



Inspectie Justitie en Veiligheid
Ministerie van Justitie en Veiligheid

Toetsingskader toezicht hackbevoegdheid politie

Inhoudsopgave

Inleiding	2
1 Aanwijzing opsporingsambtenaren en uitvoering door technisch team	7
2 Voorbereiding	10
3 Binnendringsoftware en melden onbekende kwetsbaarheden	13
4 Keuring technisch hulpmiddel	16
5 Uitvoering binnendringen en verrichten van onderzoekshandelingen	20
6 Gegevens vastgelegd in logbestanden (logging)	28
7 Technische infrastructuur en bewijslogging	31
8 Onregelmatigheden	34
9 Proces-verbaal.....	37
10 Bewerking en verstrekking van vastgelegde gegevens.....	39
11 Bewaartermijnen, verwijdering en vernietiging gegevens.....	40
12 Kwaliteitssysteem en interne controle.....	43
Bijlage I: Overzicht toetsingsnormen	46

Inleiding

De Wet computercriminaliteit III (hierna Wet CCIII) verschaft de politie de bevoegdheid om onder strikte voorwaarden een geautomatiseerd werk (een apparaat zoals een laptop of smartphone) dat in gebruik is bij een verdachte heimelijk en op afstand binnen te dringen en hierin onderzoek te doen. In de media wordt deze bevoegdheid de 'hackbevoegdheid' genoemd.¹ De bevoegdheid mag uitsluitend worden ingezet in geval van verdenking van een misdrijf dat een ernstige inbreuk op de rechtsorde oplevert, bij ernstige misdrijven in georganiseerd verband of bij aanwijzingen van een terroristisch misdrijf.² De introductie van deze bevoegdheid heeft maatschappelijk tot veel discussie geleid, waarbij bleek dat er spanning bestaat tussen enerzijds het belang van veilige samenleving en anderzijds het recht op privacy. Hierbij werd gesteld dat de politie de hackbevoegdheid nodig heeft voor het bestrijden van de steeds meer gedigitaliseerde criminaliteit. Tegelijkertijd was er bezorgdheid dat de politie te pas en te onpas binnendringt in systemen en op grote schaal de privacy van burgers schendt. Daarnaast zouden veiligheidsrisico's kunnen ontstaan als de politie kwetsbaarheden laat bestaan, in plaats van deze bij de producent te melden. Ook werd opgemerkt dat een hack door de politie kan leiden tot nevenschade, bijvoorbeeld aan de digitale infrastructuur.

De wetgever hecht grote waarde aan een rechtmatige en zorgvuldige inzet van deze bevoegdheid. Dit is belangrijk om de inbreuk op de privacy van de betrokkenen zoveel mogelijk te beperken en de betrouwbaarheid van de vergaarde gegevens te waarborgen. Door de wetgever zijn regels gesteld om dit doel te bereiken. De wetgever heeft daarbij tevens voorzien in een stelsel van maatregelen van controle en toezicht om de naleving van deze regels te waarborgen. Als onderdeel van dat stelsel is een rol weggelegd voor de Inspectie Justitie en Veiligheid (hierna: de Inspectie). De Inspectie is op grond van de Politiewet 2012 belast met het toezicht op de kwaliteit van de taakuitvoering door de politie.³ Het toezicht door de Inspectie op de uitvoering van het bevel van de officier van justitie en op de naleving van de wet- en regelgeving rond de toepassing van de hackbevoegdheid is verder verankerd in het Wetboek van Strafvordering⁴ en het Besluit onderzoek in een geautomatiseerd werk (hierna: *Bogw* of *Besluit*).⁵ Hierbij is tevens geregeld dat het toezicht van de Inspectie zich ook richt op de buitengewoon opsporingsambtenaren en bijzondere opsporingsdiensten.⁶

¹ Daar waar de term "de bevoegdheid" of "hackbevoegdheid" wordt genoemd, wordt bedoeld op de bevoegdheid om een geautomatiseerd werk dat in gebruik is bij een verdachte heimelijk en op afstand binnen te dringen en hierin onderzoek te doen.

² Zie artt. 126nba, 126uba en 126zpa Wetboek van Strafvordering.

³ Art. 65 Politiewet 2012.

⁴ Zie art. 126nba, zevende lid, Wetboek van Strafvordering.

⁵ Volledig: Besluit van 28 september 2018, houdende regels over de uitoefening van de bevoegdheid tot het binnendringen in een geautomatiseerd werk en het al dan niet met een technisch hulpmiddel onderzoek doen als bedoeld in artt. 126nba, eerste lid, 126uba, eerste lid, en 126zpa, eerste lid van het Wetboek van Strafvordering (Besluit onderzoek in een geautomatiseerd werk), Stb. 2018, 340. De wettelijke grondslag van dit besluit is gelegen in artt. 126nba lid 1 en lid 8, 126uba lid 1 en lid 3, 126zpa lid 1 en lid 3, 126ee Wetboek van Strafvordering, en art. 18 lid 1 van de Wet politiegegevens.

⁶ Art. 126nba, 7e lid, wetboek van Strafvordering; Staatsblad 2018, nr. 340, p.23 en p.49, nota van toelichting bij het Besluit onderzoek in een geautomatiseerd werk dat op 9 oktober 2018 in het Staatsblad is gepubliceerd.

De Inspectie doet jaarlijks verslag van haar bevindingen naar aanleiding van dit toezicht. Sinds de introductie van deze bevoegdheid in 2019 heeft de Inspectie jaarlijks verslag gedaan. In het kader van het toezicht op de wettelijke hackbevoegdheid van de politie maakt de Inspectie gebruik van een toetsingskader, zodat het inzichtelijk is waaraan de Inspectie toetst. In 2018 is bij het vormgeven van het toezicht een toetsingskader opgesteld en voorgelegd aan de politie. Het in 2018 opgestelde toetsingskader is gebaseerd op het toepasselijke rechtskader, waaronder (toelichting bij) de Wet CCIII, het Bogw en verslagen van parlementaire behandelingen hiervan. In het destijds opgestelde toetsingskader is de context en herkomst van de normen niet voor alle onderdelen geëxpliciteerd. Om zoveel mogelijk transparantie te bieden, heeft de Inspectie haar toetsingskader in het onderhavige document nader uitgewerkt, inclusief een beschrijving van de context en herkomst van de normen. Een eerdere conceptversie van dit document is ter consultatie voorgelegd aan de Nationale Politie.

Afbakening

Het toezicht door de Inspectie is gericht op het functioneren van het wettelijk systeem rond de uitvoering van een bevel tot onderzoek in een geautomatiseerd werk door de politie.⁷ De uitvoering van de hackbevoegdheid door de politie is centraal belegd bij één technisch team: het Digital Intrusion Team (DIGIT) van de Landelijke Eenheid van de Nationale Politie.⁸ Naast politieambtenaren kunnen opsporingsambtenaren van de Koninklijke Marechaussee en opsporingsambtenaren van de bijzondere opsporingsdiensten onderdeel vormen van dit team. Het toezicht door de Inspectie richt zich op de uitvoering door dit team.

Het toezicht omvat zowel de gevallen die de officier van justitie in het kader van strafvervolgning aan de rechter voorlegt als gevallen die niet tot strafvervolgning leiden.⁹

Concreet heeft het toezicht van de Inspectie betrekking op aspecten als de autorisaties van de opsporingsambtenaren voor handelingen ter uitvoering van een bevel van de officier van justitie, de expertise en kennis van de betrokken opsporingsambtenaren, de logging van gegevens over de uitvoering van een bevel, de inzet van een technisch hulpmiddel, de vastlegging van de met een technisch hulpmiddel geregistreerde gegevens op een technische infrastructuur, de beveiliging van gegevens en het gebruik van de gegevens, inclusief de bewaring en vernietiging daarvan.¹⁰ De logging over de uitvoering van een bevel speelt een belangrijke rol bij het toezicht. Daarnaast kan ook steekproefsgewijs toezicht plaatsvinden tijdens het binnendringen in een geautomatiseerd werk en het doen van onderzoek in de praktijk.¹¹

⁷ *Kamerstukken II 2016/17*, 34 372, nr.6 p. 106. Het systeemtoezicht wordt uitgeoefend op de uitvoering van de wettelijke regels in de praktijk.

⁸ Bogw, nota van toelichting, pagina 14. "Gelet op de bijzondere expertise en de technische voorzieningen die nodig zijn voor het uitvoeren van onderzoek in een geautomatiseerd werk wordt, in ieder geval gedurende de beginfase, de organisatie van de technische teams centraal belegd binnen de politieorganisatie. Binnen de Landelijke Eenheid van de Nationale Politie worden één of meer technische teams ingericht die worden belast met het onderzoek in een geautomatiseerd werk. Deze teams voeren dit onderzoek uit ten behoeve van de politie, de KMar en de bijzondere opsporingsdiensten."; Bogw, art. 1h definitie technisch team: Onderdeel van de Landelijke eenheid dat kan worden belast met de uitvoering van een bevel.

⁹ Bogw, nota van toelichting, hoofdstuk 5 (toezicht) p. 23; *Kamerstukken II 2016/17*, 34 372, nr.6, p.82.

¹⁰ *Kamerstukken II 2016/17*, 34 372, nr.6, p.82 en Eerste Kamer, vergaderjaar 2016/17, 34 372, D, p 32.

¹¹ Bogw, nota van toelichting, hoofdstuk 5 (toezicht) p. 23.

De Inspectie JenV houdt tevens toezicht op de naleving van de regels en procedures voor de keuring en inzet van software waarmee op apparaten gegevens worden verzameld en de vastlegging van gegevens op een beveiligde technische infrastructuur.¹²

Rechtskader

In de toepasselijke wet- en regelgeving en in verslagen van de parlementaire behandeling daarvan zijn regels opgenomen over het binnendringen en het doen van onderzoek in een geautomatiseerd werk. Essentie van dit rechtskader is enerzijds te waarborgen dat het tijdens het onderzoek vergaarde gegevens die kunnen dienen als bewijs in een strafzaak betrouwbaar, integer en herleidbaar zijn. En anderzijds dat de inbreuk op de privacy van de betrokkenen zoveel mogelijk wordt beperkt.

De kern van het toepasselijke rechtskader wordt gevormd door de Wet CCIII en het Bogw. Voor de nadere duiding van de hierin opgenomen regels en hun bedoeling maakt de Inspectie gebruik van toelichtingen en verslagen van parlementaire overleggen. Tijdens de parlementaire behandeling zijn diverse discussies gevoerd waarbij de minister en de staatssecretaris van het ministerie van Justitie en Veiligheid toezeggingen en uitspraken hebben gedaan. Indien de politie van het rechtskader afwijkt, maakt de Inspectie in de rapportage expliciet duidelijk aan welke regels, toezegging of uitspraak de norm is ontleend. De Inspectie kan hierbij aangeven aan welk risico deze toezegging of uitspraak eerder is gekoppeld tijdens de parlementaire behandeling. In het toetsingskader is de herkomst van het gehanteerde rechtskader inzichtelijk gemaakt.

Het evalueren van de effectiviteit van de wet en de uitvoerbaarheid van de regels valt buiten de reikwijdte van het toezicht door de Inspectie.

Kwaliteit van de taakuitvoering

Bij het toezicht op de kwaliteit van de taakuitvoering door de politie betreft de Inspectie de voor de politie geldende regels, inclusief de randvoorwaarden die nodig zijn om daaraan te kunnen voldoen. Een juiste, tijdige, volledige, aantoonbare en controleerbare uitvoering van de bevoegdheid en het daarover mede door middel van eigen controles kunnen afleggen van verantwoording zijn belangrijke kwaliteitsaspecten.

De grondslag van de normen en de wijze hoe de Inspectie daarmee tijdens het toezicht omgaat, is in het voorliggende toetsingskader aangegeven. De Inspectie zal de grondslag tevens bij haar bevindingen inzichtelijk maken in de rapportages.

Aanwijzingen door het Openbaar Ministerie

De zaakofficier van justitie heeft de leiding en de eindverantwoordelijkheid over het opsporingsonderzoek waarin de hackbevoegdheid wordt ingezet.¹³ De landelijk officier van justitie voor Digital Intrusion (hierna: DIGIT officier van justitie) heeft de leiding

¹² Bogw, nota van toelichting, paragraaf 3.5 p.20 en artikelsgewijze toelichting hoofdstuk 5 p.37 "De Inspectie JenV houdt toezicht op de naleving van de technische eisen en de keuringsprocedure."; Eerste Kamer, 2017-2018, 34 372 G, nadere memorie van antwoord, ontvangen 4 mei 2018, p. 14.

¹³ Artt. 132a en 148 Wetboek van Strafvordering.

over en is verantwoordelijk voor de uitvoering van het bevel door het technisch team.¹⁴ De officier van justitie kan aanwijzingen geven aan de politie.¹⁵

Indien de Inspectie constateert dat de politie afwijkt van het rechtskader, zal de Inspectie nagaan of dit op aanwijzing van de officier van justitie is gebeurd. Indien dit het geval is, kan de Inspectie onderzoeken of de politie gehandeld heeft conform deze aanwijzing. De Inspectie zal in haar verslag hierover signalerend rapporteren door eerst te verwijzen naar de betreffende regels uit het rechtskader en het hiermee beoogde te beschermen belang, om vervolgens haar feitelijke observatie te beschrijven. Het oordelen over het handelen van de officier van justitie valt buiten de toezichtbevoegdheid van de Inspectie.

Ten aanzien van de betrouwbaarheid, integriteit en herleidbaarheid van de door het technisch team van de politie verkregen gegevens kan de Inspectie risico's benoemen, waarbij aangetekend wordt dat de uiteindelijke oordeelsvorming en de beslissing of deze gegevens betrouwbaar genoeg zijn voor het gebruik in een strafzaak aan de officier van justitie en uiteindelijk de rechter is.

De Inspectie kan in aanraking komen met mogelijke schendingen van de wettelijke voorschriften door of in opdracht van een officier van justitie. Indien dit zich voordoet, kan de Inspectie de procureur-generaal van de Hoge Raad (PG-HR) informeren.¹⁶

De Inspectie benadrukt dat de toetsing en oordeelsvorming door het Openbaar Ministerie en de rechter-commissaris buiten de reikwijdte van het toezicht door de Inspectie JenV vallen.¹⁷ Dit houdt in dat de Inspectie niet oordeelt over:

- beslissingen die een officier van justitie neemt;
- de afweging van een officier van justitie of het onderzoeksbelang dringend vordert dat een niet gekeurd technisch hulpmiddel wordt ingezet;
- het oordeel van een officier van justitie dat een technisch hulpmiddel zich naar zijn aard verzet tegen keuring;
- een toets op het wettelijke vereiste van een dringend onderzoeksbelang als voorwaarde voor toepassing van de hackbevoegdheid (ernstige inbreuk op rechtsorde, proportionaliteit, subsidiariteit ¹⁸);
- het afgeven van de machtiging door de rechter-commissaris;
- het advies van de Centrale toetsingscommissie (CTC)¹⁹;
- de toestemming voor de inzet van de opsporingsbevoegdheid van het College van procureurs-generaal;
- de beoordeling of het met de hackbevoegdheid verkregen bewijs betrouwbaar genoeg is om in te brengen in een strafzaak. De Inspectie kan wel risico's signaleren voor de betrouwbaarheid van de vastgelegde gegevens.

¹⁴ Instructie voor de inzet van de bevoegdheid ex. artt. 126nba, 126uba, 126zpa en 126ffa Sv (2021I002)

¹⁵ Art. 12 lid 2 Politiewet 2012.

¹⁶ *Kamerstukken II* 2016-2017, 34 372, nr.6, p. 83.

¹⁷ *Kamerstukken II* 2016/17, 34 372, nr.6, p.82; Eerste Kamer, vergaderjaar 2016/17, 34 372, D, pagina 8 en 30; Eerste Kamer, vergaderjaar 2016/17, 34 372, D, pagina 8 en 30.

¹⁸ *Kamerstukken II* 2017-2018, 34 372 nr.27 p.13; *Kamerstukken II* 2016/17, 34 372, nr.6 p. 83.

¹⁹ De CTC, samengesteld uit leden van het openbaar ministerie en politie, is een intern adviesorgaan van het openbaar ministerie, dat het College adviseert omtrent de voorgenomen inzet van bepaalde bijzondere opsporingsbevoegdheden en methodieken.

Leeswijzer

De navolgende hoofdstukken bevatten het eigenlijke toetsingskader. De volgorde van de hoofdstukken sluit zoveel mogelijk aan bij het procesverloop van de toepassing van de hackbevoegdheid zoals dat is beschreven in de nota van toelichting bij het Bogw. Per norm is eerst gespecificeerd tegen welke criteria wordt getoetst en aan welke bron uit het rechtskader deze zijn ontleend. Voor de normen waarbij dit van toepassing is, zijn tevens duidingen en randvoorwaarden opgenomen die de Inspectie in haar toezicht hanteert. Vervolgens is de hieruit afgeleide norm opgenomen in een blauw vlak, met daarin N van 'norm' gevolgd door een volgnummer en de normtekst. Bijlage I geeft een overzicht van alle in het document opgenomen toetsingsnormen per hoofdstuk.

Een deel van de toetsingsnormen in dit toetsingskader is direct en eenduidig toetsbaar. Andere toetsingsnormen hebben een meer open karakter. Bij het toetsen van deze meer open normen, maakt de Inspectie waar mogelijk gebruik van best practices. Best practices zijn kaders die zich in de praktijk hebben bewezen en breed worden geaccepteerd. Bij de toetsing van deze meer open normen hanteert de Inspectie 'professional judgement': zij past de verzamelde kennis en ervaring van de inspecteurs toe.

1 Aanwijzing opsporingsambtenaren en uitvoering door technisch team

Door het onderzoek in een geautomatiseerd werk voor te behouden aan opsporingsambtenaren die beschikken over specialistische kennis en vaardigheden op het terrein van ICT kan de kwaliteit en professionaliteit van het onderzoek worden geborgd.²⁰

Het Besluit stelt daartoe regels aan de opsporingsambtenaren die uitvoering mogen geven aan de bevoegdheid voor het binnendringen en het doen van onderzoek in een geautomatiseerd werk. Een opsporingsambtenaar moet allereerst aangewezen zijn door zijn werkgever voor het binnendringen in een geautomatiseerd werk en het, al dan niet met een technisch hulpmiddel, verrichten van onderzoekshandelingen.²¹ In het Besluit is onderscheid gemaakt in leden en deelnemers van een technisch team. Ook deelnemers moeten door de werkgever aangewezen worden voor het mogen toepassen van de bevoegdheid.²²

N1 *De opsporingsambtenaren die belast worden met het binnendringen en het uitvoeren van onderzoekshandelingen zijn daartoe door hun werkgever aangewezen.*

Alleen opsporingsambtenaren die onderdeel vormen van een technisch team mogen belast worden met de uitvoering van deze bevoegdheid.²³ Binnen de Landelijke Eenheid worden één of meer technische teams ingericht die kunnen worden belast met het binnendringen in een geautomatiseerd werk en het verrichten van onderzoekshandelingen. Deze teams voeren het onderzoek in een geautomatiseerd werk uit ten behoeve van de politie, de Koninklijke Marechaussee en de bijzondere opsporingsdiensten.²⁴

N2 *Binnen de Landelijke Eenheid zijn een of meer technische teams ingericht die zijn belast met het binnendringen in een geautomatiseerd werk en het verrichten van onderzoekshandelingen.*

Een opsporingsambtenaar kan lid worden van een technisch team indien hij voldoet aan de benodigde kwalificaties waaronder deskundigheid- en ervaringsvereisten.²⁵ Deze vereisten voor leden van een technisch team zijn vastgelegd in de regeling *kwalificaties opsporingsambtenaren*.²⁶ In de regeling is onder meer aangegeven dat de leden van het technisch team dienen te beschikken over een certificaat van een specialistische technische opleiding en aanvullende cursussen op het gebied van de

²⁰ Bogw, nota van toelichting, hoofdstuk 3.2 pagina 13.

²¹ Bogw artikel 3 eerste lid. De strekking van artikel 3 Bogw is de aanwijzing van opsporingsambtenaren en lidmaatschap van een technisch team.

