen het delen van deze informatie. De functiescheiding tussen DIGIT en tactisch team kan plaatsvinden zolang DIGIT zelfstandig kan blijven besluiten of bepaalde binnendring- en onderzoekshandelingen haalbaar zijn en deze verantwoord binnen de kaders van een afgegeven bevel kunnen worden uitgevoerd. Het tactisch team kan hierin wensen uiten of verzoeken doen. Het technisch team beslist vervolgens of de uitvoering passend en geboden is. De speciaal aangewezen officier van justitie voor de binnendringbevoegdheid houdt toezicht op de rechtmatigheid van de inzet.

III. Centrale rol DIGIT-OM en organisatorische borging expertise ten behoeve van de continuïteit

WODC

- Toetsing van de inzet: 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.

PGHR

- Geen aanbevelingen

[15] Kamerstuk 34 372, nr. 6

Reactie: het OM heeft ervoor gekomen om het gezag over de uitvoering van de binnendringbevoegdheid centraal te beleggen. Er bestaat een speciaal voor de binnendringbevoegdheid aangewezen landelijk officier van justitie die betrokken is bij de voorbereidingen voor de inzet en de controle op de uitvoering. Dit heeft veel voordelen, zoals het samenbrengen van expertise, het bundelen van ervaring met de binnendringbevoegdheid en professionaliteit bij de uitvoering ervan. Daarbovenop wordt door deze officier toezicht gehouden tijdens een inzet. Hoewel de PGHR geen aanbevelingen doet op dit punt, deelt hij wel een constatering. De PGHR constateert dat er organisatorische risico's mee verbonden zijn, zoals het verlies van essentiële kennis bij het onverhoopte uitvallen van de DIGIT-officier en de DIGIT-parketsecretaris, alsmede het gevaar van onvoldoende gecontroleerd, solistisch optreden.

De bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk is een specialistische bevoegdheid die beperkt kan worden ingezet. Navraag bij het OM leert dat de risico's zich momenteel niet verwezenlijken. Echter, ik zal monitoren of de genoemde risico's zich voordoen zodra de inzet van de bevoegdheid toeneemt.

IV. Aanpassing wet- en regelgeving voor binnenkomende en uitgaande rechtshulpverzoeken

WODC

- 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.

PGHR

- Geconstateerd kan worden dat de Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv correspondeert met het door de Minister verwoorde uitgangspunt, zonder dat op voorhand moet worden geoordeeld dat de inhoud van deze aanwijzing zich naar de huidige stand van zaken niet verdraagt met het internationale recht. Voor verdergaande toetsing bestaat geen aanleiding.
- Kort gezegd hebben de onderzoekers geconstateerd dat de door het OM zelf opgestelde Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv niet in alle gevallen een adequate oplossing biedt wanneer de uitoefening van de bevoegdheid van artikel 126nba Sv buiten het grondgebied van Nederland plaatsheeft. In een geval waarin het ging om de ontoegankelijkmaking van een wereldwijd verspreid botnet viel te verdedigen dat voor de ontoegankelijkmaking geen toestemming is gevraagd aan alle landen waarin zich gecompromitteerde geautomatiseerde werken bevonden. Niettemin moet worden geconstateerd dat de Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv niet voorziet in een uitzondering voor een dergelijk geval
- Aanbeveling: Het verdient aanbeveling om te bezien of de Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv dient te worden aangepast om te voorzien in de situatie waarin een wereldwijd netwerk van een grote hoeveelheid botnets wordt ontmanteld.

Reactie: 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. Het uitgangspunt hierbij is dat in beginsel rechtshulp moet worden gevraagd, hetgeen strookt met het internationale recht en met het materieel-wettelijk kader van de binnendringbevoegdheid. In de meer recente «Instructie voor de inzet van de bevoegdheid ex. artt. 126nba, 126uba, 126zpa en 126ffa Sv (2021l002)» zijn nadere aanwijzingen opgenomen. De WODC-wetsevaluatie geeft aan dat in de OM-aanwijzing niets is geregeld voor inzetten op Nederlands grondgebied door het buitenland. Het is wenselijk dat ook in de Aanwijzing wordt ingegaan op inzetten op Nederlands grondgebied door het buitenland. In een reactie op het PGHR-rapport heeft het College van procureurs-generaal laten weten dat

door het OM – in samenspraak met het technisch team van de politie – wordt gekeken hoe de aanbevelingen van de PGHR rond de Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex. artikel 126nba Sv kunnen worden opgevolgd. Bij rechtshulp is sprake van de uitvoering van een bevel door de daartoe geautoriseerde diensten van het land waar het bevel op ziet. Echter, met de bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk hoeft DIGIT niet vanzelfsprekend zelf de uitvoerende partij te zijn. Er wordt bestudeerd of hier een aanvullende wettelijke regeling voor nodig is.

V. Bevel uitvoering ten behoeve van het opnemen van vertrouwelijke communicatie (art. 126 (1)(b) Sv) op mobiele apparaten en faciliterende methodieken
WODC
• Geen aanbevelingen
PGHR
• Op deze plaats verdient opmerking dat het opnemen van vertrouwelijke communicatie (OVC) in combinatie met het onderzoek in een geautomatiseerd werk in de praktijk bijzondere aandacht heeft en ook verdient. De onderzoekers achten het gericht aan- en uitzetten van de OVC niet problematisch en zelfs aan te bevelen. Op die manier wordt immers voorkomen dat wordt opgenomen op andere plekken dan in het bevel voorzien. Wel dient – om willekeur te voorkomen en disproportioneel optreden tegen te gaan – te worden verantwoord waarom op bepaalde plekken en tijden al dan niet wordt opgenomen. In de onderzochte zaken waarbij sprake was van OVC hebben de onderzoekers geen stukken aangetroffen waaruit de verantwoording achteraf expliciet blijkt. Wel volgt uit de stukken duidelijk dat voorafgaand aan de uitoefening van de bevoegdheid is vastgelegd op welke plekken gesprekken (zullen) worden opgenomen, en waarom. Aanbeveling: Het verdient (blijvend) aandacht om de inzet van OVC met betrekking tot (mobiele) geautomatiseerde werken te verantwoorden, bijvoorbeeld in processenverbaal. • Bij het toezichtonderzoek is geconstateerd dat in bepaalde gevallen faciliterende methodieken, als hier bedoeld, zijn toegepast die louter waren gegrond op artikel 3 Politiewet. Het toezichtonderzoek wijst uit dat toetsing door de DIGIT-officier plaatsvindt aan de hand van criteria die in overeenstemming zijn met de wet en de heersende jurisprudentie van de Hoge Raad dienaangaande. Binnen het bestek van het uitgevoerde dossieronderzoek geeft de uitkomst van deze toetsingen de onderzoekers geen reden voor commentaar. De DIGIT-officier heeft aangegeven dat het inmiddels huidige praktijk is dat de faciliterende methoden als hier bedoeld worden gedekt door een bevel ex artikel 126nba Sv.

Reactie: in het geval een mobiel apparaat als middel wordt gebruikt om vertrouwelijke communicatie op te nemen valt in de praktijk niet op voorhand te voorspellen waar de persoon die de telefoon draagt naar toe gaat. Binnen minuten kan de persoon zich verplaatsen tussen auto, openbare weg, eigen woning, woning van anderen en overige plaatsen. In bevelen moet de locatie vaak strikt worden beschreven, maar in de praktijk laat de locatie zich lastig voorspellen en hebben de opsporingsinstanties daar geen invloed op. Bovendien is het technisch lastig om telkens voor een korte tijd het mobiele apparaat waarop is binnengedrongen te onderbreken. Het «aan en uit schakelen» bij betreden van een niet in de machtiging opgenomen locatie is vaak niet mogelijk, omdat bijvoorbeeld het zicht ontbreekt waar het individu zich bevindt, of dat het individu zich in korte tijd beweegt tussen locaties. Dit zou vereisen dat enkele seconden de opname wordt onderbroken. Nader bekeken wordt of de wettelijke eis van de bekende locatie kan worden aangepast.

VI. Erkenning essentiële rol aan de Centrale Toetsingscommissie in de Aanwijzing opsporingsbevoegdheden

WODC

- Geen aanbevelingen

PGHR

- In de Instructie is een essentiële rol toegekend aan de Centrale toetsingscommissie (CTC). Het bestaan van de CTC en haar werkzaamheden zijn gegrond op de Aanwijzing opsporingsbevoegdheden, nr. 2014A009, Stcrt. 2014, nr. 24442, afkomstig van het College van procureurs-generaal. Deze aanwijzing voorziet echter niet in een rol van de CTC in het hiervoor beschreven werkproces voor de uitoefening van de bevoegdheid ex artikel 126nba Sv.
  Aanbeveling: Aanbevolen wordt om de Aanwijzing opsporingsbevoegdheden, nr. 2014A009, Stcrt. 2014, nr. 24442, aan te passen zodat deze voldoet aan het in hoofdstuk 3 genoemde normatief kader en de in hoofdstuk 4 genoemde Instructie, in het bijzonder wat betreft het opnemen van de rol van de CTC ten aanzien van de bevoegdheid onderzoek in een geautomatiseerd werk.