²² Zie artikel 4 eerste lid Bogw (incidentele samenwerking) met verwijzing naar aanwijzing op basis van artikel 3 eerste lid Bogw.

²³ Art. 3 tweede lid Bogw.

²⁴ Bogw, nota van toelichting, artikelsgewijze toelichting, artikel 3, p. 35.

²⁵ Art. 3 derde lid Bogw.

²⁶ Regeling van de minister van Justitie en Veiligheid van 15 februari 2019, kenmerk 2429311, houdende regels betreffende de kwalificaties van opsporingsambtenaren die door de korpschef kunnen worden aangewezen als lid van een technisch team.

Wet CCIII gevolgd moeten hebben.²⁷ De deskundigheid van betrokken opsporingsambtenaren is van essentieel belang voor de inschatting, beheersing en beperking van de risico's voor het geautomatiseerde werk.²⁸ Tevens is in de regeling aangegeven dat de leden van een technisch team een vertrouwensfunctie bekleden, waarvoor een veiligheidsonderzoek vereist is.

N3 Een opsporingsambtenaar wordt door de korpschef aangewezen als lid van een technisch team als de opsporingsambtenaar voldoet aan de vereiste (opleidings)kwalificaties.

Naast leden kunnen door de korpschef zogenaamde deelnemers aangewezen en toegevoegd worden aan een technisch team.²⁹ Deelnemers worden volgens het Besluit alleen op incidentele basis voor de duur van het bevel in een concrete zaak aangewezen.³⁰ Daarnaast dient een deelnemer volgens het Besluit te beschikken over specifieke kennis en vaardigheden, benodigd voor de uitvoering van een bevel in een concrete zaak.³¹

N4 Een opsporingsambtenaar wordt door de korpschef op een incidentele basis aangewezen als deelnemer aan een technisch team voor de duur van de uitvoering van het bevel in een concrete zaak indien hij beschikt over specifieke kennis en vaardigheden, benodigd voor de uitvoering van dat bevel.

De opsporingsambtenaren die verantwoordelijk zijn voor de voorbereiding en de uitvoering van het onderzoek in een geautomatiseerd werk maken deel uit van een *technisch team*. De resultaten van de onderzoekshandelingen worden ter beschikking gesteld aan de opsporingsambtenaren die zijn betrokken bij het operationele onderzoek, ook wel aangeduid als het *tactisch team*.³² Om het risico van tunnelvisie te beperken moet volgens het Besluit gedurende het opsporingsonderzoek een strikte taakverdeling en functiescheiding tussen het technisch en het tactisch team aanwezig zijn.³³ De samenwerking moet dusdanig plaatsvinden dat het tactisch team geen enkele invloed kan uitoefenen op het binnendringen in het geautomatiseerde werk en de plaatsing, inzet en verwijdering van een technisch hulpmiddel of eigenstandig de werking van de software te beïnvloeden.³⁴ De opsporingsambtenaren van een technisch team behoren niet tot het opsporingsteam dat het tactisch onderzoek verricht. Tevens hebben de tactisch opsporingsambtenaren geen toegang tot de

²⁷ In de toelichting op de regeling kwalificaties opsporingsambtenaren technisch team is een certificaat van de opleiding OSCP, OSWP of OSCE als vereiste vastgelegd. Daarnaast dienen leden deelgenomen te hebben aan de politiecursus 'BOB en CCIII' of de cursus 'Wet Computercriminaliteit III' van de Bijzonder strafrechtacademie (of een vergelijkbare aanbieder).

²⁸ Bogw, nota van toelichting, artikelsgewijze toelichting art. 14, p.41.

²⁹ Art. 4 eerste lid Bogw (incidentele samenwerking).

³⁰ Art. 4 tweede lid Bogw (incidentele samenwerking).

³¹ Art. 4 tweede lid Bogw (incidentele samenwerking) en artikelsgewijze toelichting op het Besluit, artikel 4 p. 35. "Hierbij kan worden gedacht aan de situatie dat een opsporingsambtenaar van een bijzondere opsporingsdienst met specifieke kennis op het gebied van digitale fraude wordt toegevoegd aan een technisch team in verband met gewenste technische expertise op dit gebied in een bepaald onderzoek." Kamerstuk 34372 nr.27 p.8 heeft het over "...ter versterking van de technische expertise van een technisch team in een concrete zaak". Hieruit kan afgeleid worden dat het specifieke kennis betreft, waarover leden van het technisch team niet beschikken.

³² Bogw, nota van toelichting p.14; Kamerstukken II 2015/16, 34 372 nr.3 p.14.

³³ Kamerstukken II 2016/17, 34 372 nr.6, p.28. Vanwege de functiescheiding wordt het onderzoek in een geautomatiseerd werk uitgevoerd door speciaal daarvoor opgeleide opsporingsambtenaren die niet betrokken zijn bij het betreffende opsporingsonderzoek.

³⁴ Bogw, nota van toelichting, p.17. "De organisatorische scheiding tussen het technische team en het tactische team behoeft de samenwerking tussen de teams gedurende het opsporingsonderzoek niet te belemmeren. De officier van justitie onder wiens leiding het opsporingsonderzoek plaatsvindt, vervult hierbij een schakelfunctie."; Bogw, nota van toelichting, p. 36; Kamerstukken II 2016/17, 34 372, nr. 6 p.40 en p.59.

technische infrastructuur waar de tijdens onderzoekhandelingen verkregen gegevens door het technisch team zijn vastgelegd.³⁵

N5 Er is sprake van een strikte functiescheiding tussen het technisch team en het tactisch team.

³⁵ Bogw, nota van toelichting, p.20; *Kamerstukken II* 2016/17, 34 372, nr.6, p.52.

2 Voorbereiding

De voorbereiding van het onderzoek in een geautomatiseerd werk start met een projectvoorstel³⁶ van een tactisch team aan de officier van justitie, waarin het onderzoek in een specifieke zaak wordt voorgesteld. Vervolgens vraagt de officier van justitie een technisch team om advies over de haalbaarheid van het onderzoek.³⁷ Het rapport haalbaarheidsonderzoek wordt ter voorbereiding van een bevel opgesteld door het technisch team, op basis van de intakegegevens en overige relevante gegevens. In het haalbaarheidsonderzoek wordt het plan van aanpak voor de uitvoering van een onderzoek in het geautomatiseerde werk uitgewerkt. Tevens wordt in het haalbaarheidsonderzoek aangegeven welke bevelen nodig zijn en wordt aandacht besteed aan de inschatting en beheersing van risico's. Dit betreft risico's t.a.v. de inbreuk op de persoonlijke levenssfeer van de verdachte, de gevolgen voor het geautomatiseerde werk, de kans op nadeel of schade bij derden, maar ook de kans op ontdekking van de inzet van het technisch team door de betrokkene.³⁸ Ook wordt in het haalbaarheidsonderzoek de effectiviteit van beschikbare middelen afgewogen, of daartoe een technisch hulpmiddel wordt ingezet en is opgenomen of en zo ja welke software van derden voor het binnendringen moet worden aangeschaft.³⁹ Het rapport haalbaarheidsonderzoek wordt door de officier van justitie gebruikt voor het verkrijgen van toestemming voor de inzet van de opsporingsbevoegdheid van het College van procureurs-generaal en de voorafgaande machtiging van de rechter-commissaris.⁴⁰

N6 Het technisch team stelt op basis van de intakegegevens en overige relevante gegevens een rapport haalbaarheidsonderzoek (advies) op, op basis waarvan de OvJ een inschatting van de beheersing en beperking van risico's voor het geautomatiseerde werk kan maken.

³⁶ Het besluit spreekt ook wel over projectplan; in de praktijk een proces-verbaal van aanvraag van een tactisch team. Een dergelijk plan kan afkomstig zijn van tactisch researchteams van de politie, van de KMar of van een bijzondere opsporingsdienst.

³⁷ Bogw, nota van toelichting, p. 14; *Kamerstukken II* 2016/17, 34 372, nr. 6, p.61: "Voor de inschatting, beheersing en beperking van de risico's voor het systeem is de deskundigheid van de opsporingsambtenaren van het technisch team van essentieel belang."

³⁸ *Kamerstukken II* 2015/16, 34 372 nr.3 p. 33.

³⁹ *Kamerstukken II* 2018/19, 34 372, nr. 29, p.10; Bogw, nota van toelichting, p. 16 en p. 44.

⁴⁰ Bogw, nota van toelichting, p. 16.

Het onderzoek in een geautomatiseerde werk kan worden uitgevoerd, zodra daartoe, na voorafgaande toestemmingen en besluitvorming, door de officier van justitie een bevel is afgegeven. Zie hoofdstuk 5 voor een toelichting op de totstandkoming en kenmerken van het bevel. In de toelichting bij het Besluit is beschreven dat het technisch team na afgifte van een bevel allereerst een technische voorverkenning uitvoert, waaruit onder meer moet blijken of het geautomatiseerde werk in gebruik is bij de verdachte.⁴¹ Na een analyse hiervan wordt een plan van aanpak opgesteld voor het binnendringen in het geautomatiseerde werk.⁴² In parlementaire stukken is aangegeven dat hierin aandacht wordt besteed aan:

- de wijze van binnendringen (aangezien dit geen onderdeel uitmaakt van het keuringsproces, zie hoofdstuk 4);⁴³
- de bruikbaarheid van binnendringingssoftware (zie hoofdstuk 3);⁴⁴
- afstemming van de methode van binnendringen op het geautomatiseerde werk in kwestie.⁴⁵ Bij de keuze van de methode van binnendringen zijn naast proportionaliteit, en subsidiariteit, aspecten als de effectiviteit van de inzet, de kans op onderkenning en het risico op gevolgschade van belang.⁴⁶

In een parlementair stuk is aangegeven dat voorafgaand aan de inzet ook de werking van een technisch hulpmiddel moet worden gecontroleerd in een testomgeving om het risico op schade voor derden tot een minimum te beperken.⁴⁷ Dit testen wordt, zonder een verband te leggen met keuring, gezien als aanvulling op het onderzochte risico in het haalbaarheidsonderzoek.

De politie probeert het geautomatiseerde werk zoveel mogelijk in de oorspronkelijke staat achter te laten, dat wil zeggen als ware de bevoegdheid nooit toegepast.⁴⁸ Het ligt voor de hand om al tijdens de voorbereiding hier aandacht aan te besteden in het plan van aanpak voor het binnendringen.

De minister heeft bij de beantwoording van vragen bij de behandeling van het wetsvoorstel voor de Wet CCIII aangegeven dat het plaatsen en verwijderen van een technisch hulpmiddel onderdeel vormt van het binnendringen.⁴⁹ Gelet op de doelstelling dat het geautomatiseerde werk in oorspronkelijke staat achtergelaten moet worden, is het van belang dat risico's ten aanzien van dat doel door plaatsing en verwijdering van een technisch hulpmiddel beperkt zijn. In het keuringsprotocol (zie hoofdstuk 4) wordt niet ingegaan op plaatsing en verwijdering van het technisch hulpmiddel. Derhalve ligt het voor de hand dat het technisch team tijdens de voorbereiding zelf aandacht besteedt aan deze risico's en hier op ingaat in het plan van aanpak. De Inspectie beziet vanuit het toezicht op de kwaliteit van de taakuitvoering in hoeverre de politie deze risico's beperkt heeft.

⁴¹ *Kamerstukken II 2017/18*, 34 372 nr.27.

⁴² Bogw, nota van toelichting, p. 16.

⁴³ *Kamerstukken II 2018/19*, 34 372 nr.29 p. 13; Bogw, nota van toelichting p. 18.

⁴⁴ *Kamerstukken I 2017/18*, 34 372 nr. G p.15.

⁴⁵ *Kamerstukken II 2016/17*, 34 372, nr.6 p.11. De methode voor het binnendringen moet nauwkeurig worden afgestemd op het geautomatiseerde werk in kwestie.

⁴⁶ *Kamerstukken II 2016/17*, 34 372, nr.6 p. 38.

⁴⁷ *Kamerstukken I 2018/19*, 34 372 nr. L p.9.

⁴⁸ *Kamerstukken II 2016/17*, 34 372 nr. 6, p.76.

⁴⁹ *Kamerstukken II 2016/17*, 34 372 nr.6, p.63 en p.70. Het verrichten van onderzoekshandelingen heeft betrekking op de verschillende bevoegdheden die zijn aangeduid in het voorgestelde artikel nba/uba/zpa, eerste lid, onderdelen a. tot en met e.

De gekozen aanpak wordt vervolgens door het technisch team getest in een proefopstelling.⁵⁰ Met het testen kan onderzocht worden wat het effect is op onderkenning van het onderzoek en hoe de kans daarop beperkt kan worden en van welke eventuele gevolgschade door het binnendringen sprake is. Ook kan getest worden wat het effect van het binnendringen is en in hoeverre daarbij het geautomatiseerde werk na afloop in oorspronkelijke staat achtergelaten kan worden. Een kwaliteitsaspect voor het controlebaar en betrouwbaar uitvoeren van testen is de aanwezigheid van een testplan, een representatieve testomgeving en van vastlegging van de resultaten van de uitgevoerde test.⁵¹

N7 Het technisch team stelt een plan van aanpak op voor het binnendringen in het geautomatiseerd werk en test dit in een proefopstelling.

⁵⁰ *Kamerstukken I 2018/2019 34 372.* In het verslag van de plenaire vergadering van de eerste kamer 19 juni 2018 is aangegeven dat de gekozen methode in de proefopstelling wordt getest. Dan wordt gekeken of alles werkt zoals het zou moeten. En als een technisch hulpmiddel wordt gebruikt, wordt gekeken of het correct kan worden ingesteld en ook nog of de werking geen onbedoelde neveneffecten heeft.

⁵¹ De Inspectie benadert dit vanuit haar toezicht op de kwaliteit van de taakuitvoering door de politie.

3 Binnendringsoftware en melden onbekende kwetsbaarheden

Om in een geautomatiseerd werk binnen te dringen kan het technisch team gebruik maken van binnendringsoftware die bijvoorbeeld gebruik maakt van kwetsbaarheden in software op het apparaat van de verdachte.⁵² Het technisch team kan daartoe binnendringsoftware inkopen bij een leverancier. In het Regeerakkoord 2017-2021 en in het Besluit is opgenomen dat deze zogenaamde commerciële binnendringsoftware van derden alleen zal worden aangeschaft als daartoe in een specifieke zaak een noodzaak bestaat. Aan de inzet van deze commerciële binnendringsoftware zijn strenge voorwaarden verbonden:

- a) Commerciële binnendringsoftware mag uitsluitend worden ingezet indien minder ingrijpende middelen niet toereikend zijn.⁵³ Dit oordeel wordt gevormd door de officier van justitie en getoetst door de rechter-commissaris.⁵⁴
- b) Een product of licentie wordt pas ingekocht na centrale toetsing door het OM, waarbij hergebruik na het onderzoek niet mogelijk is omdat het softwarepakket wordt verwijderd of de licentie is verbruikt.⁵⁵ Uit de parlementaire behandeling blijkt dat de eis tot de aanschaf van licenties in een zaak is bedoeld voor het zo min mogelijk stimuleren van de markt voor dit soort kwetsbaarheden en de daaraan verbonden negatieve gevolgen voor de veiligheid van het internet.⁵⁶
- c) De leverancier is gescreend door de Algemene Inlichtingen- en Veiligheidsdienst (AIVD). In parlementaire stukken is niet uitgewerkt op welke aspecten de leverancier door de AIVD wordt gescreend. Deze screening is anders van inhoud dan de veiligheidsonderzoeken die de AIVD uitvoert voor personen die een vertrouwensfunctie (gaan) vervullen.
- d) De leverancier levert niet aan dubieuze regimes. Het gaat dan om landen die zich schuldig maken aan ernstige schendingen van mensenrechten of internationaal humanitair recht.⁵⁷ Om deze reden voert de politie een toets uit voordat over wordt gegaan tot de aanschaf van de software. In deze toets wordt de leverancier gevraagd niet te hebben geleverd aan landen waartegen vanuit de EU of de VN restrictieve sancties bestaan en wordt gecontroleerd of in het land waar de leverancier is gevestigd een exportcontroleregime bestaat waar mensenrechten een onderdeel is in de beoordeling voor het verstrekken van een exportvergunning.⁵⁸
- e) Het functioneren van de software wordt gecontroleerd in een testomgeving.⁵⁹ Dit is onder meer van belang met het oog op het voorkomen van schade aan derden.

⁵² *Kamerstukken II 2015/16*, 34 372, nr. 3. p.34. Tevens kan handmatig worden binnengedrongen door bijvoorbeeld gebruik te maken van verkregen inloggegevens.

⁵³ Bogw, nota van toelichting hoofdstuk 3.3 p.15.

⁵⁴ Deze toetsing en oordeelsvorming bij het OM en de rechtspraak valt buiten de reikwijdte van het toezicht door de Inspectie.

⁵⁵ Bogw, nota van toelichting, hoofdstuk 3.3 p.15 en p.16 vermeldt dat "na het onderzoek het softwarepakket is verwijderd of is de licentie verbruikt waardoor hergebruik niet meer mogelijk is. Wanneer in een toekomstige zaak het gebruik van binnendringsoftware van derden wederom is aangewezen, zal eerst de bruikbaarheid van de minder ingrijpende middelen worden beoordeeld en het daarvoor benodigde gehele toetsings- en beslissingsmodel doorlopen, voordat kan worden overgegaan tot een (hernieuwde) aanschaf van een softwarepakket of van een nieuwe licentie."

⁵⁶ Zie *Kamerstukken I 2016/17*, 34 372, E, p. 4 en p. 11 en *Kamerstukken I 2016/17*, 34 372, D (MvA I), p. 20-22.

⁵⁷ *Kamerstukken II 2017/18*, 34 372 nr. 27 p.7; Regeerakkoord 2017-2021 "Vertrouwen in de toekomst" p.3.

⁵⁸ Beantwoording op 24 juli 2019 van Kamervragen over een media bericht over WhatsApp. Kenmerk 2647151.

⁵⁹ Bogw, nota van toelichting, hoofdstuk 3.3, p.16 en hoofdstuk 3.5, p.18.

N8 Er is alleen commerciële binnendringsoftware aangeschaft van leveranciers die gescreend zijn door de AIVD en waarvan door de politie is getoetst dat de leverancier niet levert aan dubieuze regimes.

N9 Commerciële binnendringsoftware is door de politie per zaak ingekocht en de ingekochte software(licentie) is uitsluitend in die specifieke zaak ingezet.

N10 In het geval binnendringsoftware wordt ingekocht, is het functioneren hiervan in een testomgeving gecontroleerd.

Melden onbekende kwetsbaarheden

Softwarecode bevat in zijn algemeenheid vrijwel altijd fouten. Onbekende kwetsbaarheden zijn fouten in software die nog onbekend zijn bij de producent van deze software. Sommige onbekende kwetsbaarheden kunnen gebruikt worden om een geautomatiseerd werk binnen te dringen. Er zijn partijen die bereid zijn veel geld te betalen voor informatie over bepaalde onbekende kwetsbaarheden. Om deze markt voor onbekende kwetsbaarheden niet te stimuleren, is het uitgangspunt dat als de politie beschikt over informatie van onbekende kwetsbaarheden⁶⁰ hiervan melding gemaakt wordt aan de producent.⁶¹ De meldingsplicht is overigens niet wettelijk verankerd: in het Wetboek van Strafvordering is alleen het uitstel van een melding van een onbekende kwetsbaarheid geregeld. Wel is de meldplicht benoemd in een Kamerbrief.⁶² In een ander Kamerstuk is aangegeven dat de officier van justitie dit uitstel uitsluitend kan bevelen op grond van een zwaarwegend opsporingsbelang en na machtiging van een rechter-commissaris.⁶³ Dit impliceert dat de OvJ bij de afweging voor uitstel tevens beoordeelt of sprake is van een onbekende kwetsbaarheid zoals bedoeld in artikel 126ffa van het Wetboek van Strafvordering. De machtiging voor uitstel is tijdelijk. De periode van geldigheid van de machtiging is wettelijk niet nader ingekaderd en wordt aan de interactie tussen de officier van justitie en de rechter-commissaris gelaten.⁶⁴

De Inspectie gaat bij haar toezicht na of de politie de OvJ tijdig op de hoogte heeft gesteld van beschikbare kennis van mogelijk onbekende kwetsbaarheden. In de situatie dat de OvJ van oordeel is dat sprake is van een onbekende kwetsbaarheid en er geen uitstel van melding is verleend, onderzoekt de Inspectie of de politie de onbekende kwetsbaarheid heeft gemeld bij de leverancier.