Reactie: de aanbeveling van de PGHR wordt overgenomen. De Aanwijzing opsporingsbevoegdheden, nr. 2014A009, Stcrt. 2014, nr. 24442 zal hierop worden aangepast.

VII. Inhoud en uitvoering van het bevel

WODC

- Geen aanbevelingen

PGHR

Inhoud van het bevel:

- De verschillende voorgeschreven stappen in het besluitvormingsproces bleken in alle onderzochte zaken telkens vastgelegd in het «nba-dossier». In alle gevallen waarin de bevoegdheid van artikel 126nba Sv is uitgeoefend, is de gerezen verdenking voldoende geconcretiseerd in het projectvoorstel (i.e. het proces-verbaal van aanvraag, met bijlagen), alsook in de adviesaanvraag aan de CTC en in het advies van de CTC zelf. Bovendien is in die documenten telkens uitvoerig stilgestaan bij de vraag of er alternatieven voorhanden zijn die minder ingrijpen in de persoonlijke levenssfeer van de betrokkene(n). De vragen naar de noodzaak, het verwachte resultaat en het afbreukrisico, alsook het risico voor het geautomatiseerde werk zijn nadrukkelijk (en telkens uitvoerig) onder ogen gezien. De daaraan gewijde passages betreffen geen routinematige «standaardbeschouwingen». Over het algemeen is vastgesteld dat de vorderingen en de bevelen correspondeerden met elkaar en met de machtigingen. De vorderingen en de bevelen voldeden aan de wettelijke voorschriften. Wel zijn een betrekkelijk gering aantal onvolkomenheden en bijzonderheden geconstateerd. Aanbeveling: Het verdient aandacht om de informatie waarvan de wet voorschrijft dat die wordt opgenomen in het bevel, zo concreet mogelijk te omschrijven.

Reactie: de aanbeveling van de PGHR wordt overgenomen. Het OM heeft mij te kennen gegeven dat zij in overleg met het technische team van de politie deze aanbeveling hebben opgevolgd.

VIII. Verlenging van de termijn waarvoor een rechter-commissaris een machtiging kan afgeven

Voornemen uit de praktijk van de opsporingsinstanties

Reactie: op dit moment is een bevel van de rechter-commissaris vier weken geldig met de mogelijkheid tot verlenging. Gegeven het nauwkeurige voorbereidingstraject en de onvoorspelbaarheid of de gekozen manier waarop een inzet wordt uitgevoerd ook succesvol is, wordt de termijn van vier weken als te kort ervaren. Bijvoorbeeld doordat

een inzet niet succesvol is en de plannen moeten worden aangepast, of DIGIT ondervindt moeilijkheden bij het binnendringen. Het kan theoretisch mogelijk zijn dat een bevel van vier weken wordt afgegeven zonder dat het daadwerkelijk lukt om binnen te dringen. Mogelijk is een vorm denkbaar dat een bevel voor vier weken wordt afgegeven vanaf het moment van binnendringen, maar dat DIGIT langer de tijd heeft voor het proces van binnendringen zelf. In samenspraak met de opsporingsinstanties wordt gezocht naar een geschikte termijn.

IX. Differentiatie kwalificaties leden en deelnemers technisch team

Voornemen uit de praktijk van de opsporingsinstanties

Reactie: op dit moment wordt er niet gedifferentieerd in niveau van de kwalificatie-eisen binnen het technisch team. Iedereen moet aan hoge eisen voldoen, terwijl er in de praktijk verschillen zijn in de taken en vereiste expertise. Er is bijvoorbeeld een ander expertiseniveau nodig voor een inzet met veel ad hoc aanpassingen dan bij werkzaamheden met een al bestaande «tool» waarvan men alleen de werking goed moet kennen. Het gebrek aan een gedifferentieerd niveau van kwalificatie-eisen maakt het moeilijker voldoende personeel in dienst te nemen en het duurt lang voor personeel inzetbaar is.

X. Duiding plan van aanpak in een haalbaarheidsonderzoek

Bestendiging van beleid.

Reactie: uit de praktijk blijkt dat er soms verschillende interpretaties bestaan over de verschillende stappen in het binnentreden. Bijvoorbeeld, of het Plan van Aanpak een blauwdruk is dat naar de letter moet worden gevolgd of een voorgenomen wijze van binnendringen waarvan kan worden afgeweken als de concrete situatie dat verlangt. Ik wil graag verduidelijken dat het Plan van Aanpak een voorgenomen werkwijze is waar men, binnen de kaders, van af moet kunnen wijken. Een bindend Plan van Aanpak leidt tot ongewenste starheid. Gegeven de eerder geschetste onvoorspelbaarheid van een inzet bestaat er een noodzaak voor een bepaalde wendbaarheid. Ook kan een minder ingrijpende inbreuk in het geautomatiseerde werk het resultaat zijn als tijdens een inzet de gewenste informatie sneller is verkregen dan voorzien.

XI. De lijst met misdrijven in het Besluit onderzoek in een geautomatiseerd werk (Bogw) wordt aangepast

Voornemen uit de praktijk van de opsporingsinstanties.

Reactie: voor de inzet van de bevoegdheid tot het vastleggen van gegevens of het ontoegankelijk maken daarvan moet sprake zijn van een misdrijf waarop een gevangenisstraf van acht jaar of meer is gesteld. Uitzondering hierop is een lijst van misdrijven in het Bogw. Er wordt ingezet om deze lijst aan te vullen met: de artikelen 10, derde lid, en 10a van de Opiumwet; artikel 55, derde lid, van de Wet wapens en munitie en artikel 151 van het Wetboek van Strafrecht. Deze uitbreiding vloeit voort uit de in afgelopen jaren toegenomen ernstige ondermijnende criminaliteit. Opsporingsonderzoeken naar in genoemde artikelen strafbaar gestelde misdrijven kunnen in sterke mate bijdragen aan de bestrijding dergelijke criminaliteit. Daarnaast kan het opnemen van misdrijven in het Bogw een bijdrage leveren aan een effectieve opsporing van de georgani-

seerde criminaliteit, zoals het wegmaken van een lijk. De uitbreiding van de lijst met dit artikel sluit aan bij het op 1 december 2022 verschenen WODC-rapport Strafbaarstelling van lijkschennis.[16] Aanpassing van het wettelijk kader is hiervoor nodig. Tot slot wordt vermeld dat er op dit moment twee wetsvoorstellen aanhangig zijn die mogelijk ook tot uitbreiding van de in het Bogw genoemde strafbare feiten nopen. Dit zijn het Wetsvoorstel tot wijziging van het Wetboek van Strafrecht en het Wetboek van Strafrecht BES in verband met de uitbreiding van de strafbaarheid voor spionage en de beoogde Wet seksuele misdrijven. Deze wetten bevatten strafbaarstellingen waarvan het wenselijk is dat opname in het Bogw wordt overwogen.

Spoor 2 de inzet van commerciële middelen

Introductie

De aanschaf van binnendringsoftware is aan strikte voorwaarden gebonden. De politie kan op dit moment binnendringsoftware van externe leveranciers aanschaffen in een specifieke zaak. Bij gebruik van die software wordt er een licentie of gebruiksrecht aangeschaft die enkel bruikbaar is in die zaak. Na het onderzoek wordt het softwarepakket verwijderd of is de licentie verbruikt waardoor hergebruik niet meer mogelijk is. Ook behoort het gebruik van binnendringsoftware van externe leveranciers een uiterste middel te zijn.[17] De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) doet naslag naar leveranciers van dergelijke software en de politie toetst dat de leveranciers niet verkopen aan dubieuze regimes.[18] Naslag houdt in dat de AIVD haar systemen raadpleegt en beoordeelt of het bedrijf een bedreiging vormt voor de nationale veiligheid. Statistieken over het gebruik van binnendringsoftware worden openbaar gemaakt in het Jaarverslag van Justitie en Veiligheid.

Deze regeling heeft tot doel om het betreden van de markt van dergelijke software tot een minimum te beperken. In het «Verslag toezicht wettelijke hackbevoegdheid politie 2021» van de IJenV staat vermeld dat in de praktijk het voorgeschreven licentiemodel leidt tot extra kosten voor de politie en daarmee mogelijk tot een extra stimulans voor de markt voor binnendringsoftware.[19] Dit wordt in het IJenV verslag over het jaar 2022 herhaald. Het WODC deelt deze constatering in de wetsevaluatie en noemt het licentiemodel duur en stelt de vraag of dit model er wel toe leidt dat de markt van onbekende kwetsbaarheden minder gestimuleerd wordt.[20] De PGHR herhaalt de constatering van de DIGIT-officier (de speciaal aangewezen officier van justitie die toeziet op de uitvoering van de binnendringbevoegdheid) die stelt dat deze licenties zeer kostbaar zijn en dat het aanschaffen van tijdelijke licenties (bij lange na) niet de goedkoopste manier is waarop de gebruiksrechten van de binnendringsoftware kunnen worden verworven.[21]

Deze vaststelling brengt het volgende dilemma met zich mee. Enerzijds bestaat de wens om de markt voor binnendringsoftware van externe leveranciers tot een minimum te beperken. Uit bovenstaande verslagen volgt evenwel dat de huidige regeling waarschijnlijk het tegenovergestelde effect heeft. Anderzijds constateert het WODC in de wetsevaluatie

---

[16] https://repository.wodc.nl/handle/20.500.12832/3226
[17] *Kamerstukken II* 2016/17, motie van het lid Recourt, 34 372, nr. 23
[18] Aanhangsel Handelingen II 2018/19, nr. 3537
[19] Inspectie Justitie en Veiligheid, Verslag toezicht wettelijke hackbevoegdheid politie 2021, p. 14)
[20] WODC, Hackbevoegdheid in de praktijk, p. 107
[21] PGHR, Onderzoek in een geautomatiseerd werk, p. 115

dat het gebruik van commerciële middelen praktisch onmisbaar is, omdat een groot deel van de inzetten (op een telefoon) anders niet kan worden uitgevoerd. In het verslag van de IJenV over het jaar 2022 staat dat in 25 van de 31 zaken waarin de binnendringbevoegdheid is ingezet gebruik is gemaakt van binnendringsoftware van een externe leverancier.[22] Dit maakt deze software een cruciaal middel in de strijd tegen ondermijnende en andere ernstige misdrijven. De PGHR stelt hierover dat het gebruik van dergelijke binnendringsoftware op zichzelf verenigbaar is met de geldende wettelijke voorschriften en met de beginselen van proportionaliteit, subsidiariteit en behoorlijkheid in individuele zaken. Echter, de uitvoeringspraktijk van artikel 126nba Sv staat op gespannen voet met het door de Minister van Justitie en Veiligheid in de wetsgeschiedenis tot uitdrukking gebrachte uitgangspunt dat bij het uitvoeren van onderzoek in een geautomatiseerd werk in beginsel geen gebruik wordt gemaakt van commerciële software waarvan onduidelijk is of die software onbekende kwetsbaarheden exploiteert. De PGHR stelt dat het probleemveld voor het overige politiek van aard is, zodat hier met de signalering van het voorgaande wordt volstaan.

I. Aanschaf van binnendringsoftware van externe leveranciers binnen de kaders van 126nba, 126uba en 126zpa Sv hoeft niet meer voor een specifieke zaak
WODC
• 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.
PGHR
• Geen aanbevelingen
IJenV
• Ten tweede is tijdens de parlementaire behandeling toegezegd dat de markt voor onbekende kwetsbaarheden zo min mogelijk moet worden gestimuleerd. De Inspectie signaleert, evenals over de drie afgelopen jaren, dat in de praktijk het voorgeschreven licentiemodel juist leidt tot extra kosten voor de politie en daarmee mogelijk tot een extra stimulans van deze markt.

Reactie: de aanschaf van binnendringsoftware wordt niet meer beperkt tot een specifieke zaak. Gegeven de mate van afhankelijkheid van deze software is effectieve toegang tot deze software nodig. In de WODC-wetsevaluatie staan redenen waaruit blijkt dat de tijd, het geld en de capaciteit die benodigd is voor de toepassing van de binnendringbevoegdheid zonder binnendringsoftware van externe leveranciers binnen het Nederlands bestek niet realistisch is. Tegelijkertijd schrijft de motie van het lid Recourt (PvdA) uit 2017[23] voor dat binnendringsoftware van een externe leverancier slechts in het uiterste geval mag worden gebruikt.

Binnendringsoftware blijft een uiterste middel dat gebruikt kan worden voor de binnendringbevoegdheid. Minder ingrijpende methoden zoals social engineering, handmatig binnendringen of gebruik van rechtmatig verkregen inloggegevens worden eerst overwogen. Echter, gegeven de context van de opsporingsonderzoeken waarin de binnendringbe-

[22] Inspectie Justitie en Veiligheid, Verslag toezicht wettelijke hackbevoegdheid politie 2022, p. 8)
[23] Kamerstukken II 2016/17, 34 588, nr. 66

voegdheid wordt gebruikt volstaan minder ingrijpende methoden veelal niet. Het is daarom goed mogelijk dat software van een externe leverancier relatief vaak wordt ingezet ten opzichte van het aantal inzetten. Toch moet van lichtzinnig gebruik geen sprake zijn. De officier van justitie maakt een professionele inschatting die wordt voorgelegd aan de Centrale toetsingscommissie welke het College van procureurs-generaal adviseert. Het gebruik kan verder worden gecontroleerd door uw Kamer via de verantwoording die wordt afgelegd in het jaarverslag van het Ministerie van Justitie en Veiligheid. Geconcludeerd kan worden dat met dit beleid de markt voor binnendringsoftware minder wordt gestimuleerd dan met het huidige beleid.

II. Toets dubieuze regimes en de naslag door de AIVD blijven bestaan

Bestendiging van beleid.

Reactie: in deze paragraaf doe ik graag de toezegging gestand aan het lid Kuik (CDA) over de internationale samenwerking om misbruik van binnendringsoftware tegen te gaan. De breed gedragen wens om misbruik van binnendringsoftware tegen te gaan blijkt onder andere uit de in maart 2023 gepresenteerde «Guiding Principles on Government Use of Surveillance Technologies» welke Nederland mede heeft ondertekend.[24] Nederland veroordeelt misbruik van binnendringsoftware en is bereid om hiertoe diplomatieke middelen in te zetten.[25] Nederland overweegt deelname aan nieuwe internationale trajecten zorgvuldig, met inachtneming van de eigen operationele benodigdheden. De inzet van binnendringsoftware in het kader van de opsporing in Nederland is conform internationale mensenrechtenverdragen, mede vanwege de strikte voorwaarden en waarborgen die op de inzet van de bevoegdheid van toepassing zijn. Dergelijke inzet is nodig in de strijd tegen criminaliteit en moet op een effectieve wijze mogelijk blijven. Inmiddels is de verklaring van de Verenigde Staten waarop het lid Kuik doelde besproken in de cyber-dialoog met de VS op 4 mei jl. en zullen de gesprekken over de mogelijke opvolging van deze verklaring worden voortgezet.

Misbruik van binnendringsoftware door repressieve regimes of waar de democratische rechtsstaat onder druk staat kan fundamentele rechten onderdrukken en democratische processen en rechtstatelijke waarden schaden. Er bestaan leveranciers die binnendringsoftware aan repressieve regimes verkopen en daarmee deze regimes faciliteren. Om deze reden houdt het kabinet vast aan het beleid dat zoveel mogelijk voorkomt dat het software van deze leveranciers ten behoeve van de opsporing afneemt. Om deze reden blijft het verbod op aanschaf van software bij leveranciers die verkopen aan dubieuze regimes bestaan en pleegt de AIVD naslag naar deze leveranciers om vast te stellen of deze geen dreiging vormen voor de nationale veiligheid.[26] Tevens zal het kabinet diplomatieke middelen blijven inzetten om landen die deze technologieën misbruiken aan te spreken, waar mogelijk en opportuun in EU-verband.