⁶⁰ Onder onbekende kwetsbaarheid wordt volgens Sv. artikel 126ffa vierde lid verstaan "een kwetsbaarheid in een geautomatiseerd werk waarvan aannemelijk is dat die niet bekend is of kan worden verondersteld niet bekend te zijn bij de producent van het apparaat of van het programma op basis waarvan automatisch computergegevens worden verwerkt, en die kan worden gebruikt om dat geautomatiseerde werk binnen te dringen."

⁶¹ Kamerstukken II 2016/17, 34 372 nr.6, p.9.

⁶² Kamerstukken I 2016/17, 26 643, nr. 428, pagina 4.

⁶³ Bogw, nota van toelichting, p.31; Sv. Artikel 126ffa derde lid.

⁶⁴ Kamerstukken I 2016/17, 34 372, nr. D, pagina 18.

Het ligt voor de hand dat melding alleen plaats kan vinden als de politie beschikt over, al dan niet ingekochte⁶⁵, kennis over de kwetsbaarheid.⁶⁶

N11 Indien de politie beschikt over kennis van een mogelijke onbekende kwetsbaarheid, meldt de politie dit allereerst bij de officier van justitie. Indien het OM geen uitstel van melding van een onbekende kwetsbaarheid heeft verleend, meldt de politie de kwetsbaarheid aan de producent van het apparaat of programma.

⁶⁵ De Inspectie merkt op dat in Kamerstukken I 2016/17, 34 372, nr. D, pagina 19,21 en 22 aangegeven is dat de politie geen informatie over onbekende kwetsbaarheden zal inkopen.

⁶⁶ *Kamerstukken I 2016/17, 34 372, nr. D, pagina 18 en 22.* Dit is in lijn met de memorie van antwoord waar gesproken wordt over het in beginsel melden aan de fabrikant als door de politie en het OM kennis verworven is van onbekende kwetsbaarheden.

4 Keuring technisch hulpmiddel

Na het binnendringen voert het technisch team onderzoek uit in het apparaat. De gegevens die middels onderzoekshandelingen worden vastgelegd, kunnen worden gebruikt als bewijs in een strafzaak. Het is dan ook van belang, voor zowel de betrokkene als voor de opsporing, dat de betrouwbaarheid en integriteit van de gegevens onomstotelijk vaststaan.⁶⁷ In het Wetboek van Strafvordering is aangegeven dat bij het verrichten van onderzoekshandelingen al dan niet gebruik kan worden gemaakt van een technisch hulpmiddel.⁶⁸ Volgens het Bogw is een *technisch hulpmiddel* 'een softwareapplicatie die gegevens detecteert, registreert en transporteert en waarmee onderzoekshandelingen worden verricht ter uitvoering van een bevel'.⁶⁹ In de nota van toelichting bij het Bogw wordt als voorbeeld hiervan op maat gemaakte software genoemd, zoals een script dat is geschreven door een technisch team en semi-handmatig wordt ingezet.

Om de betrouwbaarheid en integriteit van technische hulpmiddelen, de betrouwbaarheid en integriteit van de hiermee geregistreerde gegevens en de herleidbaarheid van de gegevens te borgen, stelt het Besluit diverse technische eisen⁷⁰ aan een technisch hulpmiddel.⁷¹

In de toelichting bij het Besluit is beschreven dat het uitgangspunt is dat bij het verrichten van onderzoekshandelingen met een technisch hulpmiddel gebruik wordt gemaakt van een vooraf goedgekeurd technisch hulpmiddel.⁷² Een technisch hulpmiddel wordt uitsluitend goedgekeurd als het voldoet aan de eisen uit het Besluit onderzoek geautomatiseerd werk (Bogw).⁷³ Het doel van de keuring is om te kunnen borgen dat de werking van een technisch hulpmiddel dusdanig betrouwbaar is dat de met een technisch hulpmiddel verkregen gegevens, die kunnen dienen als bewijs in een strafzaak, betrouwbaar, integer en herleidbaar zijn.⁷⁴

Als bij het verrichten van onderzoekshandelingen in een geautomatiseerd werk gebruik wordt gemaakt van een goedgekeurd technisch hulpmiddel mag er volgens de toelichting bij het Besluit vanuit worden gegaan dat aan de wettelijke eisen met betrekking tot betrouwbaarheid, integriteit en herleidbaarheid van de gegevens is voldaan.⁷⁵ Daarnaast biedt een goedgekeurd technisch hulpmiddel als voordeel dat risico's op misbruik door derden worden beperkt en dat specificaties van het middel niet worden prijsgegeven. Dit is van groot belang voor de afscherming van gevoelige opsporingsmethoden.⁷⁶

De beoordeling of een technisch hulpmiddel voldoet aan de eisen wordt uitgevoerd door een keuringsdienst. De minister wijst een onderdeel van de Landelijke Eenheid

⁶⁷ Bogw, nota van toelichting hoofdstuk 3.7, p. 21.

⁶⁸ Artt. 126nba, 126uba, 126zpa eerste lid, Wetboek van Strafvordering.

⁶⁹ Staatsblad 2018, nr. 340, art. 1g. Besluit onderzoek in een geautomatiseerd werk,

⁷⁰ Artt. 8 t/m 13 Bogw.

⁷¹ Bogw, nota van toelichting hoofdstuk 3.5 p. 18.

⁷² Art. 14 eerste lid Bogw en artikelsgewijze toelichting op het Besluit, art. 14 p. 40.

⁷³ Art. 14 tweede lid Bogw, eisen gesteld aan TH, verwijzend naar Bogw artt. 8 tot en met 13.

⁷⁴ Bogw, nota van toelichting, artikelsgewijze toelichting op het Besluit, art.14 p.41.

⁷⁵ Bogw nota van toelichting 3.5 p. 19.

⁷⁶ Kamerstukken II 2015/16, 34 372, nr. 3 memorie van toelichting Wet CCIII, p.110.

aan als keuringsdienst voor de keuring van technische hulpmiddelen.⁷⁷ De keuringsdienst dient een onafhankelijk en objectief oordeel te geven over de ter keuring aangeboden technische hulpmiddelen. Dit dient ook tot uitdrukking te komen in de plaatsing van de keuringsdienst binnen de politieorganisatie.⁷⁸ De minister kan een of meer andere organisaties aanwijzen als keuringsdienst.⁷⁹

N12 De keuringsdienst is door de minister van Justitie en Veiligheid aangewezen. Een aanwijzing van een andere organisatie dan de Landelijke Eenheid als keuringsdienst, geldt voor ten hoogste drie jaar.

In het Besluit is geregeld dat als de minister een of meer andere organisaties aanwijst als keuringsdienst daartoe bij ministeriële regeling regels worden gesteld. Te denken valt aan regels met betrekking tot de organisatie, middelen en werkwijze van de keuringsdienst.⁸⁰ Optioneel is dat bij ministeriële regeling ook regels gesteld kunnen worden aan het onderdeel van de Landelijke Eenheid dat door de minister is aangewezen als keuringsdienst.⁸¹

N13 De keuringsdienst voldoet aan de regels zoals vastgelegd in de relevante ministeriële regeling(en).

In het Besluit is gespecificeerd aan welke eisen een technisch hulpmiddel moet voldoen om te worden goedgekeurd. De wijze van keuring en keuringscriteria worden door de keuringsdienst in samenspraak met het openbaar ministerie nader geoperationaliseerd en vastgelegd in een keuringsprotocol dat door de minister moet worden goedgekeurd.⁸² De keuring van technische hulpmiddelen moet worden uitgevoerd op basis van dit keuringsprotocol.

N14 De keuring wordt uitgevoerd aan de hand van een door de minister goedgekeurd keuringsprotocol waarin de wijze van keuring en de eisen waaraan het technisch hulpmiddel moet voldoen om goedgekeurd te worden, zijn vastgelegd.

Het Besluit bepaalt dat de korpschef een technisch hulpmiddel ter keuring aanbiedt bij een keuringsdienst.⁸³ Van herkeuring is sprake als een goedgekeurd technisch hulpmiddel of een onderdeel hiervan zodanig wijzigt dat redelijkerwijs kan worden aangenomen dat de werking niet langer voldoet aan de gestelde technische eisen uit het Besluit.⁸⁴ Hierbij is in de nota van toelichting aangegeven dat bij een software update de keuringsdienst een inschatting maakt of redelijkerwijs kan worden aangenomen dat het technisch hulpmiddel nog aan de technische eisen voldoet. Dit gebeurt mede op basis van de notificatie die de update begeleidt waarin de impact van de update wordt vermeld. Dit kan variëren van een toevoeging van een bepaalde taal

⁷⁷ Art. 16 eerste lid Bogw (aanwijzing onderdeel Landelijke Eenheid als keuringsdienst).

⁷⁸ Art. 16, artikelsgewijze toelichting, nota van toelichting, Bogw, p.42.

⁷⁹ Art. 16 tweede lid Bogw.

⁸⁰ Art. 16 vierde lid Bogw; Zie hiertoe als voorbeeld de regeling waarin de eisen zijn vastgelegd die gelden voor TNO als aangewezen keuringsdienst. Staatscourant nr. 10713, 27 februari 2019. Regeling eisen keuringsdienst technisch hulpmiddel, 15 februari 2019, nr. 2433978; Art. 16 derde en vierde lid Bogw (stellen van regels); Art. 17 Bogw (wijze van keuring, keuringsprotocol); Art. 18 Bogw (keuringsrapport).

⁸¹ Art. 16, derde lid Bogw

⁸² Art. 17 Bogw (keuringsprotocol) en artikelsgewijze toelichting artikelen 16 t/m 19, p.42.

⁸³ Art. 18 eerste lid Bogw.

⁸⁴ Art. 14 derde lid Bogw.

waarin de software verkrijgbaar is tot een aanpassing van de functionaliteiten. Zo nodig wordt het technisch hulpmiddel opnieuw gekeurd.⁸⁵

Na afloop van de in het keuringsrapport genoemde periode kan de keuringsdienst besluiten het technische hulpmiddel opnieuw te keuren of de periode waarvoor de keuring geldt te verlengen.⁸⁶

N15 Een technisch hulpmiddel is door de korpschef ter (her)keuring aangeboden aan de keuringsdienst.

Aan de hand van het keuringsprotocol gaat de Inspectie per keuringseis na hoe en op basis waarvan de keuringsdienst tot haar oordeel is gekomen. Een kwaliteitsaspect voor de navolgbaarheid van de uitgevoerde keuring is een systematische vastlegging van de totstandkoming van de keuringsuitslag.⁸⁷ De door de keuringsdienst uitgevoerde keuring moet daarvoor op dusdanige wijze vastgelegd en te verantwoorden zijn dat de totstandkoming van de keuringsuitslag navolgbaar is voor de Inspectie.

De keuringsdienst legt als onderdeel van de dossiervorming de uitgevoerde werkzaamheden en de resultaten en analyse van de keuringsbevindingen vast. Het toezicht door de Inspectie hierop vindt plaats op basis van professional judgement.⁸⁸ Het is nadrukkelijk niet de bedoeling of intentie van de Inspectie om de keuring over te doen.

N16 De keuringsdienst kan van elk door hen goedgekeurd technisch hulpmiddel per keuringseis op een navolgbare en controleerbare wijze inzicht verschaffen in de wijze waarop zij tot haar oordeel is gekomen en daarmee de mate waarin het technisch hulpmiddel voldoet aan de gestelde eisen.

Het Besluit biedt de keuringsdienst de ruimte om vervangende waarborgen te stellen op onderdelen waar het technisch hulpmiddel niet voldoet aan de in het Besluit gestelde technische eisen.⁸⁹ Deze door de politie dan verplicht te treffen vervangende waarborgen worden door de keuringsdienst in het keuringsrapport vastgelegd.⁹⁰ Deze door de keuringsdienst aangedragen vervangende waarborgen worden door de Inspectie op basis van professional judgement bezien op relevantie in relatie tot de doelstelling van de technische eis die hieraan ten grondslag ligt, de mate waarin daarmee het onderliggende risico wordt beperkt en de uitvoerbaarheid van de waarborg.

⁸⁵ Bogw, artikelsgewijze toelichting artikel 14, p.41.

⁸⁶ Bogw, artikelsgewijze toelichting artikel 18, p. 43.

⁸⁷ Zie hiertoe als voorbeeld de regeling waarin de eisen waren vastgelegd die golden voor TNO als aangewezen keuringsdienst. Staatscourant.10713 Regeling eisen keuringsdienst technisch hulpmiddel, artikel 7 "Een aangewezen keuringsdienst voldoet aan de volgende voorwaarden: c. hij bewaart op de beveiligde infrastructuur van de politie op een systematische en behoorlijke wijze de keuringsrapporten, dossiers, verslagen, certificaten en verklaringen en overige gegevens die samenhangen met, en betrekking hebben op, de aan hem opgedragen taken."

⁸⁸ Elk te inspecteren dossier zal door minimaal twee ervaren en deskundige medewerkers van de Inspectie worden beoordeeld.

⁸⁹ Bogw, artikelsgewijze toelichting artikel 18, p.43 vermeldt verplicht te treffen vervangende procedurele waarborgen. Dit kan tot verwarring leiden. Voor de uniformiteit hanteert de Inspectie hier het begrip "vervangende waarborgen".

⁹⁰ Art. 18, derde lid, sub e. "Het keuringsrapport van een goedgekeurd technisch hulpmiddel vermeldt ten minste: e) relevante verplichte vervangende waarborgen waarmee voldaan kan worden aan één of meer eisen, bedoeld in artikelen 8 tot en met 13".

N17 Indien naar oordeel van de keuringsdienst sprake is van vervangende waarborgen waarmee alsnog voldaan kan worden aan de eisen, dan dekken deze maatregelen het risico voldoende af en zijn deze uitvoerbaar (SMART).

De keuringsdienst legt de resultaten van de keuring vast in een keuringsrapport. In het keuringsrapport van een goedgekeurd technisch hulpmiddel wordt tenminste vastgelegd:⁹¹

- a) dat het technisch hulpmiddel voldoet aan de gestelde technische eisen uit de artikelen 8 tot en met 13 van het Besluit;
- b) een referentienummer;
- c) een omschrijving van de werking van het technisch hulpmiddel;
- d) een aanduiding van de functionaliteit of functionaliteiten van het technisch hulpmiddel;
- e) de relevante verplichte vervangende waarborgen, waarmee voldaan kan worden aan één of meer eisen, bedoeld in de artikelen 8 tot en met 13 van het Besluit;
- f) relevante informatie met betrekking tot de werking van een functionaliteit of functionaliteiten van het technische hulpmiddel, zoals relevante informatie ten behoeve van de plaatsing, inzet of verwijdering van het technisch hulpmiddel⁹²;
- g) de periode waarvoor de keuring geldt, zolang de werking van het technische hulpmiddel ongewijzigd is.

N18 De keuringsdienst stelt van een uitgevoerde keuring een keuringsrapport op. Een keuringsrapport van een goedgekeurd technisch hulpmiddel bevat tenminste de onderdelen zoals benoemd in het Besluit (artikel 18.3).

De keuringsdienst stelt bij de keuring een handleiding op voor het gebruik van een hulpmiddel, waarin wordt aangegeven welke instellingen bij gebruik van een technisch hulpmiddel voor een bepaalde functionaliteit moeten worden aangevinkt.⁹³ Dit is van belang gelet op de technische eis dat de werking van een technisch hulpmiddel moet kunnen worden beperkt tot een bepaalde functionaliteit of functionaliteiten zoals vermeld in het bevel.

N19 De keuringsdienst stelt bij een goedgekeurd technisch hulpmiddel een handleiding op waarin is aangegeven welke instellingen bij gebruik van een technisch hulpmiddel voor een bepaalde functionaliteit moeten worden aangevinkt.

De keuringsdienst van een onderdeel van de Landelijke Eenheid houdt een centrale registratie bij van de keuringsrapporten.⁹⁴

N20 De keuringsdienst van een onderdeel van de Landelijke Eenheid houdt een centrale registratie bij van de keuringsrapporten.

⁹¹ Artikel 18, derde lid, Bogw (keuringsrapport).

⁹² Bogw, artikelsgewijze toelichting, artt. 16 t/m 18, p. 43.

⁹³ Bogw, artikelsgewijze toelichting artikel 9, p.38.

⁹⁴ Art. 19 Bogw.

5 Uitvoering binnendringen en verrichten van onderzoekshandelingen

Het op afstand en heimelijk binnendringen en het verrichten van onderzoek in een geautomatiseerd werk kan worden uitgevoerd, zodra daartoe, na machtiging van de rechter-commissaris, een bevel is afgegeven door de officier van justitie.

In het bevel specificeert de officier van justitie de onderzoeksdoelen waarvoor de bevoegdheid in een bepaalde zaak door de politie ingezet mag worden. De opsporingsambtenaar van het technisch team mag alleen handelingen uitvoeren die passen binnen deze afgegeven doelen. De mogelijke onderzoeksdoelen zijn limitatief in het Wetboek van Strafvordering omschreven.⁹⁵ ⁹⁶ Het betreft de doelen:

- a) de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker zoals de identiteit of locatie, en de vastlegging daarvan;
- b) het opnemen van vertrouwelijke communicatie (ovc) of het aftappen en opnemen van telecommunicatie;⁹⁷
- c) stelselmatige observatie, waarbij door de officier van justitie bepaald kan worden dat het technisch hulpmiddel op de persoon wordt bevestigd;⁹⁸
- d) de vastlegging van gegevens die in het geautomatiseerde werk zijn opgeslagen (historische gegevens) of die binnen de looptijd van het bevel nog worden opgeslagen;
- e) de ontoegankelijk making van gegevens.⁹⁹ ¹⁰⁰

De totstandkoming van de afgifte en de inhoud van een bevel is de verantwoordelijkheid van de officier van justitie en valt daarmee buiten de reikwijdte van het toezicht door de Inspectie. Het door de officier van justitie afgegeven bevel vormt wel het kader waarbinnen de politie uitvoering aan de hackbevoegdheid moet geven. In het bevel vermeldt de officier van justitie naast de eerdergenoemde doelen, het nummer of een andere aanduiding van het geautomatiseerde werk en ten aanzien van welk deel van het geautomatiseerde werk en welke categorie van gegevens aan het bevel uitvoering gegeven moet worden.

Indien door de officier van justitie bevolen wordt om de onderzoekshandelingen met behulp van een technisch hulpmiddel uit te voeren, wordt de aard en functionaliteit van het technisch hulpmiddel in het bevel aangeduid. Tevens kan de officier in het

⁹⁵ Wetboek van Strafvordering, artikelen 126nba, 126uba, 126zpa, eerste lid.

⁹⁶ *Kamerstukken II 2016/17*, 34 372 nr.6 p.30 en p.36. Het onderzoek in een geautomatiseerd werk is beperkt tot bepaalde onderzoekshandelingen, dit betreft enerzijds de toepassing van bestaande bevoegdheden, zoals het aftappen van telecommunicatie of het direct af luisteren. In deze gevallen is het binnendringen voorwaardelijk om de bestaande opsporingsbevoegdheid te kunnen uitoefenen. Anderzijds betreft het nieuwe bevoegdheden, zoals het vastleggen of ontoegankelijk maken van gegevens.

⁹⁷ Aan de uitvoering hiervan ligt respectievelijk een bevel ten grondslag op basis van artikel 126l, Sv. (opnemen van vertrouwelijk communicatie) en artikel 126m, Sv. (opnemen van niet voor het publiek bestemde communicatie die plaatsvindt met gebruikmaking van de diensten van een aanbieder van een communicatiedienst).

⁹⁸ Aan de uitvoering ligt een bevel op basis van 126g, Sv. (stelselmatige observatie) ten grondslag.