De PGHR concludeert hierbij dat: «Hoewel de leverancier van TH Brons door de AIVD is gescreend en de AIVD geen bezwaar heeft afgegeven, laat de door de politie uitgevoerde (thans: periodieke) toets de mogelijkheid open dat het systeem waarvan TH Brons onderdeel is ook wordt geleverd aan (politie- of inlichtingendiensten of vervolgingsinstanties van) landen

[24] FOC_Guiding_Principles_on_Government_Use_of_Surveillance_Technologies.pdf (freedomonlinecoalition.com)
[25] Aanhangsel Handelingen II 2021/22, nr. 3252
[26] Aanhangsel Handelingen II 2018/19, nr. 3537

die zich schuldig maken aan ernstige schendingen van mensenrechten of internationaal humanitair recht. Daar staat tegenover dat de aanwending van het systeem waarvan TH Brons onderdeel is, in de onderzochte zaken daadwerkelijk heeft geleid tot onderzoeksresultaten waartoe de inzet van TH Brons strekte. Kort gezegd, het systeem doet wat het moet doen. De afweging van de hierboven geschetste risico's en bezwaren enerzijds en het belang van de bestrijding van ernstige criminaliteit anderzijds, waarbij aan het tweede prioriteit is gegeven, is binnen het OM centraal en op zichzelf zorgvuldig, namelijk in een uitvoerig afwegingsproces, tot stand gekomen.»[27]

In antwoord hierop erken ik dat de hierboven genoemde toets door de politie[28] en de naslag door de AIVD geen honderd procent zekerheid biedt dat geen product wordt afgenomen van een ongewenste leverancier. Wel kan de inspanning om dit te voorkomen het risico beperken. Het is daarom wenselijk dat deze inspanning niet wordt verminderd.

III. Het testen

Bestendiging van beleid.

Reactie: het functioneren van de binnendringsoftware wordt in een testomgeving gecontroleerd. Daarbij wordt aandacht besteed aan de risico's voor het te onderzoeken geautomatiseerd werk en schade aan derden. Dit zal blijven gebeuren, met de aantekening dat wordt getest met het oogmerk om risico's voor het functioneren van het geautomatiseerde werk zoveel mogelijk te beperken op basis van de bestaande kennis. Testen ziet niet op het uitsluiten van risico's, dit is onmogelijk aangezien vaak wordt binnengedrongen op «vijandige infrastructuur» die niet bij voorbaat kan worden nagebootst. Tevens kan de test per inzet verschillend zijn. Een test bij een inzet op een server waar ook legitieme ondernemingen op draaien kan anders zijn dan indien dit een geautomatiseerd werk is dat voornamelijk criminele activiteiten ondersteunt. Indien na het binnendringen de risico's voor het geautomatiseerd werk anders zijn dan van tevoren voorzien, is het aan de DIGIT-officier om een afweging te maken en te bepalen of een inzet wordt voortgezet of afgebroken.

IV. Voorkomen kennisneming vergaarde gegevens bij binnendringsoftware van externe leveranciers

IJenV

De Inspectie concludeert dat de politie dit [mogelijke toegang door de leverancier tot de gegevens die verkregen worden en de mogelijkheid zelfstandig updates uit te voeren of zelf de controle over het geautomatiseerde werk over te nemen, red.] – door het black-box karakter van de gebruikte software – technisch niet kan afdwingen en niet kan controleren.

Zoals vermeld in mijn reactie op het IJenV verslag van 2021 stelt de IJenV terecht dat de technische werking van binnendringsoftware niet afdwingbaar of controleerbaar is. Dit is een dilemma omdat onmisbare expertise op deze terreinen bij commerciële partijen ligt. Dit dilemma beperkt zich niet tot de opsporing. Zoals gesteld in mijn beleidsreactie op het Inspectieverslag van

[27] PGHR, p. 137
[28] Aanhangsel Handelingen II 2018/19, nr. 3537

2020 is de Nederlandse overheid vaker afhankelijk van goede samenwerking met commerciële partijen vanwege de onmisbare expertise. Voor de betrokken commerciële partijen zijn de belangen om een betrouwbare partner voor de overheid te zijn en zich te houden aan de afspraken evident. De genoemde bindende contractuele afspraken die zijn gemaakt met leveranciers van commerciële software vormen een gebruikelijke waarborg om de samenwerkingsrelatie en de integere uitvoering van de afgenomen dienst te borgen.

Voor de volledigheid kan hierbij op de conclusie van de PGHR worden gewezen: «Werkzaamheden die de leverancier uitvoert kunnen mogelijk zelfs tijdens de daadwerkelijke inzet invloed hebben op de werking en functionaliteiten van TH Brons (pseudoniem voor de software in kwestie, red).»

In reactie hierop vermeld ik dat de politie een onderhoudscontract bij een leverancier afneemt. Voordeel hiervan is dat de continuïteit van de werking van de binnendringsoftware zo veel mogelijk gewaarborgd kan blijven. In dat contract worden strikte afspraken gemaakt over de toegang van de leverancier tot componenten van het product dat is geleverd aan de politie. Deze afspraken en de mogelijkheid deze in rechte af te dwingen vormen waarborgen om onbevoegde toegang van de leverancier tot componenten van het product tegen te gaan. Daarbij kan worden vermeld dat, als later blijkt dat leveranciers de vragen niet naar waarheid hebben beantwoord, het breken van contractuele clausules verlies van inkomsten als resultaat hebben. Bij aanschaf van deze software wordt de uitvoering van de motie Van Nispen inzake het gebruik van technologie in de opsporing nageleefd.[29]

V. de verantwoording

Bestendiging van beleid.

Reactie: ik zal blijven rapporteren over de hoeveelheid opsporingsonderzoeken waarin de binnendringbevoegdheid is ingezet en het gebruik van binnendringsoftware van externe leveranciers in die onderzoeken.

Spoor 3 gebruik onbekende kwetsbaarheden (meldplicht 126ffa Sv)

Introductie

De meeste software in de wereld bevat diverse kwetsbaarheden die (nog) niet bekend zijn bij de producent. Het betreft veelal onvolkomenheden in het programmeren. Sommige hiervan geven een mogelijkheid om toegang te krijgen tot een geautomatiseerd werk en kunnen worden gebruikt door opsporingsdiensten en inlichtingen- en veiligheidsdiensten, maar ook worden misbruikt door criminelen. De Nederlandse beleidslijn voor de omgang met dit soort kwetsbaarheden, vervat in de brief van 8 november 2016 (Kamerstuk 26 643, nr. 428) is kort gezegd «melden (bijvoorbeeld aan de producent van de software), tenzij» om zo software veiliger te maken. De uitzondering op de regel voor de opsporing is, via het amendement Recourt (PvdA) en Tellegen (VVD) (Kamerstuk 34 372, nr. 14), gecodificeerd in artikel 126ffa van het Wetboek van Strafvordering. De melding van een onbekende kwetsbaarheid kan worden uitgesteld bij een zwaarwegend opsporingsbelang na schriftelijke machtiging van de rechter-commissaris. Dit uitstel wordt periodiek getoetst. In de wetsge-

[29] Kamerstuk 29 628, nr. 1081; Aanhangsel Handelingen II 2022/23, nr. 1171

schiedenis is bovendien vastgelegd dat de politie daarnaast geen onbekende kwetsbaarheden inkoopt.

Er is nog vrij weinig ervaring opgedaan met onbekende kwetsbaarheden. Tot nu toe is tweemaal gebruik gemaakt van de mogelijkheid van artikel 126ffa Sv. Desalniettemin constateert het WODC in de wetsevaluatie twee knelpunten die hieronder gezamenlijk worden behandeld.

I. Onderzoek naar de effectiviteit van artikel 126ffa Sv
WODC
• 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. • Ten tweede kan de meldplicht samenwerking met nationale, maar ook internationale partijen bemoeilijken. In sommige landen is het gebruik van een kwetsbaarheid staatsgeheim. Als Nederland met dat soort landen zou willen samenwerken, is dat problematisch omdat Nederland de verplichting heeft om hetgeen staatsgeheim is in het buitenland, in Nederland te melden. Het risico hiervan is dat die kwetsbaarheid niet langer bruikbaar is en samenwerking voor die landen onaantrekkelijk wordt.
PGHR
Geen aanbevelingen

Reactie: De onthullingen afgelopen jaren uit crypto-communicatiediensten als Encrochat, SkyECC en Exclu, en de actie tegen de criminele darkwebmarket Genesis maken duidelijk dat de georganiseerde criminaliteit gebruik maakt van specifiek voor en door hen ontwikkelde software. Het is denkbaar dat dit soort software kwetsbaarheden bevat die onder de reikwijdte van 126ffa Sv kunnen vallen. Melding van deze kwetsbaarheden door opsporingsinstanties aan producenten van deze software zou criminaliteit faciliteren doordat hun software daardoor veiliger wordt. Op dit moment is de praktijk zo dat langdurig uitstel mogelijk is in deze gevallen, maar dat de uitstelverzoeken wel periodiek moeten worden herhaald. Dat brengt – gelet op de noodzaak deze gevoelige informatie goed te beschermen – mogelijk een overbodige werklast met zich mee voor de betrokken instanties.

De komende periode wordt bezien of het melden van onbekende kwetsbaarheden in software gemaakt voor en door criminelen uitgesloten kan worden van het bereik van artikel 126ffa Sv na een machtiging daartoe van de rechter-commissaris.