⁹⁹ *Kamerstukken II 2016/17*, 34 372, nr.6 p. 43. Het ontoegankelijk maken van gegevens is een bevoegdheid die kan worden ingezet ten behoeve van het voorkomen of beëindigen van een strafbaar feit.

¹⁰⁰ *Kamerstukken II 2016/17*, 34 372, nr.6 p. 44. Als de gegevens (als onderdeel van het ontoegankelijk maken) worden verwijderd, dan dienen zij te worden behouden ten behoeve van de strafvordering. In het kader van de ontoegankelijkmaking kunnen de gegevens dan ook niet worden gewist. De ontoegankelijkmaking betreft een voorlopige maatregel, in afwachting van een beslissing van de rechter.

bevel aangeven of het onderzoeksbelang dringend vordert dat een niet-gekeurd technisch hulpmiddel wordt ingezet. Ook vermeldt het bevel het tijdstip of de periode waarbinnen aan het bevel door de politie uitvoering moet worden gegeven.¹⁰¹ Indien bevel is gegeven voor het opnemen van vertrouwelijke communicatie (ovc)¹⁰², zijn in het bevel de locaties gespecificeerd waar dit mag plaatsvinden.

Deze in het bevel benoemde onderdelen worden door de Inspectie als kader gehanteerd om te bepalen of het technisch team handelt binnen de reikwijdte van het bevel.¹⁰³ Dit betekent bijvoorbeeld ook dat als een technisch hulpmiddel voor het verrichten van onderzoekshandelingen wordt ingezet, het technisch hulpmiddel zodanig ingericht moet zijn dat de detectie en registratie van gegevens alsmede de werking ervan beperkt is tot de in het bevel vermelde functionaliteit en het identificerende kenmerk van het geautomatiseerde werk van de gebruiker(s) op wie het bevel betrekking heeft.

In de aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid zijn regels gesteld voor het handelen buiten de grenzen van het Nederlandse grondgebied.¹⁰⁴ Deze aanwijzing is gericht aan de hoofden van OM onderdelen. De aanwijzing en het Besluit stellen geen eisen aan het handelen van de politie in internationale context.

De officier van justitie kan, los van het afgegeven bevel, de politie van aanwijzingen of instructies voorzien omtrent de toepassing van de hackbevoegdheid.

N21 *Het technisch team past de bevoegdheid tot het binnendringen en het verrichten van onderzoek in een geautomatiseerd werk toe conform door de officier van justitie afgegeven bevelen, aanwijzingen en instructies.*

Het daadwerkelijke binnendringen in het geautomatiseerde werk gaat volgens het vooraf geschreven plan van aanpak.¹⁰⁵

N22 *Het binnendringen in het geautomatiseerde werk is door het technisch team uitgevoerd volgens het vooraf opgestelde plan van aanpak.*

Het binnendringen, het plaatsen en verwijderen van een technisch hulpmiddel en het verrichten van onderzoekshandelingen, al dan niet met een technisch hulpmiddel is voorbehouden aan de opsporingsambtenaren die lid of deelnemer zijn van een technisch team.¹⁰⁶

N23 *Het binnendringen en het uitvoeren van (onderzoeks)handelingen is uitgevoerd door een lid of deelnemer van een technisch team.*

¹⁰¹ Artt. 126nba, 126uba en 126zpa tweede en derde lid Sv.

¹⁰² Hier wordt bedoeld op de afgegeven combibevelen voor de inzet van de bevoegdheid op basis van 126nba (doel b) en 126l Sv. of 126uba (doel b) en 126s Sv.

¹⁰³ Artt. 126nba, 126uba en 126zpa zevende lid Sv. "Het toezicht op de uitvoering van het bevel door de ambtenaren wordt uitgeoefend door de Inspectie overeenkomstig het bepaalde in hoofdstuk 6 van de Politiewet 2012."

¹⁰⁴ Staatscourant nr. 10277, 26 februari 2019. Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba Sv.

¹⁰⁵ Bogw, nota van toelichting, hoofdstuk 3.3 p.16.

¹⁰⁶ Bogw, nota van toelichting, hoofdstuk 3.3 p.16; Artt. 23 eerste lid, 24 eerste lid en 25 tweede lid Bogw.

Om de kwaliteit en professionaliteit van het onderzoek te borgen moeten de opsporingsambtenaren die op een ad hoc basis deelnemen aan een technisch team volgens het Besluit gedurende de uitvoering van het onderzoek begeleid worden door een lid van een technisch team.¹⁰⁷

N24 Een deelnemer aan een technisch team is gedurende de uitvoering van het bevel begeleid door een lid van een technisch team.

Tijdens de behandeling van het wetsvoorstel CCIII is door de minister aangegeven dat alleen de technische, daartoe aangewezen ambtenaren toegang hebben tot het systeem van waaruit het op afstand binnendringen van het geautomatiseerde werk wordt uitgevoerd.¹⁰⁸ Tevens is door de minister aangegeven dat de geïnfecteerde geautomatiseerde werken niet in verbinding staan met een server van de leverancier van de binnendringsoftware.¹⁰⁹

N25 Alleen de technische, daartoe aangewezen ambtenaren hebben toegang tot het systeem van waaruit het op afstand binnendringen van een geautomatiseerd werk wordt uitgevoerd. Het geautomatiseerde werk staat niet in verbinding met een server van de leverancier van de binnendringsoftware.

Indien de officier van justitie besluit dat het verrichten van onderzoekshandelingen plaatsvindt zonder technisch hulpmiddel, dan worden procedurele waarborgen getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de tijdens het onderzoek vast te leggen gegevens te garanderen.¹¹⁰ Het kunnen afleggen van verantwoording over de implementatie en opvolging van deze waarborgen op een controleerbare en aantoonbare wijze is een belangrijk aspect voor de kwaliteit van de taakuitvoering.

N26 De politie draagt op een controleerbare en aantoonbare wijze zorg voor de implementatie van en verantwoording over de opvolging van de procedurele waarborgen die getroffen moeten worden indien de onderzoekshandelingen worden verricht zonder gebruik te maken van een technisch hulpmiddel.

Inzet technisch hulpmiddel

Als voor het verrichten van onderzoekshandelingen een technisch hulpmiddel ingezet wordt, is het uitgangspunt dat dit een vooraf goedgekeurd hulpmiddel betreft. De keuringsdienst keurt een technisch hulpmiddel goed als dit voldoet aan de gestelde technische eisen uit het Besluit. Zie tevens hoofdstuk 4. Het Besluit biedt de keuringsdienst de ruimte om vervangende waarborgen te stellen op onderdelen waar het technisch hulpmiddel niet voldoet aan de in het Besluit gestelde technische eisen.¹¹¹ Deze door de politie dan verplicht te treffen vervangende waarborgen worden door de keuringsdienst in het keuringsrapport vastgelegd. Het is bij de uitvoering van het bevel dan ook zaak dat de politie deze vervangende waarborgen aantoonbaar heeft geïmplementeerd en verantwoording over de naleving aflegt. In de toelichting van het

¹⁰⁷ Art. 4 derde lid Bogw (incidentele samenwerking); Bogw, nota van toelichting, p.36.

¹⁰⁸ Kamerstukken II 2016/17, 34 372, nr. 6 p.52.

¹⁰⁹ Kamerstukken II 2016/17, 34 372, nr. 6 p.78.

¹¹⁰ Art. 21 vijfde lid Bogw.

¹¹¹ Art. 18 derde lid sub e Bogw; Bogw, artikelsgewijze toelichting artt. 16 t/m 18, p.43.

Besluit is aangegeven dat hierover in de processen-verbaal van de opsporingshandelingen verantwoording afgelegd kan worden.¹¹²

N27 De keuringsdienst kan in het keuringsrapport aangeven dat een technisch hulpmiddel uitsluitend mag worden ingezet indien verplichte vervangende waarborgen worden toegepast. Indien de politie een dergelijk technisch hulpmiddel inzet, implementeert zij deze waarborgen en legt zij verantwoording af over de naleving hiervan.

Naast het keuringsrapport stelt de keuringsdienst bij een goedgekeurd technisch hulpmiddel ook een handleiding op. In deze handleiding is aangegeven welke instellingen bij gebruik van een technisch hulpmiddel voor een bepaalde functionaliteit moeten worden aangevinkt. Zie hoofdstuk 4 (keuring technisch hulpmiddel). Ook hiervan is het tijdens de uitvoering van het bevel zaak dat de politie opvolging geeft aan deze inrichtingsinstructie en daarover verantwoording aflegt. In de toelichting van het Besluit is aangegeven dat hierover in het proces-verbaal van plaatsing verantwoording afgelegd dient te worden.¹¹³

N28 Indien een goedgekeurd technisch hulpmiddel ingezet wordt voor het verrichten van onderzoekshandelingen, draagt de politie in het kader van de uitvoering van het bevel zorg voor de implementatie van en de verantwoording over de opvolging van de door de keuringsdienst opgestelde handleiding.

De officier van justitie kan in het bevel bepalen dat het onderzoeksbelang dringend vordert dat een niet gekeurd technisch hulpmiddel wordt gebruikt.¹¹⁴ Het Besluit beschrijft daaropvolgend twee mogelijke vervolgtrajecten. In de eerste situatie, wat tevens het uitgangspunt is, vindt keuring achteraf plaats en vermeldt de officier van justitie de uitkomst van de keuring na afloop van het gebruik in de processtukken.¹¹⁵ Indien de situatie zich voor zou doen dat een reeds ingezet technisch hulpmiddel toch achteraf door de keuringsdienst wordt afgekeurd, dan wordt dit voorgelegd aan de rechter in de strafzaak, die beslist over het gebruik van de gegevens als bewijs.¹¹⁶

In de tweede situatie kan, als uitzondering op de hoofdregel, de keuring van een technisch hulpmiddel geheel achterwege blijven.¹¹⁷ De officier van justitie is in die situatie van oordeel dat de aard van het technisch hulpmiddel zich verzet tegen

¹¹² Bogw, artikelsgewijze toelichting op het Besluit, artikel 18 p.43.

¹¹³ Bogw, artikelsgewijze toelichting artikel 9, p.38. Er is sprake van verschrijving in de verwijzing, dit moet artikel 23 van het Besluit zijn.

¹¹⁴ Art. 15, eerste lid, Bogw; Art. 21 tweede lid Bogw. "In dat geval vermeldt de officier van justitie in het bevel dat toepassing is gegeven aan artikel 21, tweede lid". In de nota van toelichting, pagina 44 is overigens aangegeven dat bij de afweging om dat te bepalen, de officier van justitie in overleg met de keuringsdienst moet nagaan of het technisch hulpmiddel naar verwachting zal voldoen aan de gestelde eisen uit artt. 8 t/m 13 Bogw.

¹¹⁵ Art. 15 eerste lid, art. 21 derde lid en artikelsgewijze toelichting bij artikel 21, p. 44, Bogw; Kamerstukken I 2017/18, 34 372, nr. G, p.15. *Indien een technisch hulpmiddel na afloop van de inzet ervan ter keuring wordt aangeboden en niet wordt goedgekeurd, dan betekent dit dat niet is voldaan aan de wettelijke eisen omtrent betrouwbaarheid, integriteit en herleidbaarheid van de met het technische hulpmiddel vastgelegde gegevens. Het is dan aan de officier van justitie om te bepalen in hoeverre de gegevens voldoende betrouwbaar, integer en herleidbaar zijn voor het gebruik in een strafzaak. De kans dat de gegevens niet kunnen worden gebruikt als bewijsmateriaal is dan, mede afhankelijk van de reden van afkeuring, reëel. Als de officier besluit om de gegevens toch te gebruiken als bewijs in een strafzaak, dient hij maatregelen te treffen om rechterlijke controle op de rechtmatigheid van de inzet en de betrouwbaarheid, integriteit en herleidbaarheid van de vastgelegde gegevens mogelijk te maken.*

¹¹⁶ Kamerstukken II 2018/19, 34 372, nr. 29, p.13.

¹¹⁷ In de artikelsgewijze toelichting artikel 15, p.42 en artikel 21, p.45 is aangegeven dat de hiervan in de praktijk geen lichtzinnig gebruik van gemaakt zal worden en dat het naar verwachting om uitzonderlijke gevallen gaat.

keuring.¹¹⁸ In dat geval vermeldt de officier in de processtukken welke aanvullende waarborgen zijn getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de vastgelegde gegevens te garanderen.¹¹⁹ De aanvullende waarborgen kunnen op aangeven van de officier van justitie ook (deels) buiten de inzet van het technisch team getroffen zijn. In de toelichting van het Besluit is aangegeven dat als aanvullende waarborg gedacht kan worden aan het opnemen van een uitgebreide omschrijving van de functionele specificaties van een op maat gemaakt technisch hulpmiddel, het voegen van een digitale kopie van de software en de broncode bij het proces-verbaal, het vooraf en achteraf maken van een forensische kopie en het audiovisueel vastleggen van de uitvoering van onderzoekshandelingen.¹²⁰

Het is zaak dat deze aanvullende waarborgen voor zover deze betrekking hebben op het handelen door de politie aantoonbaar getroffen zijn.¹²¹ Het kunnen afleggen van verantwoording over de implementatie en opvolging van deze waarborgen op een controleerbare en aantoonbare wijze is een belangrijk aspect voor de kwaliteit van de taakuitvoering.

N29 Indien de Officier van Justitie van oordeel is dat de aard van een technisch hulpmiddel zich verzet tegen keuring, draagt de politie zorg voor de implementatie van aanvullende waarborgen om de betrouwbaarheid, integriteit en herleidbaarheid van vastgelegde gegevens te waarborgen en legt zij verantwoording af over de naleving hiervan.

In het Besluit zijn in hoofdstuk 5 de technische eisen vastgelegd waaraan een technisch hulpmiddel dat wordt gebruikt voor het verrichten van onderzoekshandelingen moet voldoen. Deze eisen hebben tot doel om te waarborgen dat de gegevens die met dit technisch hulpmiddel worden vergaard betrouwbaar, integer en herleidbaar zijn en dat het technisch hulpmiddel zelf betrouwbaar en integer functioneert.¹²² Bij de in hoofdstuk 4 genoemde keuring wordt door de keuringsdienst getoetst of het technisch hulpmiddel voldoet aan deze gestelde technische eisen. In de toelichting op het Besluit is gesteld dat de Inspectie toezicht houdt op de naleving van de technische eisen.¹²³ Bij een gekeurd technisch hulpmiddel ontleent de Inspectie een voldoende mate van zekerheid over de naleving van de technische eisen door toezicht te houden op de keuringsdienst en het door de keuringsdienst uitgevoerde keuringsproces. De politie kan, als tijdens de uitvoering van een bevel een goedgekeurd technisch hulpmiddel wordt ingezet, aan de hand van het keuringsrapport aantonen dat het ingezette middel voldoet aan deze gestelde eisen. Onderdeel van deze aantoonbaarheid vormt tevens de controleerbare opvolging van eventuele in het keuringsrapport benoemde verplicht te treffen vervangende waarborgen en de opvolging van de door de keuringsdienst opgestelde handleiding. Tevens moet uiteraard zeker gesteld zijn dat het technisch hulpmiddel dat ingezet wordt, identiek is aan het goedgekeurde technisch hulpmiddel.

¹¹⁸ Art. 15, tweede lid; artikel 21, vierde lid en artikelsgewijze toelichting artikel 21 p. 45, Bogw.

¹¹⁹ Art. 21, vierde lid Bogw.

¹²⁰ Bogw, artikelsgewijze toelichting artikel 21, p.45.

¹²¹ De Inspectie richt zich hierbij op waarborgen die door het technisch team zijn getroffen.

¹²² Bogw, nota van toelichting, hoofdstuk 3.5, p. 18.

¹²³ Bogw, nota van toelichting, hoofdstuk 3.5, p. 20.

In de situatie dat door de officier van justitie nog niet geoordeeld is dat de aard van het ingezette technisch hulpmiddel zich verzet tegen keuring, blijven de technische eisen gelden.¹²⁴

In de situatie dat de officier van justitie oordeelt dat de aard van het technisch hulpmiddel zich verzet tegen keuring, moeten conform het Besluit aanvullende waarborgen getroffen worden om de betrouwbaarheid, integriteit en herleidbaarheid van de met het technisch hulpmiddel vastgelegde gegevens te garanderen.¹²⁵ Het is aan de officier van justitie om te bepalen of het samenstel van de te treffen aanvullende waarborgen het risico voor de betrouwbaarheid, integriteit en herleidbaarheid voldoende afdekken. Deze aanvullende waarborgen worden vermeld door de OvJ en kunnen mogelijk (deels) buiten het technisch team om getroffen worden. Het toezicht van de Inspectie richt zich op de toereikende implementatie van de door het technisch team te treffen benoemde aanvullende waarborgen. De Inspectie kan daarbij signalerend rapporteren over mogelijk aanwezige restrycties.

N30 De politie kan te allen tijde aantonen dat een ingezet technisch hulpmiddel voldoet aan de technische eisen die het Besluit daaraan in artikelen 8 t/m 13 stelt, dan wel dat de risico's voor de betrouwbaarheid, integriteit en herleidbaarheid van de door middel van het technisch hulpmiddel vergaarde gegevens beperkt zijn.

Verwijdering van een technisch hulpmiddel

Volgens het Bogw verwijdt een opsporingsambtenaar van het technisch team het technisch hulpmiddel voordat het onderzoek is beëindigd.¹²⁶ In de nota van toelichting bij het Bogw is aangegeven dat een technisch hulpmiddel wordt verwijderd uit het te onderzoeken geautomatiseerde werk, nadat het onderzoeksdoel is bereikt of de periode waarvoor het bevel is afgegeven is verstreken.¹²⁷ Een opsporingsambtenaar moet binnendringen in het geautomatiseerd werk om het technisch hulpmiddel te verwijderen. Dit binnendringen mag uitsluitend binnen de looptijd van het bevel. In de praktijk zal verwijdering van het technisch hulpmiddel dus moeten plaatsvinden voordat het onderzoek is beëindigd. In alle gevallen zal zoveel mogelijk worden geprobeerd het geautomatiseerde werk in de oorspronkelijke staat achter te laten, dat wil zeggen als ware de bevoegdheid nooit toegepast.¹²⁸

N31 Een technisch hulpmiddel is verwijderd uit een geautomatiseerd werk door een opsporingsambtenaar van een technisch team zodra het onderzoeksdoel is bereikt of voordat de periode, waarbinnen aan het bevel uitvoering moet worden gegeven, is verlopen.

In sommige gevallen kan worden afgezien van de verwijdering van geïnstalleerde software of het ongedaan maken van de in het geautomatiseerde werk aangebrachte wijzigingen. Hierbij moet worden gedacht aan zwaarwegende belangen die zich verzetten tegen het verwijderen, zoals de situatie dat het verwijderen aanzienlijke

¹²⁴ Hoofdstuk 5 art. 8 t/m 13 Bogw en nota van toelichting hoofdstuk 3.5, p.18. Om de betrouwbaarheid en integriteit van technische hulpmiddelen, de betrouwbaarheid en integriteit van de hiermee geregistreeerde gegevens en de herleidbaarheid van de gegevens te borgen stelt het Besluit in hoofdstuk 5 diverse technische eisen aan het technisch hulpmiddel.

¹²⁵ Art. 21, vierde lid Bogw.

¹²⁶ Zesde lid Artikel 126nba, Sv.

¹²⁷ Bogw, Nota van Toelichting, artikelsgewijze toelichting artikel 25 en 26.

¹²⁸ *Kamerstukken II* 2015/16, 34 372 nr. 3 memorie van toelichting, p.36; *Kamerstukken II* 2016/17, 34 372 nr. 6, p.76.

risico's met zich mee brengt voor het systeem waarin het technische hulpmiddel is geïnstalleerd. Deze risico's worden in de voorfase zoveel mogelijk in kaart gebracht en de officier van justitie wordt hierover door het technisch team geïnformeerd.¹²⁹ Zie hoofdstuk 2 (voorbereiding, haalbaarheidsonderzoek).