Een ander element dat het WODC in de wetsevaluatie heeft erkend is de omgang met artikel 126ffa Sv in de samenwerking, bijvoorbeeld met internationale partnerdiensten. Ook dit wordt nader bestudeerd. Internationale samenwerking is in de onderzoeken waarin de binnendringbevoegdheid wordt toegepast vaak van groot belang voor de bestrijding van ernstige criminaliteit.

Spoor 4 het toezicht van de Inspectie Justitie en Veiligheid en controle door het OM

Introductie[30]

De WODC-wetsevaluatie beschrijft de ervaringen met de verschillende toezicht-mechanismen op de uitvoering van de binnendringbevoegdheid. Twee instanties die zich bezighouden met dit toezicht zijn de IJenV en de PGHR. Voor de uitoefening van de binnendringbevoegdheid behoeft de officier van justitie de machtiging van de rechter-commissaris. De inzet vindt plaats onder het gezag van de speciaal aangewezen officier van justitie voor de binnendringbevoegdheid. Ten slotte kan de rechter die uitspraak doet in een strafzaak de rechtmatigheid van de inzet van de binnendringbevoegdheid beoordelen.

Het WODC noemt het in de wetsevaluatie wenselijk dat er meer duidelijkheid komt over de reikwijdte en bevoegdheden van de diverse instanties die toezicht houden. Het is voorstelbaar dat met een dergelijke hoeveelheid toezichthouders sprake is van overlap en daarmee leidt de reikwijdte van de verschillende toezichthouders tot discussie. Het WODC vermeldt overigens in de wetsevaluatie dat sprake is van een patstelling, dit wordt door beide partijen niet herkend.

Het toezicht op de binnendringbevoegdheid is zwaar en intensief wanneer men dit vergelijkt met andere bijzondere opsporingsmiddelen. Het WODC haalt in de wetsevaluatie een geïnterviewde aan die stelt dat: «het toezicht dat de Inspectie uitvoert erg intensief is, zeker in vergelijking met het toezicht op de andere politietaken. Maar de intensiteit van dit toezicht is door de wetgever bepaald. Mocht dit intensieve toezicht uiteindelijk niet wenselijk zijn, dan is de Inspectie bereid om haar toezicht anders in te richten.»[31] Het WODC concludeert in de wetsevaluatie daarover: «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 ervaart dit als lastig in verband met de ontwikkelfase waarin de uitvoering van de nieuwe bevoegdheid zich bevindt.» [32] De wetgever heeft inderdaad toentertijd nalevingstoezicht van de IJenV gevraagd, wat een intensieve vorm van toezicht is. De IJenV heeft daar kundig invulling aan gegeven. Het houden van deze vorm van toezicht was nieuw voor de IJenV en vergt veel inspanning.

[30] Dit spoor is ook relevant voor de toezegging aan de Eerste Kamer (kenmerk 171938.01U).
[31] WODC (2022) De hackbevoegdheid in de praktijk, p. 156
[32] WODC (2022) De hackbevoegdheid in de praktijk, p. 156

I. De politie stelt een visie op voor passende kwaliteitszorg
WODC wetsevaluatie
• De Inspectie JenV 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.
PGHR
• Geen aanbevelingen
WODC rechtsvergelijkend onderzoek
• Op basis van ons onderzoek nemen wij geen positie in ten aanzien van deze discussie. Wel is het relevant om te noemen dat, als ten aanzien van de hackbevoegdheid de rol van het toezicht verder wordt verkend, een aantal landen in onderhavig onderzoek naar voren is gekomen dat mogelijk handvatten kan bieden.

Reactie: in alle vier de verslagen van de IJenV is opgenomen dat het bij DIGIT ontbreekt aan een intern kwaliteitssysteem om eventuele tekortkomingen in de toepassing van de binnendringbevoegdheid tijdig te identificeren en te verhelpen. Het is voor de IJenV op deze wijze niet goed mogelijk om systeemtoezicht uit te voeren, omdat DIGIT niet beschikt over een eigen kwaliteitssysteem. Voor het opzetten van een kwaliteitssysteem zijn drie elementen van belang.

Ten eerste, hoogwaardig toezicht moet behouden blijven. Ten tweede, moet het kwaliteitssysteem passend zijn binnen de politieorganisatie en in beginsel aansluiten bij het algemene stelsel van opsporingsbevoegdheden. Ten derde moet voldoende ruimte bestaan voor het onvoorspelbare karakter van de inzet.

De beslissing voor een beweging naar systeemtoezicht past binnen de ontwikkeling die DIGIT doormaakt. In de opstartfase van deze bevoegdheid is dit intensieve toezicht nuttig gebleken aangezien bij de politie ervaring moest worden opgedaan. Door de politie en het OM is de afgelopen jaren de nodige ervaring opgedaan met de binnendringbevoegdheid. In het algemeen kan worden gesteld dat de binnendringbevoegdheid op een vakkundige, integere en rechtmatige wijze wordt ingezet. Het is nodig om nader te bepalen wat in de praktijk bij de politie georganiseerd zou moeten worden, met name gelet op de beschikbare middelen van het team en de andere door DIGIT in de wetsevaluatie naar voren gebrachte zorgen, om over te kunnen gaan op systeemtoezicht.

In dit kader kan worden vastgesteld dat het handvat dat het WODC in haar rechtsgelijkend onderzoek naar voren brengt op het terrein van toezicht niet goed aansluit op de Nederlandse situatie. In het rapport wordt gerefereerd aan een aparte externe toezichthouder of een rol voor een onderzoeksrechter op de uitvoering van de bevoegdheid. Een andere wijze van toezicht op de daadwerkelijke inzet door bijvoorbeeld de rechter-commissaris (RC) past niet bij de rol en positie van de RC bij de uitoefening van bijzondere opsporingsmiddelen. De rol en positie van de RC in Nederland is anders dan die van een onderzoeksrechter in andere landen. Voor wat betreft het toezicht op de uitvoering van een bevel door de IJenV is haar positie wettelijk vastgelegd in de Politiewet. Het beleggen

van toezicht bij een alternatieve instantie past niet in het Nederlands wettelijk kader.

Spoor 5 de keuring van technische hulpmiddelen

Introductie

Ter uitvoering van een bevel van de officier van justitie kan gebruikt gemaakt worden van een technisch hulpmiddel. Het technisch hulpmiddel betreft een stuk softwarecode die (deels) op het geautomatiseerd werk dat is binnengedrongen wordt gezet. Deze softwarecode detecteert, registreert en transporteert gegevens die relevant zijn voor het opsporingsonderzoek. De code kan met behulp van binnendringsoftware van externe leveranciers worden geplaatst, maar dat hoeft niet. Voor het gebruik van bewijs in een strafzaak is de integere, herleidbare en betrouwbare bewijsvergaring belangrijk. Of een technisch hulpmiddel hiertoe in staat is, wordt vooraf door de keuringsdienst van de politie beoordeeld en is uiteindelijk onderhevig aan het oordeel van de rechter in een strafzaak. Voor een inzet van de binnendringbevoegdheid moet op dit moment in beginsel sprake zijn van een vooraf goedgekeurd technisch hulpmiddel. Keuring achteraf is tevens mogelijk. Ook kan het voorkomen dat een technisch hulpmiddel naar zijn aard niet te keuren is. Dan zal de officier van justitie andere maatregelen moeten nemen om de integriteit van de gegevens te waarborgen en dit inzichtelijk maken aan de rechter in de uiteindelijke strafzaak. Als laatste is het mogelijk dat hulpmiddelen naar hun aard niet te keuren zijn, dit kan bijvoorbeeld het geval zijn bij technische hulpmiddelen van externe leveranciers.

Het Bogw schrijft in hoofdstukken 5, 6 en 7 verschillende eisen voor aan de keuring en het keuringsproces. Deze eisen zijn geïnspireerd op het Besluit technische hulpmiddelen strafvordering dat voor technische hulpmiddelen geldt in de opsporing in den brede, zoals voor een richtmicrofoon of een peilbaken. Echter hulpmiddelen die voor de binnendringbevoegdheid worden gebruikt verschillen in een aantal opzichten van traditionele hulpmiddelen. Technische hulpmiddelen voor de binnendringbevoegdheid worden, in een specifieke configuratie vaak voor één inzet gebruikt; gestandaardiseerde componenten moeten mogelijk worden aangepast naar aanleiding van de concrete zaak. Tevens volgen updates naar verschillende versies elkaar sneller op of deze updates hebben meer invloed op de werking van het middel dan bij traditionele technische hulpmiddelen. Daarbovenop is de context verschillend. Het binnendringen is dynamisch en de samenstelling van het geautomatiseerde werk is niet volledig voorspelbaar. Ter plekke, op dat moment, kan een technisch hulpmiddel worden geconfigureerd voor een correcte werking. Daarbovenop kan de configuratie van een technisch hulpmiddel niet altijd te reconstrueren zijn nadat een inzet heeft plaatsgevonden. Dit geldt in het bijzonder bij technische hulpmiddelen van een externe leverancier die onderdeel zijn van de software waarmee wordt binnengedrongen. Door de leverancier wordt geen inzicht in de werking van het middel gegeven, aangezien dit onderdeel is van het intellectueel eigendom. De wijze waarop het binnendringen plaatsvindt, bijvoorbeeld de wijze van het omzeilen van de beveiliging van een geautomatiseerd werk, maakt overigens geen deel uit van het keuringsproces.

In de WODC-wetsevaluatie wordt geconstateerd dat DIGIT de keuring als een groot knelpunt beschouwt. Het rechtsvergelijkend onderzoek van het WODC uit 2023 geeft goed inzicht in de redenen waarom dit het geval is. Gewezen wordt op de lange doorlooptijd van keuring. Zoals in de vorige alinea beschreven is het gebruikelijk dat software vaak wordt geüpdatet en kan dit vervolgens dezelfde lange doorlooptijd voor keuring vereisen.

Ook wordt erop gewezen dat vanuit de opsporingspraktijk vragen rijzen over het nut en de noodzakelijkheid van (het voldoen aan) alle eisen. Verder geschiedt de inzet van technische hulpmiddelen veelal in een digitale omgeving die door de politie niet volledig onder controle is, bijvoorbeeld omdat de gebruiker van het geautomatiseerd werk te allen tijde handelingen kan uitvoeren. In de praktijk zou men meer gebruik willen maken van een risicoanalyse met betrekking tot het gebruikte technisch hulpmiddel en de bewijswaarde van de verzamelde gegevens.

I. De keuringseisen worden aangepast

WODC

- 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.
- 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. In de wetsevaluatie en wordt vermeld dat deze hoogstwaarschijnlijk ook niet goedgekeurd kunnen worden.
- In de uitvoeringspraktijk wordt (ook) gebruikgemaakt van tactische aanvullende waarborgen. Deze maken geen onderdeel uit van het keuringsproces.

PGHR

- De uitvoeringspraktijk van artikel 126nba Sv staat op gespannen voet met het door de Minister van Justitie en Veiligheid (in de parlementaire geschiedenis van de Wet computercriminaliteit III en in de toelichting op het Bogw) tot uitdrukking gebrachte uitgangspunt dat bij het uitvoeren van onderzoek in een geautomatiseerd werk in beginsel gebruik wordt gemaakt van een (vooraf) goedgekeurd technisch hulpmiddel.
- Het technisch hulpmiddel waarvan de DIGIT-officier heeft geoordeeld dat het naar zijn aard niet voor keuring geschikt is, betreft een technisch hulpmiddel dat onderdeel is van een commercieel verkregen, kostbaar systeem dat in het toezichtonderzoek de codenaam «TH Brons» heeft gekregen. Het besluit van de DIGIT-officier om geheel af te zien van de keuring van TH Brons steunt op de geldende regelgeving (artikel 21 lid 4 Bogw). De afwegingen die hieraan ten grondslag liggen zijn op zichzelf zorgvuldig tot stand gekomen en verdedigbaar.

IJenV

- Ten eerste heeft de wetgever als hoofdregel gesteld dat software die ingezet wordt als technisch hulpmiddel vooraf goedgekeurd moet zijn als deze wordt ingezet. In uitzonderingsgevallen kan keuring van een technisch hulpmiddel geheel achterwege blijven, namelijk indien de aard van het technisch hulpmiddel zich naar het oordeel van de officier van justitie daartegen verzet. Gelet op het feit dat de hackbevoegdheid voor het overgrote deel van de zaken in 2022 is ingezet voor het hacken van telefoons met een niet gekeurd commercieel technisch hulpmiddel signaleert de Inspectie dat hiermee de door de wetgever voorziene uitzonderingsgevallen standaardpraktijk zijn geworden.

I. De keuringseisen worden aangepast

WODC rechtsvergelijkend onderzoek

- Voor veel landen geldt dat de hackbevoegdheid een relatief nieuwe bevoegdheid is. Daarnaast is de daarvoor benodigde digitale expertise voor veel betrokkenen relatief nieuw. Dit leidt ertoe dat wet- en regelgeving niet altijd aansluiten op de praktijk.
- Op Zweden na vindt in ieder land een vorm van keuring of toetsing plaats van het te gebruiken technisch hulpmiddel. De wijze waarop verschilt echter per land. Nederland kent de meest gedetailleerde beschreven keuring van technische hulpmiddelen.
- Op basis van de interviews blijkt dat nog weinig jurisprudentie beschikbaar is waarin de kwaliteit van de gegevens, verzameld met behulp van de hackbevoegdheid, ter discussie is gesteld. Dat maakt het lastig om de vraag te beantwoorden in welke mate een zittingsrechter de inzet van de bevoegdheid en de kwaliteit van de gegevens toetst.
- Op basis van het onderzoek zijn een drietal scenario's geformuleerd die mogelijk een aanvulling kunnen bieden op de wijze waarop in Nederland met technische hulpmiddelen en gegevens, verzameld middels de hackbevoegdheid, wordt omgegaan.

1. Broncode moet gecontroleerd kunnen worden en controle op toegangsgegevens
2. Veranderende rol toezicht (onderzoekrechter of toezichthouder)
3. Keuring op maat (risico-analyse in de keuring en borging aanvullende tactische waarborgen).

Reactie: er wordt een voorstel uitgewerkt waar in beginsel alle hulpmiddelen die gegevens automatisch detecteren, registeren en transporteren ter keuring worden aanboden bij een keuringsdienst. Echter, het uitgangspunt dat alleen goedgekeurde hulpmiddelen worden ingezet wordt verlaten. Alle middelen worden in beginsel ter keuring aangeboden zodat wordt getoetst in welke mate een hulpmiddel aan de eisen uit het Bogw voldoet. Hiervan wordt een rapport opgemaakt. Op deze manier worden de integriteit en de werking van het middel geanalyseerd en gecontroleerd door een derde partij en de relevante factoren voor de bewijswaarde worden inzichtelijk en toetsbaar gemaakt. Is het middel goedgekeurd, dan wordt een goedgekeurd middel ingezet. Als het middel niet of ten dele is goedgekeurd kan de officier van justitie bepalen of aanvullende verificatiemaatregelen moeten worden genomen als aan een eis niet of niet volledig wordt voldaan. Op die manier krijgen de rechter, verdediging en officier van justitie inzicht in de bewijswaarde in de rechtszaal van de verkregen informatie. Deze werkwijze zorgt ervoor dat middelen op een efficiënte en verantwoorde wijze kunnen worden ingezet. Keuring achteraf of het oordelen dat een hulpmiddel naar zijn aard niet te keuren is blijft mogelijk.

Dit voorstel sluit aan bij het derde scenario dat het WODC in haar rapport heeft geschetst in het rechtsvergelijkend onderzoek van 2023 en past in het Nederlandse systeem van strafvordering. De andere twee scenario's sluiten minder goed aan op de Nederlandse situatie. In de praktijk is gebleken dat leveranciers van commerciële software hun broncode niet delen.

Dit voorstel vereist een wijziging in het Bogw. Hiervoor is nader overleg nodig tussen het OM, de Landelijke Eenheid en andere betrokken partijen. Uit dit overleg kunnen ook alternatieve effectieve oplossingen voortkomen of nieuwe inzichten worden verkregen in de normstelling van de eisen zelf.

II. Uitleg technisch hulpmiddel
WODC wetsevaluatie
• Er bestaat discussie over de precieze invulling van de begrippen technisch hulpmiddel en handmatige inzet.
PGHR
• Uit het onderzoek is gebleken dat de definitie van «technisch hulpmiddel» aan dat begrip onvoldoende richting geeft en dat deze definitie zodoende – afhankelijk van de omstandigheden van het geval – ruimte laat voor uiteenlopende antwoorden op de vraag of de softwareapplicatie die (eventueel) wordt aangewend voor het verrichten van onderzoek in een geautomatiseerd werk als een technisch hulpmiddel moet worden aangemerkt. • «De meer functionele uitleg van het begrip «technisch hulpmiddel» die de onderzoekers voorstellen, heeft als voordeel dat iedere applicatie in principe ter keuring kan (moet) worden aangeboden, behoudens indien het gaat om een eenvoudig script (waarvan de werking niet hoeft te worden afgeschermd). De goedkeuring van applicaties vergemakkelijkt de afscherming ervan. De goedkeuring garandeert bovendien de betrouwbaarheid, integriteit en herleidbaarheid van de gegevens die zijn verkregen bij het onderzoek in een geautomatiseerd werk.» Aanbeveling: Het verdient aanbeveling om het begrip «technisch hulpmiddel» uit te leggen als: iedere applicatie waarmee wordt beoogd in een geautomatiseerd werk onderzoekshandelingen te verrichten en die qua complexiteit verder reikt dan een eenvoudig script waarvan de werking op zichzelf niet hoeft te worden afgeschermd.