Er kan zich een situatie voordoen dat een technisch hulpmiddel niet of niet volledig kan worden verwijderd uit een geautomatiseerd werk. In de parlementaire stukken is aangegeven dat de met verwijdering belaste opsporingsambtenaar in dat geval het transport van de door het technisch hulpmiddel geregistreerde gegevens naar de technische infrastructuur beëindigt.¹³⁰ Op basis van de logging kan worden gecontroleerd of de ontvangst van gegevens op de technische infrastructuur daadwerkelijk is beëindigd.¹³¹

N32 Indien een technisch hulpmiddel niet of niet volledig kan worden verwijderd uit een geautomatiseerd werk, beëindigt de met verwijdering belaste opsporingsambtenaar het transport van de door het technische hulpmiddel geregistreerde gegevens naar de technische infrastructuur.

Indien het achtergebleven technisch hulpmiddel (of sporen daarvan) risico's oplevert voor het functioneren van het geautomatiseerde werk stelt de opsporingsambtenaar de officier van justitie hiervan in kennis en stelt hij informatie ter beschikking ten behoeve van de volledige verwijdering.¹³² De Inspectie merkt hierbij op dat er een verschil beoogd lijkt te zijn tussen de niet of niet volledige verwijdering met en zonder risico's voor het geautomatiseerde werk. Als er een risico is, dan wordt de officier van justitie in kennis gesteld, anders wordt alleen een proces-verbaal opgesteld.

N33 Indien de niet of niet volledige verwijdering van een technisch hulpmiddel risico's oplevert voor het functioneren van het geautomatiseerde werk waarin het is geplaatst, stelt de opsporingsambtenaar de officier van justitie hiervan in kennis en stelt hij informatie ter beschikking ten behoeve van de volledige verwijdering.

De opsporingsambtenaar maakt van een niet of niet-volledige verwijdering proces-verbaal op dat toegezonden wordt aan de officier van justitie. Zie hoofdstuk 9 (proces-verbaal).

Communicatie met leverancier technisch hulpmiddel

Tijdens de parlementaire behandeling van het wetsvoorstel CCIII is door de minister in beantwoording op vragen aangegeven dat in het kader van het onderzoek met een technisch hulpmiddel er geen verbinding tot stand gebracht wordt met een server van de maker van het technisch hulpmiddel. Er wordt uitsluitend een verbinding tot stand gebracht tussen het binnengedrongen geautomatiseerde werk en de server van de politie.¹³³ In de beantwoording geeft de minister aan dat de leverancier geen mogelijkheid heeft om zelfstandig updates uit te voeren en zelf de controle over het

¹²⁹ Kamerstukken II 2015/16, 34 372 nr. 3 memorie van toelichting, p.36.

¹³⁰ Bogw, artikel 26 eerste lid; Kamerstukken II 2015/16, 34 372 nr. 3 memorie van toelichting, p.36.

"Wanneer de software aanwezig blijft in het geautomatiseerde werk waarin de bevoegdheid is toegepast, wordt vanuit de server van de politie het dataverkeer stopgezet zodat de politie geen gegevens meer kan ontvangen van het geautomatiseerde werk."; Kamerstukken II 2016/17, 34 372 nr.6 p.78. "Hier zien de opsporingsambtenaren van het technisch team op toe".

¹³¹ Art. 26 artikelsgewijze toelichting, Bogw, p. 47.

¹³² Art. 26 tweede lid, Bogw; Art. 126nba zesde lid Sv; Kamerstukken II 2015/16, 34 372 nr. 3 memorie van toelichting, p.105.

¹³³ Kamerstukken II 2016/17, 34 372, nr.6 p.45 en p.51.

geautomatiseerd werk over te nemen. Evenmin kunnen andere klanten van de leverancier toegang krijgen tot het geautomatiseerd werk.¹³⁴

N34 Het technisch hulpmiddel staat tijdens de inzet niet in contact met de producent van deze software.

Centrale registratie toegang en toegangsverlening technisch hulpmiddel

In het Besluit is aangegeven dat voor toegang tot technische hulpmiddelen een formeel proces gevolgd moet worden dat vergelijkbaar is met het proces voor de registratie, uitgifte en inname van 'klassieke' technische hulpmiddelen (zoals een microfoon en/of een videocamera).¹³⁵ De korpschef wijst één of meer ambtenaren aan die belast zijn met de centrale registratie van de toegang tot technische hulpmiddelen. Deze ambtenaar verschaft toegang tot het technisch hulpmiddel aan de met plaatsing van het technisch hulpmiddel belaste opsporingsambtenaar voor de duur van het bevel. De ambtenaar die belast is met de centrale registratie registreert de naam van de opsporingsambtenaar die om toegang heeft verzocht, het tijdstip van toegangsverlening en enkele kenmerken van het technisch hulpmiddel.¹³⁶

N35 De registratie van de beperkte en gecontroleerde toegangsverlening tot en uitgifte van technisch hulpmiddelen vindt centraal plaats door daartoe door de korpschef aangewezen ambtenaren.

Monitoring en bewaking politieomgeving¹³⁷

Om het risico te beperken dat de server van de politie die in verbinding staat met geïnfecteerde geautomatiseerde werken gehackt wordt, richt de politie haar eigen geautomatiseerde omgeving zo veilig mogelijk in en beschermt en bewaakt zij de gebruikte systemen voortdurend tegen mogelijke aanvallen van buiten.¹³⁸

N36 De systemen van de politie worden voortdurend beschermd en bewaakt tegen mogelijke aanvallen van buiten.

¹³⁴ Kamerstukken II 2016/17, 34 372, nr.6 p.74.

¹³⁵ Staatsblad 2006, nr. 524. 'Besluit technische hulpmiddelen strafvordering, dit Besluit is op 7 november 2006 in het Staatsblad gepubliceerd.

¹³⁶ Art. 22 Bogw en artikelsgewijze toelichting op artikel 22, p.45.

¹³⁷ Dit heeft ook betrekking op handmatige inzetten.

¹³⁸ Kamerstukken II 2016/17, 34 372, nr. 6 p.78.

6 Gegevens vastgelegd in logbestanden (logging)

Onder logging verstaat het Besluit de elektronische verslaglegging over de uitvoering van een bevel.¹³⁹ Hierbij wordt onderscheid gemaakt tussen gegevens over:

- de verrichte handelingen tijdens de voorbereidende fase, het binnendringen in het geautomatiseerd werk alsmede de handelingen die gedurende de onderzoeksfase worden verricht.¹⁴⁰ De toelichting noemt dit 'inzetlogging'. Hierbij wordt de vastlegging genoemd van het beeldscherm en de toetsaanslagen van de opsporingsambtenaar, de communicatie tussen de technische infrastructuur¹⁴¹ en het geautomatiseerd werk en gebruikte scripts en softwareversies.¹⁴²
- gegevens over de toegang tot een technisch hulpmiddel en het functioneren van de technische infrastructuur.¹⁴³ De toelichting noemt dit 'systeemlogging' die automatisch door alle gebruikte systemen wordt gegenereerd en centraal wordt verzameld en vastgelegd en betreft hierbij ook de logging van toegang tot een technisch hulpmiddel;¹⁴⁴
- gegevens over de ter uitvoering van het bevel door middel van onderzoekshandelingen verkregen gegevens. Hiermee worden niet de gegevens zelf bedoeld die mogelijk kunnen dienen als bewijs in een strafzaak, maar de gegevens over deze gegevens (metadata).¹⁴⁵ Voorbeelden van metadata zijn de datum, tijd van vastlegging, locatie, de naam van de opsporingsambtenaar of hash/checksums van het bewijs.

Een voorwaarde om te kunnen komen tot een juiste en volledige implementatie en controleerbare naleving van de logging is dat de politie zelf vastlegt en verantwoordt op welke wijze zij beoogt invulling te geven aan de vastlegging van gegevens over de uitvoering in logbestanden. De invulling en inrichting hiervan kan bovendien per zaak verschillen.

Het uitgangspunt voor deze logging is dat vastlegging doorlopend en automatisch plaatsvindt.¹⁴⁶ De gegevens over de verrichte handelingen (inzetlogging) mogen als uitzondering handmatig vastgelegd worden als deze gegevens naar hun aard niet automatisch vastgelegd kunnen worden.¹⁴⁷ De nota van toelichting benoemt het journaal van de opsporingsambtenaar, maar ook de vastlegging van gebruikte scripts

¹³⁹ Bogw, nota van toelichting I, hoofdstuk 3.4 p.17.

¹⁴⁰ Art. 5 eerste lid sub a Bogw en artikelsgewijze toelichting artikel 5, p.36 waarin aangegeven is dat alle handelingen die tijdens het onderzoek in een geautomatiseerd werk plaatsvinden, worden gelogd.

¹⁴¹ Art. 1 lid g Bogw definieert de technische infrastructuur als een technische voorziening van een technisch team bedoeld voor de vastlegging van gegevens ter uitvoering van bevel.

¹⁴² Bogw, nota van toelichting, hoofdstuk 3.4 p.17.

¹⁴³ Art. 5 eerste lid sub b en d Bogw.

¹⁴⁴ Bogw, nota van toelichting, hoofdstuk 3.4 p.18.

¹⁴⁵ Art. 5 eerste lid sub c Bogw.

¹⁴⁶ Bogw, artikel 5, eerste lid en tweede lid.

¹⁴⁷ Bogw, artikel 5 tweede lid, handelingen naar hun aard niet automatisch vast te leggen; Bogw artikelsgewijze toelichting bij het Besluit, artikel 5, p.36; Bogw nota van toelichting hoofdstuk 3.4 p.17. "De inzetlogging zal zoveel mogelijk geautomatiseerd plaatsvinden. Voor zover dit technisch niet mogelijk is, wordt procedureel binnen de politieorganisatie vastgelegd dat handmatige logging plaatsvindt."

en softwareversies waarvan aannemelijk is dat vastlegging procedureel ingeregeld wordt.¹⁴⁸

De logging is in de eerste plaats van belang voor het uitvoeren van de interne controle door de politie op de verrichte handelingen en de controle op het functioneren van de technische infrastructuur.¹⁴⁹ Op basis van deze logging moet de politie zowel tijdens de uitvoering van een bevel als na afloop daarvan kunnen vaststellen of een onregelmatigheid¹⁵⁰ heeft plaatsgevonden die van invloed is op de betrouwbaarheid en integriteit van de ter uitvoering van het bevel geregistreerde en vastgelegde gegevens i.c. de vergaarde gegevens die kunnen dienen als bewijs in een strafzaak.¹⁵¹ In de memorie van antwoord is daarnaast aangevoerd dat de logging plaatsvindt met het oog op controle op de uitvoering zodat zowel tijdens het onderzoek als op een later moment geen twijfel kan bestaan over de aard en consequenties van de handelingen die zijn verricht bij de uitvoering van het bevel.¹⁵² In aansluiting daarop is in de nota van toelichting aangegeven dat de politie aan de hand van de logging verantwoording moet kunnen afleggen als, in een strafzaak of in het kader van het toezicht door de Inspectie JenV, twijfels ontstaan over de verrichte handelingen en/of de betrouwbaarheid van het hiermee vergaarde bewijs.¹⁵³ De logging is ook van belang mocht er sprake zijn van het optreden van schade en een mogelijke schadeclaim door betrokkene en in gevallen waarin twijfel ontstaat over de wijze waarop de gegevens zijn verkregen of over de betrouwbaarheid van de verkregen gegevens, bijvoorbeeld op grond van een verweer van de verdachte of diens raadsman.¹⁵⁴

Om effectief controle te kunnen uitoefenen en toezicht te kunnen houden, moet aan de hand van de logging van elke verrichte handeling een antwoord geformuleerd kunnen worden op het wie, wat, waar, wanneer, waarmee en op welke wijze handelingen uitgevoerd zijn. Om daaraan te kunnen voldoen, moet bij de inrichting van logging hieraan aandacht besteed worden.

N37 Gedurende de uitvoering van een bevel zijn doorlopend en automatisch gegevens in logbestanden vastgelegd over:

- a. de handelingen die worden verricht ter uitvoering van een bevel;*
- b. de toegang tot een technisch hulpmiddel;*
- c. de gegevens die al dan niet met een technisch hulpmiddel op de technische infrastructuur worden vastgelegd ter uitvoering van een bevel;*
- d. het functioneren van de technische infrastructuur.*

¹⁴⁸ Bogw, nota van toelichting hoofdstuk 3.4 p.17.

¹⁴⁹ Bogw, nota van toelichting, hoofdstuk 3.4, p.18; Bogw, Nota van Toelichting, hoofdstuk 3.4, p.18. In dat kader is tevens aangegeven dat voor het functioneren van de technische infrastructuur de systeemlogging gebruikt wordt voor het signaleren, onderzoeken en verhelpen van problemen met betrekking tot de betrouwbaarheid, integriteit en beschikbaarheid van de technische infrastructuur; *Kamerstukken I 2016/17, 34 372 D, pagina 20. "Op deze wijze kan zowel tijdens het verrichten van onderzoekshandelingen als achteraf intern toezicht plaatsvinden binnen de politieorganisatie op de uitvoering van het bevel van de officier van justitie."*

¹⁵⁰ Ten aanzien van het begrip onregelmatigheid verwijst de Inspectie naar hoofdstuk 8.

¹⁵¹ Art. 6 eerste lid Bogw, vaststelling van onregelmatigheden. nota van toelichting hoofdstuk 3.4 p.17.

¹⁵² *Kamerstukken I 2016/17, 34 372 D, pagina 6.*

¹⁵³ Bogw, nota van toelichting I, hoofdstuk 4, artikel 6 pagina 36. Vaststelling van onregelmatigheden.

¹⁵⁴ *Kamerstukken II 2016/17 34 372, nr.6, p.69 en p.80.*

Eisen m.b.t. betrouwbaarheid logbestanden

Gelet op het belang van de logging schrijft het Besluit voor dat de inhoud van logbestanden niet gewijzigd kan worden en dat de toegang tot logbestanden beperkt is tot alleen daartoe geautoriseerde personen.¹⁵⁵ Een uitwerking hiervan is dat de doorlopende en automatische logging over de uitgevoerde handelingen vastgelegd worden op een server van de politie en dat leden van het technisch team geen toegang tot de logbestanden hebben.¹⁵⁶ De politie dient maatregelen te treffen om te voorkomen en dat onbevoegde wijziging of kennisneming van de logbestanden heeft plaatsgevonden en ook om dit achteraf te kunnen vaststellen. Hieruit vloeit voort dat om dit achteraf te kunnen vaststellen er mogelijk gebruik gemaakt moet kunnen worden van security logging die niet onder de categorieën valt zoals benoemd in art. 5 lid 1 sub a Bogw.

Een voorwaarde voor het kunnen treffen van passende maatregelen is dat de politie vanuit een ontwerp vastgelegd heeft op welke wijze invulling gegeven wordt aan de bedoelde doorlopende en automatische logging en op welke locaties sprake is van de opslag, transport en verwerking van deze gegevens en logbestanden. Zie norm N37. Deze uitwerking en onderbouwing is van belang om te kunnen komen tot het treffen van aantoonbaar passende maatregelen voor het borgen van de betrouwbaarheid en integriteit van de logbestanden, het afleggen van verantwoording over de implementatie daarvan en het effectief uitvoeren van de eigen interne controle. Verantwoording daaromtrent is ook van belang voor het toezicht door de Inspectie op de volledigheid van de vastlegging van gegevens in logbestanden en of de juiste gegevens daartoe worden vastgelegd.

N38 *Voor de vastlegging van gegevens in logbestanden zijn maatregelen getroffen om wijziging van de logbestanden of kennisneming hiervan door onbevoegden te voorkomen en achteraf te kunnen vaststellen of wijziging of kennisneming heeft plaatsgevonden.*

Het loggingsproces is zo ingericht dat de loggingsinformatie tijdens de fase van bewijsvergaring te allen tijde blijft functioneren en niet valt te manipuleren, te wijzigen of te verwijderen zonder dat dit achteraf zichtbaar is.¹⁵⁷ De Inspectie merkt op dat het hier de logvoorziening als geheel betreft en niet de individuele logbestanden. Bijvoorbeeld door het treffen van maatregelen om te voorkomen dat logininstellingen ten behoeve van de werking van het logmechanisme aangepast worden die kunnen leiden tot het niet of niet volledig meer loggen van gebeurtenissen.

N39 *Het loggingsproces is zo ingericht dat de loggingsinformatie tijdens de fase van bewijsvergaring te allen tijde blijft functioneren en niet valt te manipuleren, te wijzigen of te verwijderen.*

¹⁵⁵ Art. 7 Bogw en de artikelsgewijze toelichting op het Besluit artikel 7, p.37. Art. 7 tweede lid Bogw stelt dat logbestanden uitsluitend toegankelijk moeten zijn voor door de korpschef aangewezen ambtenaren.

¹⁵⁶ *Kamerstukken II* 2016/17, 34372 nr. 6, p. 52 en p.59.

¹⁵⁷ *Kamerstukken II* 2016/17, 34 372, nr. 6, p.52 en p.59.

7 Technische infrastructuur en bewijslogging

Door het technisch team verzamelde gegevens die kunnen dienen als bewijs in een strafzaak moeten vastgelegd worden op een technische infrastructuur. Voor deze gegevens die gedurende de onderzoeksfase geregistreerd en vastgelegd zijn, hanteert de nota van toelichting het begrip bewijslogging. Deze gegevens, die al dan niet met een technisch hulpmiddel zijn verkregen, dienen conform het Besluit vastgelegd te worden op een technische infrastructuur.¹⁵⁸ Het is niet voorgeschreven dat de logbestanden (zie hoofdstuk 5, handelingen etc.) vastgelegd moeten worden op de technische infrastructuur. Het Besluit definieert de technische infrastructuur als een technische voorziening van een technisch team bedoeld voor de vastlegging van gegevens ter uitvoering van een bevel.¹⁵⁹

Het begrip technische infrastructuur wordt in het Besluit in verband gebracht met diverse onderwerpen waaronder de (bewijs)logging, onregelmatigheden, selectie van gegevens, data overdracht, technische hulpmiddelen en verwijdering en vernietiging van gegevens. Het Besluit stelt eisen aan een technische infrastructuur. Om bij deze onderwerpen te kunnen komen tot een juiste invulling en afweging, is het van belang dat de reikwijdte van de technische infrastructuur door de politie eenduidig bepaald en vastgelegd is. De politie heeft dit bovenal zelf nodig om te kunnen komen tot het treffen van passende maatregelen en uitvoering te kunnen geven aan eigen controles op de naleving hiervan. Deze reikwijdte van de technische infrastructuur kan overigens per zaak verschillen. Het bepalen van de reikwijdte omvat een concretisering en vastlegging van welke systemen, toepassingen en infrastructuren onderdeel vormen van de technische infrastructuur.

Eisen m.b.t. betrouwbaarheid technische infrastructuur en bewijslogging

De vastlegging van de in de onderzoeksfase geregistreerde gegevens vindt plaats op een technische infrastructuur. De gegevens die tijdens de onderzoeksfase worden vastgelegd, kunnen worden gebruikt als bewijs in een strafzaak. Gelet hierop dienen de betrouwbaarheid en integriteit van de gegevens onomstotelijk vast te staan, zowel in het belang van de betrokkene als in het belang van de opsporing.¹⁶⁰

De technische infrastructuur moet in staat zijn om het unieke gegeven dat door het technisch hulpmiddel aan de geregistreerde gegevens is toegevoegd, te herkennen. Op deze wijze kan een herleidbaar gegevensspoor worden gecreëerd en daarmee de herkomst van de vastgelegde gegevens vastgesteld worden. Bij de vastlegging van de gegevens op de technische infrastructuur moet de datum en tijd van vastlegging worden geregistreerd.¹⁶¹ Hierdoor ontstaat zekerheid over de datum en het tijdstip van

¹⁵⁸ Art. 27 eerste lid Bogw. Vastlegging van gegevens op een technische infrastructuur.

¹⁵⁹ Artikel 1 lid g Bogw, definitie van een technische infrastructuur.

¹⁶⁰ Nota van toelichting Bogw hoofdstuk 3.7, p.21.

¹⁶¹ Art. 27 derde lid Bogw. In de toelichting op dit artikel p.47 is aangegeven dat daardoor zekerheid bestaat over de datum en tijdstip van vastlegging.

vastlegging. Dit impliceert dat de technische infrastructuur kan beschikken over een voorziening waarmee een nauwkeurige en betrouwbare tijd verkregen kan worden.