In antwoord op de constatering van de PGHR inzake de definitie van een technisch hulpmiddel kan worden aangegeven dat in nader overleg met de betrokken actoren de definitie verder zal worden aangescherpt. In tegenstelling tot een automatische vergaring van opsporingsinformatie is het ook mogelijk om dit handmatig te doen. Uit de praktijk blijkt dat er soms een verschil van inzicht bestaat wanneer sprake is van een handmatige inzet of de beweegredenen daarvoor. Een handmatige vergaring van opsporingsinformatie kan een noodzakelijke stap zijn in het functioneren van het middel. Daarnaast kan om operationele redenen worden gekozen voor een handmatige vergaring (bijvoorbeeld om de heimelijkheid van de operatie te waarborgen). Deze keuze wordt door DIGIT in overleg met de DIGIT-officier gemaakt. Een niet ter keuring aangeboden hulpmiddel wordt overigens wel altijd getest en geverifieerd door DIGIT zelf. In deze testfase wordt het risico voor de werking van het geautomatiseerd werk waarop wordt binnengedrongen ingeschat.

Spoor 6 Procedurele of aanvullende waarborgen, vernietigen van gegevens en overige punten

Introductie

In zijn rapport wijst de PGHR op een ongerijmdheid in de regelgeving rond geheimhoudersgegevens. Het Wetboek van Strafvordering verplicht tot het vernietigen van gegevens die vallen onder het verschoningsrecht van een professionele geheimhouder. Echter, uit het Bogw vloeit voort dat er geen wijzigingen mogen worden aangebracht in de zogenoemde logbestanden en de (overige) gegevens die op een technische infrastructuur van de politie zijn opgeslagen. Ook het WODC merkt in de wetsevaluatie op dat vanuit DIGIT is aangegeven dat de wijze waarop met geheimhoudersgegevens omgegaan moet worden in strijd is met de regelgeving van de binnendringbevoegdheid. Voor de toekomst beveelt de PGHR aan mogelijk een wettelijke grondslag te geven voor een regisserende rol van de rechter-commissaris. Voor de nabije toekomst zou zo een rol al aan de rechter-commissaris kunnen worden toegekend.

Een ander element bij de vernietiging van gegevens is welke regels van toepassing zijn. Voor interceptie (stromende gegevens) bestaan bijvoorbeeld andere termijnen dan voor de vergaring van gegevens die zijn opgeslagen. Echter, indien bijvoorbeeld tijdens een inzet op een telefoon berichten binnenkomen is dat feitelijk interceptie, terwijl wanneer DIGIT een week later wederom een inzet pleegt op de telefoon deze gegevens feitelijk opgeslagen gegevens zijn. Dit levert in een onderzoek een onoverzichtelijke lappendeken van regelgeving op.

I. logging
WODC
Geen conclusie
PGHR
Geen aanbevelingen (zie *II*)
IJenV
• Ook in 2022 heeft de politie nog onvoldoende uitgewerkt hoe zij logging inricht en toepast. Controles van de logging door de politie zelf vinden op ad-hocbasis plaats. Beeldschermopnamen blijken ook begin 2022 nog niet volledig. Door de grote hoeveelheid aan logging in de vorm van beeldschermopnamen is de toepassing hiervan niet goed bruikbaar voor proactieve controledoeleinden. • Daarnaast is de handmatige verslaglegging, in de vorm van het journaal, niet in alle gevallen juist en volledig. Dit heeft gevolgen voor de juistheid van de processen-verbaal omdat de processen-verbaal gebaseerd zijn op de informatie uit het journaal. DIGIT is door het Openbaar Ministerie geïnstrueerd om minimaal te verbaliseren en maximaal te journaliseren. Hierdoor is een juist en volledig journaal van nog groter belang.

De PGHR geeft hierbij aan dat ondanks de door de IJenV geconstateerde (en door de DIGIT-officier niet betwiste) onvolkomenheden, zoals onvolledige logging, gebrekkige beeldschermopnamen en toetsaanslagenregistratie, de DIGIT-officier de toestand niet dermate zorgwekkend acht dat er aanleiding is voor ingrijpen. Dit standpunt achten de onderzoekers verdedigbaar. De bewijslogging is daarnaast wel op orde, behoudens de signalering van de problematiek van de tijdelijke opslag van de bewijslogging op een voorziening binnen TH Brons zelf. Omdat deze tijdelijke opslaglocatie in verbinding met en onder beheer van de leverancier staat, is onbevoegde toegang tot en oneigenlijk gebruik van de gegevens technisch niet uit te sluiten. In dat geval is niet aan de waarborgen voor beveiligde opslag voldaan.

Verder stelt de PGHR dat uit het onderzoek is gebleken dat de inhoud van het begrip «onregelmatigheid» in artikel 6 (en 23 en 24) Bogw aanleiding kan geven voor discussie. De DIGIT-officier hanteert in dit verband een uitleg waarin alleen die onregelmatigheden die afbreuk doen aan de betrouwbaarheid en de integriteit van de gegevens die kunnen dienen als bewijs in een strafzaak dienen te worden geverbaliseerd. Dat oordeel achten de onderzoekers goed verdedigbaar.

De IJenV vermeldt in haar verslag over 2022 dat weliswaar veel loging aanwezig is en daarmee technisch gezien sprake is van doorlopende en automatische logging op verschillende niveaus, maar dat een risicoanalyse nodig is om de logging voldoende effectief te laten zijn en het doel en het gebruik van de logging te verbeteren. De politie werkt aan een verbetering van de inrichting van de logging en zal de dialoog met betrokken partijen over voortzetten.

II. Uitbreiding van de logging bij stelselmatige observatie

WODC

Geen conclusie

PGHR

Aanbeveling: Het verdient aanbeveling tijdens het daadwerkelijk binnendringen en verrichten van onderzoekshandelingen in een geautomatiseerd werk («een actie») de locatiegegevens van het binnengedrongen geautomatiseerd werk te loggen, en indien en voor zover die actie van langere duur is daartoe een bevel stelselmatige observatie ex artikel 126g Sv af te geven met het oog op het vastleggen van de locatiegegevens die het geautomatiseerde werk in kwestie genereert.

Ik deel de opvatting van de PGHR dat het belangrijk is om vast te stellen waar een geautomatiseerd werk zich bevindt zodat een afweging kan worden gemaakt aan de hand van de Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv, indien een inzet in het buitenland plaatsvindt. De politie heeft naar aanleiding van de aanbeveling van de PGHR een aantal wijzigingen doorgevoerd om voorafgaand aan het verrichten van binnendring- of onderzoekshandelingen te bepalen waar een geautomatiseerd werk zich bevindt. Het beoogde doel van de PGHR wordt daarmee behaald, echter op een andere wijze dan door de PGHR is voorgesteld. De reden hiervoor is dat deze wijzigingen privacy vriendelijker waren dan het stelselmatig loggen van een locatie.

III. Opmaken proces-verbaal

WODC

Geen conclusie

PGHR

- Opmaken proces-verbaal: Bij het dossieronderzoek werden aanvankelijk tekortkomingen gezien, met name wat betreft de duur van de periode die is gelegen tussen het onderzoek in een geautomatiseerd werk en de verslaglegging ervan. Hoewel niet in alle zaken, is bij het vervolgonderzoek in meer recente zaken verbetering geconstateerd. Al met al blijft de betrekkelijk globale en gestandaardiseerde wijze waarop de onderzoekshandelingen van DIGIT worden omschreven problematisch. Als gevolg daarvan kunnen controle en toezicht hierop slechts zeer beperkt plaatsvinden. Naar het oordeel van de onderzoekers is een gedetailleerder proces-verbaal geboden.
  Aanbeveling: Het verdient aanbeveling het opmaken van proces-verbaal tijdiger en volledige, dat wil zeggen: voorzien van meer concrete informatie, te doen plaatsvinden. Onder andere de verslaglegging over de door DIGIT getroffen waarborgen verdient aandacht.

Reactie: de aanbeveling van de PGHR wordt overgenomen. Het OM heeft mij te kennen gegeven dat zij de aanpassingen en verbeteringen hebben doorgevoerd.

IV. De rechter-commissaris krijgt een regisserende rol in de omgang met geheimhoudersgegevens
WODC
Geen conclusie
PGHR
• Het komt de onderzoekers voor dat de hiervoor beschreven ongerijmdheid in de regelgeving de aandacht behoeft van de Minister en dat daarin niet, althans niet op langere termijn, kan worden voorzien door uitsluitend beleidsregels van het OM. De onderzoekers achten het raadzaam om in dit verband een (wettelijke) grondslag te geven aan een regisserende rol voor de rechter-commissaris. In afwachting van nieuwe regelgeving zou (ook) het OM erop kunnen aansturen de rechter-commissaris een regisserende rol toe te kennen. Aanbeveling: Het verdient aanbeveling om (eventueel in afwachting van nieuwe regelgeving) de rechter-commissaris een regisserende rol toe te kennen bij het filteren van gegevens die afkomstig zijn van geheimhouders. • De kwestie zou bovendien onderdeel moeten zijn van het bredere debat over de wijze waarop het verschoningsrecht bij de uitoefening van bijzondere opsporingsbevoegdheden in acht wordt genomen en over de methode van het (selectief) bewaren c.q. vernietigen van digitale gegevens waarop het verschoningsrecht (mogelijk) van toepassing is. • De uitvoeringspraktijk ten aanzien van geheimhoudersgegevens geeft geen aanleiding tot nadere opmerkingen behalve dat in één zaak niet voldoende duidelijk is geworden of de omgang met geheimhoudersgegevens plaatshad overeenkomstig het hiervoor omschreven beleid.
IJenV
• Specifiek voor geheimhouderinformatie concludeert de Inspectie dat de DIGIT-officier van justitie onverwijld in de praktijk in kennis wordt gesteld door DIGIT als opsporingsambtenaren per toeval kennisnemen van mogelijke geheimhouderinformatie. • Er zijn echter aan de kant van DIGIT geen processen, werkinstructies en ondersteunende systemen zoals nummerherkenning ingericht om geheimhouderinformatie te herkennen. Op grond van het Besluit bewaren en vernietigen niet-gevoegde stukken dient in ieder geval het nummerherkenningsysteem te worden toegepast als het gaat om het aftappen van communicatie. Ook dienen op grond van het Besluit onderzoek in een geautomatiseerd werk alleen de gegevens te worden overgedragen door het technisch team die van belang zijn voor het onderzoek. Geheimhouderinformatie is dit vanzelfsprekend niet. In de huidige praktijk worden alle verzamelde gegevens door DIGIT overgedragen.

Reactie: Zoals door de PGHR beschreven, is de omgang met informatie van geheimhouders bij de uitvoering van de binnendringbevoegdheid als volgt. Het DIGIT (het technisch team) zelf neemt in de regel geen kennis van de inhoud van de gegevens die bij het onderzoek in een geautomatiseerd werk worden geregistreerd. Mocht DIGIT desalniettemin tijdens een inzet tóch bekend raken met de mogelijkheid dat gegevens worden geregistreerd of ingezien waarover het verschoningsrecht zich uitstrekt, dan wordt dit onmiddellijk beëindigd en wordt de DIGIT-officier hiervan op de hoogte gesteld. Dit laatste gebeurt ook indien deze kennisname na afloop van een inzet gebeurt.

Nadat de in het bevel aangegeven informatie door DIGIT is vergaard, onderzoekt een aparte medewerker geheimhouders of zich onder de door DIGIT overgedragen dataset gegevens van geheimhouders bevinden. Zo ja, dan stelt hij de zaaksofficier hiervan op de hoogte. Vervolgens is het aan de zaaksofficier om hierover te beslissen en zo nodig de vernietiging van die gegevens te gelasten. Met dit beleid nemen de leden van het tactische team die uitvoering geven aan het opsporingsonderzoek, geen kennis van de ongefilterde gegevens en kan het tactisch team alleen al om die reden geen gebruik maken van de gegevens van geheimhouders. Het beleid voorziet derhalve in de filtering van geheimhoudersgegevens uit de gegevens die bij de procestukken worden gevoegd.

Dit beleid voorziet echter niet in de filtering van dergelijke gegevens uit de technische infrastructuur van DIGIT en uit de forensische kopieën die worden vervaardigd van de gegevensdragers waartoe DIGIT zich bij het onderzoek in een geautomatiseerd werk toegang heeft verschaft. In artikel 7 en artikel 28 Bogw staat immers dat er geen wijzigingen worden aangebracht in de inhoud van de gegevens of de logging die bij een onderzoek in een geautomatiseerd werk op een technische infrastructuur zijn vastgelegd. Deze bepalingen strekken ertoe de betrouwbaarheid, de integriteit en de herleidbaarheid van de bij dit onderzoek verkregen gegevens te garanderen. [33]

Volgens de PGHR staan artikel 7 en artikel 28 Bogw op gespannen voet met de algemeen geldende regeling in het Wetboek van Strafvordering inzake de voeging van processtukken. Deze regeling, uitgewerkt in artikel 126aa Sv en lagere regelgeving, stelt namelijk dat gegevens onmiddellijk worden vernietigd indien zij vallen onder het verschoningsrecht. In een schriftelijke reactie op het rapport van de PGHR en recent in de overlegvergadering heeft het College van procureurs-generaal aangegeven bezig te zijn met de aanbeveling en de hierboven genoemde punten van de PGHR te bestuderen. Op dit moment is het verschoningsrecht in beweging, zo blijkt ook uit de recente prejudiciële vragen die zijn gesteld.[34] Als onderdeel van de inzet op dit spoor wordt de inbreng van het OM meegenomen. De politie zal een proces inrichten om uitvoering te geven aan wijzigingen in de werkwijze die mogelijk uit dit proces voortkomen.

V. Technische infrastructuur

IJenV

- Het Besluit stelt eisen aan de (informatie)beveiliging. Ook heeft de politie zelf eisen gesteld aan de beveiliging. De voortgang van het planmatig aantoonbaar en controleerbaar op niveau brengen en houden van beheersingsmaatregelen voor de (informatie)beveiliging stagneert. Dit betekent dat, evenals voorgaande jaren, DIGIT onvoldoende is nagegaan of haar processen en systemen voldoen aan de gestelde eisen.
- De Inspectie vindt het belangrijk dat de politie, als basis voor goed systeemtoezicht, zelf zorgdraagt voor het controleerbaar en aantoonbaar treffen van passende maatregelen om beveiligingsrisico's te beheersen en de betrouwbaarheid en integriteit van de logging en de technische infrastructuur te waarborgen. Dit vormt de basis voor de politie om vanuit een eigen interne verantwoordelijkheid toe te zien op het inrichten van deze maatregelen, de structurele naleving daarvan en daarover op een controleerbare wijze verantwoording af te kunnen leggen.

Hoewel volgens de IJenV in 2022 het autorisatiebeheer nog niet op orde was, heeft de IJenV op basis van haar waarnemingen geen aanwijzingen dat zich grote technische beveiligingsrisico's in de technische infrastructuur van DIGIT hebben voorgedaan. De politie is zich erg bewust van de noodzaak van de beveiliging van de technische infrastructuur. Verschillende maatregelen zijn hierbij reeds van toepassing, zoals het feit dat de servers waarop de gegevens worden opgeslagen door de politie worden beheerd en zich in Nederland bevinden. Het verder op orde brengen van de zogenaamde plan-do-check-act-cyclus, zoals beschreven door de IJenV wordt meegenomen bij de vormgeving van het interne kwaliteitssysteem genoemd in spoor 4.

[33] PGHR (2022) Onderzoek in een geautomatiseerd werk, p. 75–79; 95–97; 127, 126; 133, 134
[34] Openbaar Ministerie en het verschoningsrecht | Nieuwsbericht | Openbaar Ministerie (om.nl); ECLI:NL:GHSHE:2023:1329

Reactie: er kunnen verschillende gegevensbewaringsregimes van toepassing zijn op data die wordt verzameld via de binnendringbevoegdheid. Een ogenschijnlijke kleine aanpassing in het ene regime kan behoorlijke gevolgen hebben in het andere. Dit punt dient daarom gerichter te worden uitgewerkt voordat kan worden besloten of, en zo ja, hoe hieraan een vervolg kan worden gegeven.

Verder kan worden toegelicht dat de gegevens die DIGIT kan vergaren omschreven wordt in het bevel. Dit kunnen omvangrijke gegevensbestanden zijn. Het gegevensbeschermingsregime dat hierop van toepassing is, is neergelegd in de Wet politiegegevens en voor zover de dataset uit het opsporingsdossier wordt overhandigd aan het OM om aan het strafdossier te worden toegevoegd geldt de Wet justitiële en strafvorderlijke gegevens.