N40 De vastlegging van de tijdens het onderzoek geregistreerde gegevens vindt plaats op een technische infrastructuur, waarbij het unieke kenmerk en de datum en tijd van vastlegging wordt geregistreerd.

De veiligheid van de technische infrastructuur is voor de opsporingsinstanties van groot belang omdat het compromitteren hiervan van invloed kan zijn op de integriteit van de gegevens die kunnen dienen als bewijs in een strafzaak. Om de betrouwbaarheid, integriteit en herleidbaarheid van de bewijslogging te borgen, heeft de wetgever eisen gesteld aan deze technische infrastructuur en de gegevens die daarin vastgelegd worden.¹⁶² De politie moet maatregelen treffen om aan deze eisen te voldoen. De gegevens mogen niet inhoudelijk worden bewerkt en dienen te worden beveiligd tegen wijziging en kennisneming door onbevoegden. De vastgelegde gegevens zijn uitsluitend toegankelijk voor de door de korpschef aangewezen ambtenaren. Tactische opsporingsambtenaren hebben daartoe geen toegang.¹⁶³ Vereist is dat de opslag van deze gegevens uitsluitend plaatsvindt op een beveiligde politieserver in beheer van de politie die zich in Nederland bevindt.¹⁶⁴ Voor de opslag van onderzoeksgegevens op de technische infrastructuur van de politie wordt geen gebruik gemaakt van een server van de leverancier van de (onderzoeks)software.¹⁶⁵

Onder betrouwbaarheid wordt verstaan de mate waarin de gegevens integer (juist en volledig) zijn en toegang tot de gegevens beperkt is (exclusiviteit/vertrouwelijkheid). Met beperking van toegang wordt bedoeld op het beperken van kennisname van de gegevens door onbevoegden (exclusiviteit/vertrouwelijkheid), maar ook het voorkomen dat vastgelegde gegevens gewijzigd kunnen worden (integriteit). Daarnaast is de herleidbaarheid van de bewijslogging van belang zodat te allen tijde vastgesteld kan worden hoe, door middel van welke handelingen, wanneer en door wie de bewijslogging is verkregen.

Ook bedreigingen die behoren bij de kwaliteitsaspecten beschikbaarheid en continuïteit kunnen een effect hebben op de integriteit van de gegevens vastgelegd in logbestanden en de bewijslogging. De Inspectie doelt in dit kader op de mogelijke negatieve gevolgen voor de integriteit van de gegevens door het (tijdelijk) niet beschikbaar zijn van gegevensverwerkende voorzieningen. Met andere woorden: hoe wordt door de politie omgegaan met een situatie waarin gegevens niet afgeleverd kunnen worden door (tijdelijke) onbeschikbaarheid in de transport- en verwerkingsketen. Hoe wordt in die situatie zorggedragen dat gegevens niet verloren raken, tussentijds integer blijven en na afloop van de onbeschikbaarheid alsnog integer vastgelegd worden. Een andere situatie is dat de vastgelegde gegevens zelf niet meer beschikbaar of integer zijn. Bijvoorbeeld door een virus besmetting of

¹⁶² Artt. 27 en 28 Bogw. Betrouwbaarheid en integriteit van een technische infrastructuur; *Kamerstukken II* 2015/16, 34 372, nr.3 p.110. "De gegevens worden onverwijld naar de politieserver gezonden en automatisch voorzien van een digitale handtekening (hashcode), zodat de gegevens daarna niet kunnen worden gewijzigd zonder dat dit zichtbaar is. De server bij de politie dient binnen een beveiligde omgeving te zijn geplaatst en aan bepaalde eisen te voldoen ter voorkoming van manipulatie van de gegevens."

¹⁶³ Bogw, artikelsgewijze toelichting bij het Besluit, artikelen 27 en 28, p.47.

¹⁶⁴ Bogw, nota van toelichting, hoofdstuk 3.5 p. 18; Bogw, nota van toelichting, artikelsgewijze toelichting artikel 27 en 28; *Kamerstukken II* 2016/17, 34 372, nr.6, p.74.; *Kamerstukken II* 2018/19, 34. 372, nr. 29 p. 11 en p. 12.

¹⁶⁵ *Kamerstukken II* 2018/19, 34 372, nr. 29, p.12.

technische problemen met verlies of beschadiging van vastgelegde gegevens tot gevolg. Als repressieve maatregel kan hiervoor herstel middels back-up en restore plaatsvinden. De vraag is dan hoe door de politie zeker gesteld is dat de back-ups betrouwbaar (juist en volledig) zijn en dat het terugzetten van de door middel van een back-up veiliggestelde gegevens (restore) betrouwbaar verloopt en data verlies geminimaliseerd is. Het ligt voor de hand dat DIGIT deze bedreigingen meeneemt in een risicoanalyse die leidt tot een samenhangend en passend pakket van te treffen beheersingsmaatregelen. De Inspectie zal voor haar toezicht in beginsel nagaan of deze bedreigingen door DIGIT onderkend zijn en welke maatregelen daartoe voorzien zijn. Zie tevens hoofdstuk 12 (kwaliteitssysteem en interne controle).

In het belang van de betrouwbaarheid, integriteit en herleidbaarheid van de gegevens en het bepalen welke maatregelen, waar nodig zijn, dient de politie zicht en grip te hebben op de gehele keten van opslag, transport en verwerking van de bewijslogging gegevens. Denk hierbij bijvoorbeeld ook aan back-ups en het terugzetten hiervan middels restore procedures. Maar ook het in kaart brengen van andere locaties waar deze gegevens zich bevinden zoals USB-sticks en de diverse omgevingen waarvan door het technisch team gebruik gemaakt wordt. Dit inzicht vormt een randvoorwaarde voor de politie om passende beheersingsmaatregelen te kunnen identificeren, te implementeren en toe te zien op naleving daarvan.

N41 De politie treft maatregelen om wijzigingen van de vastgelegde gegevens of kennisneming hiervan door onbevoegden te voorkomen en achteraf te kunnen vaststellen of wijziging of kennisneming hiervan heeft plaatsgevonden. Er worden passende technische en organisatorische maatregelen getroffen om het beveiligingsniveau te waarborgen dat op het risico afgestemd is.

8 Onregelmatigheden

In een aantal artikelen van het Besluit is sprake van het (kunnen) constateren van het plaatsvinden van een onregelmatigheid. Een definitie of concrete voorbeelden van wat als een onregelmatigheid beschouwd moet worden, ontbreekt in het Besluit. Wel is bij de beantwoording van Kamervragen aangegeven dat ondanks maatregelen het kan voorkomen dat er technische aanwijzingen zijn dat het bewijs door onbevoegden is geraadpleegd of gewijzigd. In een dergelijk geval dient in het proces-verbaal te worden opgenomen dat deze aanwijzingen er zijn en, indien mogelijk, welk effect deze aanwijzingen hebben op de integriteit van het bewijs.¹⁶⁶ In een ander kamerstuk wordt als voorbeeld van een onregelmatigheid de situatie genoemd waarin een verschil ontstaat in de geregistreerde tijd, bijvoorbeeld door onderbreking van het loggingsproces.¹⁶⁷

Onregelmatigheid i.r.t. impact op bewijslogging

Binnen het werkingsgebied van Bogw artikel 6 is een onregelmatigheid omschreven als een gebeurtenis die van invloed is op de betrouwbaarheid en integriteit van de ter uitvoering van het bevel vastgelegde gegevens op een technische infrastructuur.¹⁶⁸ Het plaatsvinden van deze onregelmatigheden moet zowel tijdens de uitvoering van het bevel als na afloop daarvan aan de hand van logbestanden vastgesteld kunnen worden.¹⁶⁹ Zie hoofdstuk 6 (gegevens vastgelegd in logbestanden). Een randvoorwaarde om onregelmatigheden aan de hand van logging adequaat te kunnen signaleren, is dat in beeld is welke gebeurtenissen als onregelmatigheid aangemerkt moeten worden. Op basis hiervan kan de logging zodanig worden ingericht dat de juiste informatie gelogd wordt om deze onregelmatigheden te kunnen signaleren. Hierbij is er een relatie met de wijze waarop de doorlopende en automatische logging van gegevens vastgelegd in logbestanden plaatsvindt. Zie hoofdstuk 6. Deze wijze en de inrichting daarvan kan overigens per zaak verschillen.

N42 *De logging en controle is zodanig ingericht dat vastgesteld kan worden of onregelmatigheden plaatsvinden.*

De bovenstaande norm betreft hier zowel onregelmatigheden die mogelijk van invloed zijn op de juistheid, volledigheid en herleidbaarheid van de ter uitvoering van een bevel geregistreerde en vastgelegde gegevens alsmede het plaatsvinden van onregelmatigheden tijdens plaatsing van een technisch hulpmiddel of bij het verrichten van onderzoekshandelingen. Dit wordt bij het kopje "onregelmatigheden in bredere zin" nader toegelicht.

¹⁶⁶ Kamerstukken I 2016/17, 34372 F, p.10. Nader voorlopig verslag van de vaste commissie voor veiligheid en justitie; Kamerstukken I 2017/18, 34372 G, p.23 nadere memorie van antwoord.

¹⁶⁷ Kamerstukken II 2016/17, 24 372, nr.6 p. 52.

¹⁶⁸ Art. 6 eerste lid Bogw (vaststelling van onregelmatigheden); Bogw nota van toelichting hoofdstuk 3.4 p. 17 "of een onregelmatigheid heeft plaatsgevonden die van invloed is op de betrouwbaarheid en integriteit van de ter uitvoering van het bevel geregistreerde en vastgelegde gegevens.". In de artikelsgewijze toelichting op het artikel bij artikel 6, p.36 is dit omschreven als een "onregelmatigheid die van invloed is op de betrouwbaarheid van de met de onderzoekshandelingen verkregen gegevens".

¹⁶⁹ In art. 5 eerste lid Bogw en de nota van toelichting op het Besluit, hoofdstuk 3.4 p.17 is aangegeven welke logbestanden dit betreft.

Het Besluit geeft op basis van artikel 6 geen directe aanwijzing wie deze controle moet uitoefenen op het plaatsvinden van onregelmatigheden. Wel is aangegeven dat van het constateren van een onregelmatigheid door een opsporingsambtenaar van een technisch team proces-verbaal op moet worden gemaakt.¹⁷⁰ In de praktijk treedt de opsporingsambtenaar bij constatering van een dergelijke gebeurtenis in overleg met de DIGIT OvJ en beoordeelt de DIGIT OvJ of deze gebeurtenis een onregelmatigheid is. In die situatie gaat de opsporingsambtenaar over tot het opmaken van een proces-verbaal. In de nota van toelichting op het Besluit is daarnaast aangegeven dat de logging ten eerste en vooral bedoeld is voor de interne controle van de tijdens de uitvoering van het bevel verrichte handelingen en het functioneren van de technische infrastructuur.¹⁷¹

Tevens is tijdens de beantwoording van vragen op het wetsvoorstel CCIII door de minister aangegeven dat tijdens de uitvoering van het bevel tot het op afstand binnendringen van een geautomatiseerd toezicht wordt uitgeoefend door de leidinggevende functionarissen binnen de opsporingsdienst en door de betrokken officier van justitie.¹⁷²

Uit de nota van toelichting kan worden afgeleid dat de verantwoordelijkheid voor het constateren van onregelmatigheden en de controle op het plaatsvinden daarvan primair is belegd bij de politieorganisatie.¹⁷³ De Inspectie houdt toezicht op de kwaliteit van de taakuitvoering door de politie. Deze interne controle van gegevens in logbestanden is een randvoorwaarde voor het borgen van deze kwaliteit.

Het is uiteindelijk aan de officier van justitie en de rechter om te beoordelen in hoeverre de geconstateerde onregelmatigheid afbreuk doet aan de bewijskracht van de gegevens.¹⁷⁴

N43 De politie controleert aan de hand van de gegevens in de logbestanden of onregelmatigheden hebben plaatsgevonden.

De bovenstaande norm betreft hier zowel onregelmatigheden die mogelijk van invloed zijn op de betrouwbaarheid en integriteit van de ter uitvoering van een bevel vergaarde gegevens, die kunnen dienen als bewijs in een strafzaak alsmede het plaatsvinden van onregelmatigheden tijdens plaatsing van een technisch hulpmiddel of bij het verrichten van onderzoekshandelingen. Dit wordt hieronder verder toegelicht.

Onregelmatigheden in bredere zin

De begripsbepaling van een onregelmatigheid is niet beperkt tot alleen de gebeurtenissen die (negatieve) invloed hebben op de betrouwbaarheid en integriteit van de 'bewijslogging'. Aan de hand van de formulering in het Besluit is af te leiden

¹⁷⁰ Art. 6 tweede lid Bogw en nota van toelichting hoofdstuk 3.4, p.18.

¹⁷¹ Bogw, nota van toelichting op het Besluit hoofdstuk 3.4, p.18. Ook in het verslag van het schriftelijk overleg (kamerstuk 34372 nr. 27 p.11 en p.12) wordt het uitvoeren van interne controle los gezien van het toezicht dat door de Inspectie wordt uitgevoerd.

¹⁷² Kamerstukken II 2016/17, 34 372, nr.6, p.59.

¹⁷³ In de nota van toelichting op het Besluit hoofdstuk 3.4. p.18 is aangegeven dat de Inspectie Justitie en Veiligheid in het kader van haar toezichthoudende taak met gebruikmaking van de logging onderzoek kan doen naar eventuele onregelmatigheden bij de uitvoering van het onderzoek in een geautomatiseerd werk. De Inspectie benadrukt dat haar systeemtoezicht niet dient ter vervanging van de interne controlemechanismen, het interne kwaliteitssysteem en daarmee de eigen verantwoordelijkheid die de politieorganisatie daarin heeft.

¹⁷⁴ Bogw, nota van toelichting op het Besluit hoofdstuk 3.4, p. 18.

dat er ook sprake kan zijn van andere onregelmatigheden die geen invloed hebben op de betrouwbaarheid en integriteit van de bewijslogging.¹⁷⁵ Van het plaatsvinden van gebeurtenissen die geen directe invloed hebben op de betrouwbaarheid en integriteit van de 'bewijslogging' maar wel vallen binnen de reikwijdte van artikel 7 moeten krachtens het derde lid van artikel 7 maatregelen getroffen worden om achteraf te kunnen vaststellen of bedoelde gebeurtenissen hebben plaatsgevonden. Het betreft het optreden van wijziging en onbevoegde kennisname van gegevens vastgelegd in logbestanden. Deze gebeurtenissen kunnen derhalve ook als onregelmatigheid aangemerkt worden, echter zonder de in artikel 6 bedoelde directe impact op de bewijslogging. Met andere woorden: De onregelmatigheden die van invloed zijn op de betrouwbaarheid en integriteit van de bewijslogging vormen een subset van de gebeurtenissen die onder het begrip onregelmatigheden worden verstaan.

Het Besluit benoemt dat de opsporingsambtenaar melding maakt in het proces-verbaal van onregelmatigheden die plaatsvinden bij de plaatsing van een technisch hulpmiddel of bij het verrichten van onderzoekshandelingen. Hieruit kan afgeleid worden dat de opsporingsambtenaar van het technisch team die deze handelingen verricht, zelf verantwoordelijk is voor het constateren van de onregelmatigheid en het vermelden daarvan, bijvoorbeeld in het journaal. In de artikelsgewijze toelichting op het Besluit is daarbij aanvullend aangegeven dat via de logging controle kan worden uitgeoefend op het plaatsen van een technisch hulpmiddel en op de verrichte onderzoekshandelingen.¹⁷⁶ De verantwoordelijkheid voor deze controlerende taak aan de hand van logging is ook hier op de eerste plaats belegd bij de politie zelf.

Een eenduidige vastlegging van de gebeurtenissen die in dit kader als onregelmatigheid beschouwd moeten worden, is randvoorwaardelijk om te waarborgen dat deze onregelmatigheden altijd en op uniforme wijze door de opsporingsambtenaar gemeld worden. Op basis van dat vastgelegde referentiekader kan de opsporingsambtenaar bepalen of tijdens het uitvoeren van deze handelingen sprake is van een onregelmatigheid waarvan melding gemaakt moet worden in het proces-verbaal. Zie hoofdstuk 9 voor de kaders van een proces-verbaal.

Daarnaast dient logging beschikbaar en op een zodanige wijze ingericht te zijn dat de politie vanuit een eigen controlerende taak kan constateren of deze onregelmatigheden opgetreden zijn.

De Inspectie merkt op dat voor het constateren van deze onregelmatigheden mogelijk gebruik gemaakt kan worden van dezelfde logbestanden die gebruikt worden om het plaatsvinden van de eerdergenoemde onregelmatigheden met een impact op de bewijslogging te signaleren.

De toetsingselementen voor deze onregelmatigheden vormen onderdeel van normen N41 (reikwijdte gebeurtenissen), N42 (vertaling naar inrichting) en N43 (uitvoeren van controles).

¹⁷⁵ Art. 6 eerste lid Bogw. Er zijn in het Besluit echter nog enkele andere bepalingen waar het begrip onregelmatigheid benoemd is. De directe relatie met de invloed van een onregelmatigheid op de betrouwbaarheid en integriteit van de 'bewijslogging' wordt daar echter niet gelegd; Bogw artt. 23 vierde lid en artikel 24 derde lid voor respectievelijk het plaatsen van een technisch hulpmiddel en het verrichten van onderzoekshandelingen.

¹⁷⁶ Bogw artikelsgewijze toelichting artikel 23 en 24, p.46.

9 Proces-verbaal

Een proces-verbaal is een officieel op papier gesteld verslag van de politie.¹⁷⁷ Een proces-verbaal vormt samen met het journaal en de elektronische logging een belangrijke waarborg voor de controlebaarheid van de uitvoering van het bevel.¹⁷⁸ De verbaliseringsplicht houdt in dat de opsporingsambtenaren proces-verbaal opmaken van de door hen verrichte handelingen zodat daarover verantwoording afgelegd kan worden.¹⁷⁹ In het journaal wordt door de opsporingsambtenaren, als een soort dagboek, handmatig verslaglegging gedaan over het procesverloop, de afspraken en de verrichtingen die zich niet lenen voor automatische vastlegging. Het journaal is een intern werkdocument van de politie dat niet bij de processtukken hoeft te worden gevoegd.¹⁸⁰

Volgens het Besluit dienen opsporingsambtenaren als onderdeel van de inzet van de hackbevoegdheid een proces-verbaal op te stellen voor een aantal specifiek omschreven handelingen en gebeurtenissen.

Het betreft de volgende handelingen en gebeurtenissen:

art. 6.2	Onregelmatigheden. Indien een onregelmatigheid wordt geconstateerd maakt een opsporingsambtenaar van een technisch team daarvan proces-verbaal op, dat aan de officier van justitie wordt gezonden. Zie tevens hoofdstuk 8 over de context en definitie van onregelmatigheden en de randvoorwaarden voor logging die daarmee mee samen hangen.
art 23.3	Plaatsing Technisch Hulpmiddel (TH). De opsporingsambtenaar maakt proces-verbaal op van de plaatsing, dat aan de officier van justitie wordt gezonden. In de nota van toelichting op het Besluit is aangegeven dat in het proces-verbaal van plaatsing verantwoording wordt afgelegd over het inschakelen van de in het bevel van de officier aangeduide functionaliteiten en de naleving van de door keuringsdienst opgestelde handleiding voor het gebruik van het hulpmiddel, waaronder de gehanteerde instellingen bij het gebruik van een technisch hulpmiddel voor een bepaalde functionaliteit. ¹⁸¹
art 23.4	Plaatsing TH. Indien bij de plaatsing van een technisch hulpmiddel een onregelmatigheid plaatsvindt, maakt de opsporingsambtenaar hiervan melding in het proces-verbaal.
art 24.2	Verrichten onderzoekshandelingen. De opsporingsambtenaar maakt proces-verbaal op van het verrichten van onderzoekshandelingen, dat aan de officier van justitie wordt gezonden. In de toelichting van het Besluit is aangegeven dat in dit proces-verbaal ook verantwoording afgelegd wordt over de naleving van de te treffen vervangende waarborgen waarvan in een keuringsrapport van een goedgekeurd technisch hulpmiddel mogelijk sprake is. ¹⁸²
art 24.3	Verrichten onderzoekshandelingen. Indien bij het verrichten van onderzoekshandelingen een onregelmatigheid plaatsvindt, maakt de opsporingsambtenaar hiervan melding in het proces-verbaal.
art 25.3	Verwijdering TH. De opsporingsambtenaar maakt proces-verbaal op van de verwijdering, dat aan de officier van justitie wordt gezonden.

¹⁷⁷ <https://www.politie.nl/informatie/wat-is-een-proces-verbaal.html>

¹⁷⁸ Kamerstukken II 2015/16, 34372 nr. 3, p. 78.

¹⁷⁹ Kamerstukken II 2016/17 34 372, nr.6 p. 84.

¹⁸⁰ Aanwijzing opsporingsbevoegdheden. <https://wetten.overheid.nl/BWBR0035498/2014-09-01>

¹⁸¹ Bogw, nota van toelichting p. 38; Bogw artikelsgewijze toelichting p.46,

¹⁸² Bogw, artikelsgewijze toelichting, art. 18 p.43.

art 26.3	Verwijdering TH. De opsporingsambtenaar maakt proces-verbaal op van de niet of niet volledige verwijdering, dat aan de officier van justitie wordt gezonden. Van de stopzetting van de verbinding dient proces-verbaal te worden opgemaakt. ¹⁸³
art 29.3	Selectie van gegevens. Bij de selectie van gegevens legt een opsporingsambtenaar van een technisch team in een proces-verbaal vast welke bewerkingen hebben plaatsgevonden op de forensische kopie van de vastgelegde gegevens. Het proces-verbaal wordt aan de officier van justitie toegezonden.
art 4.4 ¹⁸⁴	Vernietiging gegevens. Als bij de uitoefening van een bijzondere opsporingsbevoegdheid een proces-verbaal of een ander voorwerp mededelingen bevat door of aan een verschoningsgerechtigde dan worden het betreffende proces-verbaal of voorwerp vernietigd. Het bevel van de officier van justitie tot vernietiging is schriftelijk. Van de vernietiging wordt proces-verbaal opgemaakt, dat wordt gezonden aan de officier van justitie.

Het Wetboek van Strafvordering stelt eisen aan de verslaglegging door opsporingsambtenaren en de inhoud van een proces-verbaal.¹⁸⁵ De met de opsporing van strafbare feiten belaste ambtenaren maken ten spoedigste proces-verbaal op van het door hen opgespoorde strafbare feit of van hetgeen door hen tot opsporing is verricht of bevonden. Het opmaken van proces-verbaal kan onder verantwoordelijkheid van het openbaar ministerie achterwege worden gelaten.¹⁸⁶ Ingeval het opmaken van een proces-verbaal achterwege blijft, zal evenwel dienen te worden voorzien in een zodanige vastlegging van de desbetreffende verrichtingen en bevindingen, dat doeltreffend kan worden gereageerd op een verzoek van de rechter in het eindonderzoek tot nadere verantwoording omtrent dat onderdeel van het opsporingsonderzoek.¹⁸⁷ Het proces-verbaal wordt op ambtseed of -belofte¹⁸⁸, persoonlijk opgemaakt, gedagtekend en ondertekend; daarbij moeten tevens zoveel mogelijk uitdrukkelijk worden opgegeven de redenen van wetenschap.

De door de opsporingsambtenaren opgemaakte processen-verbaal moeten onverwijld gezonden worden aan de officier van justitie.¹⁸⁹ Toezending kan met instemming van de officier van justitie achterwege worden gelaten.

N44 De opsporingsambtenaar maakt van door hem verrichte handelingen en eventueel geconstateerde onregelmatigheden ten spoedigste proces-verbaal op dat aan de officier van justitie wordt gezonden.

¹⁸³ Kamerstukken II 2016/17 34 372, nr.6 p. 80.

¹⁸⁴ Kamerstukken II 2016/17 34 372, nr.6 p. 37 en Besluit bewaren en vernietigen niet-gevoegde stukken, artikel 4 vierde lid.

¹⁸⁵ Zie wetboek van strafvordering art.152 (ten spoedigste), art. 153 (ambtseed, persoonlijk, gedagtekend, ondertekend en redenen van wetenschap), art. 156 (onverwijld toekomen).

¹⁸⁶ Zie wetboek van strafvordering art. 149b.

¹⁸⁷ Zie <https://bewijs-in-strafzaken.nl/verbaliseringsplicht-art-152-sv/>

¹⁸⁸ Art. 9 lid 1 en 2 Besluit algemene rechtspositie politie.

¹⁸⁹ Zie artt. 6 tweede lid, 23 derde lid, 24 tweede lid, 25 derde lid, 26 derde lid en 29 derde lid Bogw en art 156 Sv.

10 Bewerking en verstrekking van vastgelegde gegevens

De resultaten van het onderzoek worden door het technisch team ter beschikking gesteld aan het tactisch team belast met het opsporingsonderzoek. Uitsluitend de gegevens die binnen de reikwijdte van het bevel van de officier van justitie vallen, worden ter beschikking gesteld aan het tactisch onderzoeksteam.¹⁹⁰ Het kan hierbij nodig zijn om gegevens te filteren zodat binnen de categorieën van gegevens die in het bevel van de officier zijn opgenomen uitsluitend de gegevens die van belang zijn voor het opsporingsonderzoek ter beschikking komen van het tactische team.

Het technisch team draagt in dat geval zorg voor de selectie van onderzoeksgegevens.¹⁹¹ Het Besluit stelt dat bij het maken van een selectie van vastgelegde gegevens sprake is van een bewerking. Op grond van het Besluit moet deze bewerking plaatsvinden op basis van een forensische kopie van de vastgelegde gegevens op een technische infrastructuur.¹⁹² In het proces-verbaal legt de opsporingsambtenaar de bewerkingen vast die plaatsgevonden hebben op deze kopie. Zie hoofdstuk 9 voor de verslaglegging in een proces-verbaal.¹⁹³ Deze regels zijn van belang omdat de gegevens die tijdens de onderzoeksfase worden vastgelegd, kunnen worden gebruikt als bewijs in een strafzaak. Gelet hierop dienen de betrouwbaarheid en integriteit van de gegevens onomstotelijk vast te staan, zowel in het belang van de betrokkene als in het belang van de opsporing.¹⁹⁴

N45 *Alleen die gegevens die binnen de categorieën van gegevens in het bevel van de officier van justitie zijn opgenomen, zijn door het technisch team verstrekt aan een opsporingsambtenaar die is belast met het opsporingsonderzoek.*

N46 *Bij de selectie van gegevens is gebruikgemaakt van een forensische kopie van de ter uitvoering van het bevel vastgelegde gegevens.*

¹⁹⁰ Kamerstukken II 2016/17, 34 372, nr.6, p.14 en p.27.

¹⁹¹ Bogw, nota van toelichting hoofdstuk 3.3, p. 17.

¹⁹² Art. 29 Bogw en nota van toelichting hoofdstuk 3.7, p.21; Bogw, artikelsgewijze toelichting, artikel 29, p.48, "Selectie kan bijvoorbeeld aan de orde zijn bij het opnemen van vertrouwelijke communicatie of het aftappen en opnemen van telecommunicatie of de vastlegging van gegevens die in het geautomatiseerde werk zijn of worden opgeslagen, zoals email-verkeer. Hierbij kan niet worden uitgesloten dat gegevens worden verkregen over andere personen die bij de communicatie zijn betrokken. Deze gegevens zijn niet van belang voor het opsporingsonderzoek. Daarom wordt uitsluitend het email-verkeer waarvan de email-adressen zijn opgenomen op een vooraf opgestelde lijst ter beschikking gesteld van het tactische onderzoeksteam."

¹⁹³ Art. 29 derde lid Bogw.

¹⁹⁴ Art. 29 Bogw en nota van toelichting hoofdstuk 3.7, p.21; Bogw, artikelsgewijze toelichting, artikel 29, p.48.

11 Bewaartermijnen, verwijdering en vernietiging gegevens

De nota van toelichting bij het Besluit beschrijft de taak en de rol van de Inspectie met betrekking tot het toezicht op het functioneren van het wettelijke systeem rond de uitvoering van een bevel tot onderzoek in een geautomatiseerd werk.¹⁹⁵ Aangegeven is dat het toezicht van de Inspectie betrekking heeft op aspecten als de vastlegging, de beveiliging en het gebruik van gegevens, inclusief de bewaring en vernietiging daarvan.

In de toelichting bij het Bogw is beschreven dat op grond van andere wettelijke bepalingen de volgende eisen gelden voor bewaartermijnen, verwijdering en vernietiging van verzamelde gegevens:¹⁹⁶

- Zodra de gegevens niet langer noodzakelijk zijn voor het doel van het onderzoek, worden deze verwijderd of gedurende een periode van maximaal een half jaar bewaard teneinde te bezien of zij aanleiding geven tot een nieuw onderzoek.¹⁹⁷ De situatie dat de gegevens niet langer noodzakelijk zijn voor het doel van het onderzoek zal – in geval van een opsporingsonderzoek dat heeft geleid tot een vervolging – pas optreden op het moment dat de rechter ten aanzien van de zaak onherroepelijk heeft beslist.¹⁹⁸ Als de zaak niet is opgelost en niet is ingezonden aan het openbaar ministerie, wordt het onderzoek meestal wel voortgezet maar op een minder intensief niveau. De gegevens blijven dan doorgaans nodig voor het doel van het onderzoek tot uiterlijk het moment waarop de feiten, waar het onderzoek zich op richt zijn verjaard.¹⁹⁹ De gegevens die worden vastgelegd in het kader van een onderzoek in een geautomatiseerd werk vallen onder het regime van de Wet politiegegevens (Wpg). De Wpg kent regels over de bewaartermijnen van politiegegevens. De gegevens die worden verwerkt met het oog op de schending van de rechtsorde in een bepaald geval kunnen worden verwerkt voor zover dat noodzakelijk is voor het doel van het onderzoek. Dit betekent dat de gegevens kunnen worden bewaard totdat de verdachte onherroepelijk is veroordeeld.²⁰⁰ Na afloop van deze termijn worden de gegevens verwijderd.²⁰¹ De verwijderde politiegegevens worden gedurende een termijn van vijf jaren bewaard ten behoeve van verwerking met het oog op de afhandeling van klachten en de verantwoording van verrichtingen en vervolgens gearchiveerd of vernietigd.²⁰²
- Op grond van het Wetboek van Strafvordering geldt een speciale regeling voor de processen-verbaal en andere voorwerpen waaraan gegevens kunnen worden ontleend die zijn verkregen door observatie (doel c), het opnemen van vertrouwelijke communicatie (doel b, 126l) en het opnemen van telecommunicatie met behulp van een technisch hulpmiddel (doel b, 126m). Deze

¹⁹⁵ Bogw, nota van toelichting, hoofdstuk 5, p. 23-24 (Toezicht).

¹⁹⁶ Bogw, nota van toelichting, hoofdstuk 4, p. 22, (Gegevensverwerking)

¹⁹⁷ Als bedoeld in artikel 9 eerste lid Wpg of een nieuwe verwerking als bedoeld in artikel 10 Wpg.

¹⁹⁸ Nota van Toelichting, hoofdstuk 4, p. 22.

¹⁹⁹ Bogw, nota van toelichting, hoofdstuk 4, p. 22.

²⁰⁰ *Kamerstukken II* 2016/17, 34 372, nr. 6, p.41.

²⁰¹ Art. 9 lid 4 Wet politiegegevens.

²⁰² Art. 14 eerste lid Wet politiegegevens.

stukken worden door de officier van justitie, voor zover die niet bij de processtukken zijn gevoegd, ter beschikking gehouden van het onderzoek.²⁰³ Zodra twee maanden zijn verstreken nadat de zaak is geëindigd en de notificatie, bedoeld in artikel 126bb Sv is verricht, doet de officier van justitie de processen-verbaal en andere voorwerpen vernietigen.²⁰⁴ Op grond van deze notificatieplicht moet de betrokkene schriftelijk door de officier van justitie in kennis gesteld worden van het feit dat heimelijk is binnengedrongen in een geautomatiseerd werk en onderzoekshandelingen zijn verricht. Deze notificatie is niet vereist als het proces-verbaal van de toepassing van een bijzondere opsporingsbevoegdheid bij de processtukken wordt gevoegd of als mededeling redelijkerwijs niet mogelijk is.²⁰⁵ Van de vernietiging wordt proces-verbaal opgemaakt, dat wordt gezonden aan de officier van justitie.²⁰⁶

- Indien een opsporingsambtenaar bij de uitoefening van de bevoegdheid kennisneemt van mededelingen waarvan hij weet of redelijkerwijs kan vermoeden dat deze zijn gedaan door of aan een geheimhouder, dan stelt hij hiervan de officier van justitie onverwijld in kennis.²⁰⁷ De officier van justitie kan vervolgens bevelen terstond de processen-verbaal en andere voorwerpen te vernietigen.²⁰⁸

De kern van bovenstaande in relatie tot het handelen door de politie is dat verwijdering of vernietiging van gegevens door de politie op aangeven van de officier van justitie plaatsvindt of wettelijke bepalingen die daartoe verplichten.

Vanuit de kwaliteit van de taakuitvoering vloeit voort dat de politie haar processen, procedures en technische voorzieningen zodanig inricht en toepast dat op het moment dat de officier van justitie daartoe verzoekt, gegevens tijdig, juist en volledig worden vernietigd en verwijderd. Ook geldt hierbij dat deze gegevens juist en volledig bewaard en toegankelijk zijn en blijven gedurende de periode dat dat vereist wordt. Voor wat betreft maatregelen voor het naleven van de bewaartermijnen kan bijvoorbeeld worden gedacht aan een continuïteitsplan en maatregelen zoals back-up en restore. Voor de bewaartermijnen is sprake van een gedifferentieerd regime.²⁰⁹

Dit vraagt om een uitwerking van de wijze waarop verwijdering, vernietiging en naleving van bewaartermijnen van deze gegevens in de praktijk moet worden uitgevoerd en wat dat betekent voor gegevens die op diverse plaatsen zijn vastgelegd.

N47 *De politie richt de werkprocessen, procedures en technische voorzieningen op een dusdanige wijze in en past deze zodanig toe dat gegevens tijdig, juist en volledig worden verwijderd en vernietigd. Ook geldt hierbij dat gegevens juist en volledig bewaard en toegankelijk zijn en blijven gedurende de periode dat dat vereist wordt.*

²⁰³ Art. 126cc eerste lid Sv.

²⁰⁴ Art. 3 eerste lid Besluit bewaren en vernietigen niet-gevoegde stukken; nota van toelichting Bogw, hoofdstuk 4, p.23.

²⁰⁵ Art. 126bb eerste en derde lid Sv.

²⁰⁶ *Kamerstukken II* 2016/17 34 372, nr.6 p. 37; Besluit bewaren en vernietigen niet-gevoegde stukken, artikel 4 vierde lid.

²⁰⁷ Art. 4 eerste lid Besluit bewaren en vernietigen niet-gevoegde stukken.

²⁰⁸ Art. 126aa tweede lid Sv. Op grond van Titel IVA geldt een verplichting tot vernietiging van gegevens die mededelingen bevatten, gedaan door of aan een verschoningsrechtigde; *Kamerstukken II* 2016/17, 34 372, nr.6 p. 6, p. 17 en p.37; Art. 4 tweede lid Besluit bewaren en vernietigen niet-gevoegde stukken.

²⁰⁹ Zie Bogw p.22.

Een opsporingsambtenaar moet de officier van justitie informeren zodra hij kennisneemt van mogelijke mededelingen gedaan aan of door zogenaamde verschoningsgerechtigden, ook wel geheimhouders genoemd.

N48 Zodra de opsporingsambtenaar bij het onderzoek van de opgeslagen gegevens kennisneemt van mededelingen waarvan hij weet of redelijkerwijs kan vermoeden dat deze zijn gedaan door of aan een geheimhouder, stelt hij de officier van justitie hiervan onverwijld in kennis.

12 Kwaliteitssysteem en interne controle

De betrouwbaarheid, integriteit en herleidbaarheid van gegevens is cruciaal voor het gebruik van de verkregen gegevens als bewijs in een strafzaak.²¹⁰ Het Besluit hecht dan ook een groot belang aan het borgen van de betrouwbaarheid, integriteit en herleidbaarheid van bewijslogging en de gegevens vastgelegd in logbestanden. Hiertoe dienen volgens het Besluit maatregelen getroffen te worden om onbevoegde kennisname en het wijzigen van deze gegevens te voorkomen en om achteraf te kunnen vaststellen of hiervan sprake was.

Voor de vastlegging van de bewijslogging schrijft het Besluit voor dat dit op een technische infrastructuur plaatsvindt. Het Besluit benadrukt dat de veiligheid van de technische infrastructuur van groot belang is omdat het compromitteren hiervan van invloed kan zijn op de integriteit van het bewijs.²¹¹

De minister heeft daarnaast in een reactie op vragen van de vaste commissie aangegeven dat voor de beveiligde omgeving waar de onderzoeksgegevens worden weggeschreven, zwaardere fysieke en cryptografische beveiligingseisen gelden dan de gebruikelijke eisen voor de digitale infrastructuur van de politie.²¹² Aangegeven is dat in het algemeen de veiligheidsstandaarden voor de digitale infrastructuur van de politie dan ook moeten voldoen aan hoge standaarden.

De Politiewet biedt een aanknopingspunt om te komen tot een nadere invulling van dit hoge beveiligingsniveau en de veiligheidsstandaarden. In artikel 23 van de Politiewet 2012 is aangegeven dat bij ministeriële regeling regels gesteld kunnen worden over de informatiebeveiliging door de politie. Deze regeling is uitgewerkt in de Regeling Informatiebeveiliging Politie (RIP).²¹³

De regeling is van toepassing op het gehele proces van informatievoorziening en de gehele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. In de RIP is geregeld dat voor elk informatiesysteem door middel van een risicoanalyse bepaald moet worden welk stelsel van passende technische en organisatorische maatregelen getroffen moet worden. De te treffen beveiligingsmaatregelen moeten vervolgens in lijn met het RIP vastgelegd worden in een informatiebeveiligingsplan waarna controle op de kwaliteit van implementatie en controle op naleving ingericht moet zijn.

Voor invulling van het RIP heeft de politie zich gecommitteerd aan de Baseline Informatiebeveiliging Overheid (BIO) en zijn in een addendum per rubriceringsniveau door de politie specifieke maatregelen vastgesteld (BIO+).²¹⁴

²¹⁰ *Kamerstukken II* 2018/19, 34 372, nr. 29, p.7.

²¹¹ Bogw, artikelsgewijze toelichting, artt. 27 en 28, p.48.

²¹² *Kamerstukken II* 2018/19, 34 372, nr. 29, p.11. Verslag van het schriftelijk overleg van 7 mei 2018,

²¹³ <https://wetten.overheid.nl/BWBR0008599/2017-12-15>

²¹⁴ Addendum BIO: Politie-specifieke maatregelen. Versie 1.0, 15 april 2020.

Voor de beveiliging van de technische infrastructuur is er tevens een relatie met de Wet politiegegevens (Wpg).²¹⁵ De gegevens die ter uitvoering van een bevel worden vastgelegd op een technische infrastructuur zijn namelijk persoonsgegevens die worden verwerkt in het kader van de uitoefening van de politietaak, als bedoeld in de artikelen 3 en 4, eerste lid van de Wpg. Het Besluit geeft aan dat de toepasselijkheid van de Wpg ook geldt voor de vastgelegde gegevens over de uitvoering van een bevel in logbestanden.²¹⁶ De Wpg heeft o.a. zijn uitwerking op bewaartermijnen en de vernietiging van gegevens, maar ook op de beveiliging van deze gegevens.

Overigens is de Inspectie JenV geen Wpg-toezichthouder. Indien de Inspectie in aanraking komt met mogelijke schendingen van de regels rond de bescherming van persoonsgegevens, kan zij de Autoriteit Persoonsgegevens (AP) informeren.²¹⁷ De AP is belast met het toezicht op de naleving van de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens, en beschikt over de nodige wettelijke bevoegdheden ter handhaving.

Vanuit de Wet politiegegevens geldt tevens de algemene eis tot het treffen van passende technische en organisatorische maatregelen om een beveiligingsniveau te waarborgen dat op het risico is afgestemd. Dit heeft met name betrekking op de verwerking van de bijzondere categorieën van politiegegevens, op een zodanige manier dat de politiegegevens beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging. Door een algemene maatregel van bestuur zijn nadere regels gesteld over het treffen van de bedoelde passende technische en organisatorische maatregelen.²¹⁸

Om vanuit deze verschillende invalshoeken te komen tot passende maatregelen is het van belang dat volgens een vastgestelde methodiek en door middel van toepassing van risicomanagement door de politie gekomen wordt tot een samenhangend geheel van te treffen beheersingsmaatregelen. Aan de hand van een plan moeten deze beheersingsmaatregelen vervolgens worden geïmplementeerd, dient gecontroleerd te worden of deze maatregelen juist zijn toegepast en dient eventuele bijstelling plaats te vinden bij verandering van betrouwbaarheidseisen of risico's. Samenvattend betreft het hier het opzetten en effectueren van kwaliteitszorg gericht op informatiebeveiliging door middel van een PDCA-cyclus.²¹⁹ De beheersing van beveiligingsrisico's is van belang om te waarborgen dat passende beheersingsmaatregelen voor de betrouwbaarheid en integriteit van de logging en de technische infrastructuur getroffen worden en zijn. Dit vormt de basis om door de politie vanuit een 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. Zie tevens norm N40 (hoofdstuk 7, technische infrastructuur en bewijslogging). De Inspectie ziet hierop toe vanuit haar toezicht op de kwaliteit van de taakuitvoering door de politie.²²⁰

²¹⁵ <https://wetten.overheid.nl/BWBR0022463/2020-01-01>

²¹⁶ Bogw, nota van toelichting I, hoofdstuk 4, pagina 22.

²¹⁷ *Kamerstukken II* 2016/17, 34 372, nr.6, p. 83.

²¹⁸ Staatsblad 2018 nr.496, 6 december 2018. Besluit implementatie richtlijn gegevensbescherming opsporing en vervolging; Art. 6:1a derde lid (beveiliging van politiegegevens) Besluit politiegegevens, <https://wetten.overheid.nl/BWBR0023086/2021-04-01>

²¹⁹ Regeling Informatiebeveiliging Politie, artikel 2, tweede lid en artikel 6. <https://wetten.overheid.nl/BWBR0008599/2017-12-15>

²²⁰ Art. 65 Politiewet 2012.

N49 De politie treft passende technische en organisatorische maatregelen om een beveiligingsniveau te waarborgen dat op het risico is afgestemd. Door middel van periodieke controles ziet de politie toe of deze maatregelen juist zijn toegepast en vindt eventuele bijstelling plaats (kwaliteitssysteem gericht op informatiebeveiliging door middel van een PDCA-cyclus).

Kwaliteitssysteem en interne controle

In de nota van toelichting bij het Besluit is aangegeven dat de Inspectie systeemtoezicht uitoefent, hetgeen een vorm van interne controle of interne borging binnen de politie veronderstelt.²²¹ Het belang van de interne controle wordt ook onderstreept in de toelichting bij het Besluit waarbij aangegeven is dat de logging ten eerste en vooral bedoeld is voor de interne controle van de tijdens de uitvoering van het bevel verrichte handelingen en het functioneren van de technische infrastructuur.²²² Interne controle is als instrumentarium onderdeel van een kwaliteitssysteem waarmee in dit kader eventuele tekortkomingen in de toepassing en uitvoering van de hackbevoegdheid tijdig door de politie organisatie zelf geïdentificeerd en verholpen kunnen worden. Dit sluit aan op de beantwoording van vragen tijdens de wetsbehandeling van de Wet CCIII waarbij de minister aangeeft dat tijdens de uitvoering van het bevel tot het op afstand binnendringen van een geautomatiseerd werk ook toezicht uitgeoefend wordt door de leidinggevende functionarissen binnen de opsporingsdienst.²²³ Hierbij kan bijvoorbeeld gedacht worden aan controles ten aanzien van de kwaliteit van het journaal, haalbaarheidsonderzoeken, processen-verbaal, volledigheid van logging en het adequaat functioneren van voorzieningen voor het doorlopend en automatisch vastleggen van handelingen.

De Inspectie houdt toezicht op de kwaliteit van de taakuitvoering door de politie.²²⁴ Een intern kwaliteitssysteem waaronder een eigen interne controle is een randvoorwaarde voor het borgen van deze kwaliteit. Met een dergelijk systeem kan de politie zelf de kwaliteit van de inzet van de bevoegdheid tijdens alle fasen van de uitvoering borgen en eventuele onregelmatigheden en tekortkomingen hierin tijdig identificeren en verhelpen. Dit is van belang voor een rechtmatige toepassing van de bevoegdheid door de politie.

N50 De politie heeft een kwaliteitssysteem ingericht, waarmee de kwaliteit van de inzet en uitvoering van de hackbevoegdheid wordt gewaarborgd. Onderdeel daarvan vormt de inrichting en uitvoering van interne controle.

²²¹ "Systeemtoezicht of systeemgericht toezicht is het toezicht door de overheid dat gebruikmaakt van zelfregulerende systemen binnen organisaties of branches. Systeemtoezicht is een benadering van de onder toezicht staande waarbij in het toezicht gebruik wordt gemaakt van de eigen activiteiten van deze onder toezicht staande die gericht zijn op het systematisch vergroten van de eigen kwaliteit en regelgeving. Het betreft al het toezicht waarbij de opzet, reikwijdte en werking van (kwaliteits)systemen en (bedrijfs)processen bij organisaties worden vastgesteld. Dit wordt gedaan door audit achtige onderzoeken met reality checks uit te voeren, waarbij gebruik wordt gemaakt van de interne borgingssystemen binnen organisaties of sectoren", aldus (onder meer) het lemma 'systeemtoezicht' (onderdeel Rijksoverheid, begrippenkader rijksinspecties) in de Eerste Nederlandse Systematisch Ingerichte Encyclopaedie (E.N.S.I.E.), elektronische versie (bijgewerkt tot 2018). Zie bovendien: J. Helderma & M.E. Honingh, Systeemtoezicht. Een onderzoek naar de condities en werking van systeemtoezicht in zes sectoren, Den Haag: WODC 2009.

²²² Bogw, nota van toelichting, p.18.

²²³ Kamerstukken II 2016/17, 34 372, nr.6, p.59.

²²⁴ Art. 126nba lid 7 Wetboek van Strafvordering.

Bijlage I: Overzicht toetsingsnormen

In de onderstaande tabel zijn alle normen uit de voorgaande paragrafen opgenomen. In de kolom 'grondslag' is per norm aangegeven waarop deze is gebaseerd. De cijfers in deze kolom verwijzen naar drie categorieën (zie ook de paragraaf 'afbakening' in de inleiding van het hoofddocument):

1. Normen die rechtstreeks voortvloeien uit wet-of regelgeving (zoals artikelen uit het Bogw of het Wetboek van Strafvordering).
2. Normen die zijn ontleend aan toezeggingen / uitspraken uit het parlementaire traject en/of aan toelichtingen (zoals MvT Wet CCIII, NvT Bogw).
3. Normen die de Inspectie heeft geformuleerd vanuit haar toezicht op de kwaliteit van de taakuitvoering.

Norm		Grondslag
1. Aanwijzing opsporingsambtenaren en uitvoering door technisch team		
N1	De opsporingsambtenaren die belast worden met het binnendringen en het uitvoeren van onderzoekshandelingen zijn daartoe door hun werkgever aangewezen.	1
N2	Binnen de Landelijke Eenheid zijn een of meer technische teams ingericht die zijn belast met het binnendringen in een geautomatiseerd werk en het verrichten van onderzoekshandelingen.	1
N3	Een opsporingsambtenaar wordt door de korpschef aangewezen als lid van een technisch team als de opsporingsambtenaar voldoet aan de vereiste (opleidings)kwalificaties.	1
N4	Een opsporingsambtenaar wordt door de korpschef op een incidentele basis aangewezen als deelnemer aan een technisch team voor de duur van de uitvoering van het bevel in een concrete zaak indien hij beschikt over specifieke kennis en vaardigheden, benodigd voor de uitvoering van dat bevel.	1 + 2
N5	Er is sprake van een strikte functiescheiding tussen het technisch team en het tactisch team.	2
2. Voorbereiding		
N6	Het technisch team stelt op basis van de intakegegevens en overige relevante gegevens een rapport haalbaarheidsonderzoek (advies) op, op basis waarvan de OvJ een inschatting van de beheersing en beperking van risico's voor het geautomatiseerde werk kan maken.	2
N7	Het technisch team stelt een plan van aanpak op voor het binnendringen in het geautomatiseerd werk en test dit in een proefopstelling.	2
3. Binnendringingssoftware		
N8	Er is alleen commerciële binnendringingssoftware aangeschaft van leveranciers die gescreend zijn door de AIVD en waarvan door de politie is getoetst dat de leverancier niet levert aan dubieuze regimes.	2
N9	Commerciële binnendringingssoftware is door de politie per zaak ingekocht en de ingekochte software(licentie) is uitsluitend in die specifieke zaak ingezet.	2
N10	In het geval binnendringingssoftware wordt ingekocht, is het functioneren hiervan in een testomgeving gecontroleerd.	2
N11	Indien de politie beschikt over kennis van een mogelijke onbekende kwetsbaarheid, meldt de politie dit allereerst bij de officier van justitie. Indien het OM geen uitstel van melding van een onbekende kwetsbaarheid heeft verleend, meldt de politie de kwetsbaarheid aan de producent van het apparaat of programma.	2
4. Keuring technisch hulpmiddel		
N12	De keuringsdienst is door de minister van Justitie en Veiligheid aangewezen. Een aanwijzing van een andere organisatie dan de Landelijke Eenheid als keuringsdienst, geldt voor ten hoogste drie jaar.	1
N13	De keuringsdienst voldoet aan de regels zoals vastgelegd in de relevante ministeriële regeling(en).	1

N14	De keuring wordt uitgevoerd aan de hand van een door de minister goedgekeurd keuringsprotocol waarin de wijze van keuring en de eisen waaraan het technisch hulpmiddel moet voldoen om goedgekeurd te worden, zijn vastgelegd.	1
N15	Een technisch hulpmiddel is door de korpschef ter (her)keuring aangeboden aan de keuringsdienst.	1
N16	De keuringsdienst kan van elk door hen goedgekeurd technisch hulpmiddel per keuringseis op een navolgbare en controleerbare wijze inzicht verschaffen in de wijze waarop zij tot haar oordeel is gekomen en daarmee de mate waarin het technisch hulpmiddel voldoet aan de gestelde eisen.	3
N17	Indien naar oordeel van de keuringsdienst sprake is van vervangende waarborgen waarmee alsnog voldaan kan worden aan de eisen dan dienen deze maatregelen het risico voldoende af te dekken en uitvoerbaar (SMART) te zijn.	3
N18	De keuringsdienst stelt van een uitgevoerde keuring een keuringsrapport op. Een keuringsrapport van een goedgekeurd technisch hulpmiddel bevat tenminste de onderdelen zoals benoemd in het Besluit (artikel 18.3).	1
N19	De keuringsdienst stelt bij een goedgekeurd technisch hulpmiddel een handleiding op waarin is aangegeven welke instellingen bij gebruik van een technisch hulpmiddel voor een bepaalde functionaliteit moeten worden aangevinkt.	2
N20	De keuringsdienst van een onderdeel van de Landelijke Eenheid houdt een centrale registratie bij van de keuringsrapporten.	1
5. Uitvoering binnendringen en verrichten van onderzoekshandelingen		
N21	Het technisch team past de bevoegdheid tot het binnendringen en het verrichten van onderzoek in een geautomatiseerd werk toe conform door de officier van justitie afgegeven bevelen, aanwijzingen en instructies.	1
N22	Het binnendringen in het geautomatiseerde werk is door het technisch team uitgevoerd volgens het vooraf opgestelde plan van aanpak.	2
N23	Het binnendringen en het uitvoeren van (onderzoeks)handelingen is uitgevoerd door een lid of deelnemer van een technisch team.	1
N24	Een deelnemer aan een technisch team is gedurende de uitvoering van het bevel begeleid door een lid van een technisch team.	1
N25	Alleen de technische, daartoe aangewezen ambtenaren hebben toegang tot het systeem van waaruit het op afstand binnendringen van een geautomatiseerd werk wordt uitgevoerd.	2
N26	De politie draagt op een controleerbare en aantoonbare wijze zorg voor de implementatie van en verantwoording over de opvolging van de procedurele waarborgen die getroffen moeten worden indien de onderzoekshandelingen worden verricht zonder gebruik te maken van een technisch hulpmiddel.	3
5.1 Inzet technisch hulpmiddel		
N27	De keuringsdienst kan in het keuringsrapport aangeven dat een technisch hulpmiddel uitsluitend mag worden ingezet indien verplichte vervangende waarborgen worden toegepast. Indien de politie een dergelijk technisch hulpmiddel inzet, implementeert zij deze waarborgen en legt zij verantwoording af over de naleving hiervan.	2 + 3
N28	Indien een goedgekeurd technisch hulpmiddel ingezet wordt voor het verrichten van onderzoekshandelingen draagt de politie in het kader van de uitvoering van het bevel zorg voor de implementatie van en de verantwoording over de opvolging van de door de keuringsdienst opgestelde handleiding.	2
N29	Indien de Officier van Justitie van oordeel is dat de aard van een technisch hulpmiddel zich verzet tegen keuring, draagt de politie zorg voor de implementatie van aanvullende waarborgen om de betrouwbaarheid, integriteit en herleidbaarheid van vastgelegde gegevens te waarborgen en legt zij verantwoording af over de naleving hiervan.	2 + 3
N30	De politie kan te allen tijde aantonen dat een ingezet technisch hulpmiddel voldoet aan de technische eisen die het Besluit daaraan in artikelen 8 t/m 13 stelt, dan wel dat de risico's voor de betrouwbaarheid, integriteit en herleidbaarheid van de door middel van het technisch hulpmiddel vergaarde gegevens beperkt zijn.	1 + 3
5.2 Verwijdering van een technisch hulpmiddel		
N31	Een technisch hulpmiddel is verwijderd uit een geautomatiseerd werk door een opsporingsambtenaar van een technisch team zodra het onderzoeksdoel is bereikt of uiterlijk zodra de periode, waarbinnen aan het bevel uitvoering moet worden gegeven, is verlopen.	1

N32	Indien een technisch hulpmiddel niet of niet volledig kan worden verwijderd uit een geautomatiseerd werk, beëindigt de met verwijdering belaste opsporingsambtenaar het transport van de door het technische hulpmiddel geregistreerde gegevens naar de technische infrastructuur.	1
N33	Indien de niet of niet volledige verwijdering van een technisch hulpmiddel risico's oplevert voor het functioneren van het geautomatiseerde werk waarin het is geplaatst, stelt de opsporingsambtenaar de officier van justitie hiervan in kennis en stelt hij informatie ter beschikking ten behoeve van de volledige verwijdering.	1
5.3 Communicatie met leverancier technisch hulpmiddel		
N34	Het technisch hulpmiddel staat tijdens de inzet niet in contact met de producent van deze software.	2
N35	De registratie van de beperkte en gecontroleerde toegangsverlening tot en uitgifte van technisch hulpmiddelen vindt centraal plaats door daartoe door de korpschef aangewezen ambtenaren.	1
N36	De systemen van de politie worden voortdurend beschermd en bewaakt tegen mogelijke aanvallen van buiten.	2
6. Gegevens vastgelegd in logbestanden (logging)		
N37	Gedurende de uitvoering van een bevel zijn doorlopend en automatisch gegevens in logbestanden vastgelegd over: a) de handelingen die worden verricht ter uitvoering van een bevel; b) de toegang tot een technisch hulpmiddel; c) de gegevens die al dan niet met een technisch hulpmiddel op de technische infrastructuur worden vastgelegd ter uitvoering van een bevel; d) het functioneren van de technische infrastructuur.	1
N38	Voor de vastlegging van gegevens in logbestanden zijn maatregelen getroffen om wijziging van de logbestanden of kennisneming hiervan door onbevoegden te voorkomen en achteraf te kunnen vaststellen of wijziging of kennisneming heeft plaatsgevonden.	1
N39	Het loggingsproces is zo ingericht dat de loggingsinformatie tijdens de fase van bewijsvergaring te allen tijde blijft functioneren en niet valt te manipuleren, te wijzigen of te verwijderen.	2
7. Technische infrastructuur en bewijslogging		
N40	De vastlegging van de tijdens het onderzoek geregistreerde gegevens vindt plaats op een technische infrastructuur, waarbij het unieke kenmerk en de datum en tijd van vastlegging wordt geregistreerd.	1
N41	De politie treft maatregelen om wijzigingen bij de vastgelegde gegevens of kennisneming van de vastgelegde gegevens hiervan door onbevoegden te voorkomen en achteraf te kunnen vaststellen of wijziging of kennisneming hiervan heeft plaatsgevonden. Er worden passende technische en organisatorische maatregelen getroffen om het beveiligingsniveau te waarborgen dat op het risico afgestemd is.	1
8. Onregelmatigheden		
N42	De logging en controle is zodanig ingericht dat vastgesteld kan worden of onregelmatigheden plaatsvinden.	1
N43	De politie controleert aan de hand van de gegevens in de logbestanden of onregelmatigheden hebben plaatsgevonden.	2
9. Proces-verbaal		
N44	De opsporingsambtenaar maakt van door hem verrichte handelingen en eventueel geconstateerde onregelmatigheden ten spoedigste proces-verbaal op dat aan de officier van justitie wordt gezonden.	1
10. Verstrekking en bewerking van vastgelegde gegevens		
N45	Alleen die gegevens die binnen de categorieën van gegevens in het bevel van de officier van justitie zijn opgenomen, zijn door het technisch team verstrekt aan een opsporingsambtenaar die is belast met het opsporingsonderzoek.	2
N46	Bij de selectie van gegevens is gebruikgemaakt van een forensische kopie van de ter uitvoering van het bevel vastgelegde gegevens.	1 + 2

11. Bewaartermijn, verwijdering en vernietiging gegevens		
N47	De politie richt de werkprocessen, procedures en technische voorzieningen op een dusdanige wijze in en past deze zodanig toe dat gegevens tijdig, juist en volledig worden verwijderd en vernietigd. Ook geldt hierbij dat gegevens juist en volledig bewaard en toegankelijk zijn en blijven gedurende de periode dat dat vereist wordt.	3
N48	Zodra de opsporingsambtenaar bij het onderzoek van de opgeslagen gegevens kennisneemt van mededelingen waarvan hij weet of redelijkerwijs kan vermoeden dat deze zijn gedaan door of aan een geheimhouder, stelt hij de officier van justitie hiervan onverwijld in kennis.	1
12. Kwaliteitssysteem en interne controle		
N49	De politie treft van passende technische en organisatorische maatregelen om een beveiligingsniveau te waarborgen dat op het risico is afgestemd. Door middel van periodieke controles ziet de politie toe of deze maatregelen juist zijn toegepast en vindt eventuele bijstelling plaats (kwaliteitssysteem gericht op informatiebeveiliging door middel van een PDCA-cyclus).	3
N50	De politie heeft een kwaliteitssysteem ingericht waarmee de kwaliteit van de inzet en uitvoering van de hackbevoegdheid wordt gewaarborgd. Onderdeel daarvan vormt de inrichting en uitvoering van interne controle.	3

Inspectie Justitie en Veiligheid

*Toezicht, omdat rechtvaardigheid en veiligheid
niet vanzelfsprekend zijn.*

Dit is een uitgave van:

Inspectie Justitie en Veiligheid
Ministerie van Justitie en Veiligheid
Turfmarkt 147 | 2511 DP Den Haag
Postbus 20301 | 2500 EH Den Haag

Contactformulier | www.inspectie-jenv.nl

Maart 2022

*Aan deze publicatie kunnen geen rechten worden ontleend.
Vermenigvuldigen van informatie uit deze publicatie is toegestaan,
mits deze uitgave als bron wordt vermeld.*