

Besluit van * houdende regels over de uitoefening van de bevoegdheid tot het binnendringen in een geautomatiseerd en het al dan niet met een technisch hulpmiddel onderzoek doen als bedoeld in de artikelen 126nba, eerste lid, 126uba, eerste lid, en 126zpa, eerste lid van het Wetboek van Strafvordering (Besluit onderzoek in een geautomatiseerd werk)

Wij Willem-Alexander, bij de gratie Gods, Koning der Nederlanden, Prins van Oranje-Nassau, enz. enz.

Op de voordracht van de Staatssecretaris van Veiligheid en Justitie van (PM datum), nr. (PM);

Gelet op de artikelen 126nba, eerste en achtste lid, 126uba, eerste en derde lid, 126zpa, eerste en derde lid, en 126ee van het Wetboek van Strafvordering en artikel 18, eerste lid, van de Wet politiegegevens;

De Afdeling advisering van de Raad van State gehoord (advies PM datum, nr. PM);

Gezien het nader rapport van de Staatssecretaris van Veiligheid en Justitie van (PM datum), nr. (PM);

Hebben goedgevonden en verstaan:

Hoofdstuk 1 Algemene bepalingen

Artikel 1 Definities

In dit besluit wordt verstaan onder:

- a. bevel: bevel van de officier van justitie als bedoeld in de artikelen 126nba, eerste lid, 126uba, eerste lid, 126zpa, eerste lid, van het Wetboek van Strafvordering;
- b. korpschef: korpschef als bedoeld in artikel 27 van de Politiewet 2012;
- d. onderzoekshandeling: handeling van een opsporingsambtenaar van een technisch team met het oog op een doel als bedoeld in de artikelen 126nba, eerste lid, onder a tot en met e, 126uba, eerste lid, onder a tot en met e, en 126zpa, eerste lid, onder a tot en met e, van het Wetboek van Strafvordering ter uitvoering van een bevel;
- e. Onze Minister: Minister van Veiligheid en Justitie;
- f. Landelijke eenheid: Landelijke eenheid als bedoeld in artikel 3, eerste lid, van het Besluit beheer politie;
- g. technisch hulpmiddel: softwareapplicatie die gegevens detecteert, registreert en transporteert en waarmee onderzoekshandelingen worden verricht ter uitvoering van een bevel;
- h. technische infrastructuur: technische voorziening van een technisch team bedoeld voor de vastlegging van de door een technisch hulpmiddel geregistreerde gegevens;
- i. technisch team: onderdeel van de Landelijke eenheid dat kan worden belast met de uitvoering van een bevel.

Hoofdstuk 2 Toepassing van de bevoegdheid met het oog op het vastleggen van gegevens of het ontoegankelijk maken van gegevens

Artikel 2 Aanwijzing van misdrijven

Als misdrijven als bedoeld in de artikelen 126nba, eerste lid, onder c, 126uba, eerste lid, onder c, en 126zpa, eerste lid, onder c, van het Wetboek van Strafvordering worden aangewezen de misdrijven, bedoeld in de artikelen 98, eerste en tweede lid, 98c, eerste lid, 131, eerste en tweede lid, 138ab, eerste tot en met derde lid, 138b, eerste tot en met derde lid, 138c, 139c, eerste lid, 139d, eerste tot en met derde lid, 139g, eerste lid, 140, eerste lid, 142a, eerste en tweede lid, 160, 161, aanhef en onder 1°, 161bis, aanhef en onder 1° en 2°, 161sexies, aanhef en onder 1°, 177, eerste en tweede lid, 179, 182, eerste en tweede lid, onder 1°, 197a, eerste en tweede lid, 200, eerste lid, 205, eerste en derde lid, 225, eerste en tweede lid, 226, eerste lid, 227, eerste lid, 231, eerste en tweede lid, 231a, eerste en tweede lid, 232, eerste en tweede lid, 240b, eerste lid, 247, 248a, 248e, 285b, eerste lid, 350a, eerste tot en met derde lid, 350c, eerste lid, 350d, 363, eerste en tweede lid en 420bis, eerste lid, van het Wetboek van Strafrecht.

Hoofdstuk 3 Deskundigheid van opsporingsambtenaren

Artikel 3 Lidmaatschap van een technisch team

1. Een opsporingsambtenaar als bedoeld in de artikelen 141, onder b, c en d, en 142 van het Wetboek van Strafvordering kan door de korpschef worden aangewezen voor het binnendringen in een geautomatiseerd werk en het, al dan niet met een technisch hulpmiddel, onderzoek doen, bedoeld in de artikelen 126nba, eerste lid, 126uba, eerste lid, en 126zpa, eerste lid, van het Wetboek van Strafvordering, indien hij lid is van een technisch team.
2. Een opsporingsambtenaar als bedoeld in het eerste lid kan lid worden van een technisch team indien hij heeft voldaan aan door Onze Minister aangewezen kwalificaties.

Artikel 4 Incidentele samenwerking

1. In aanvulling op artikel 3 kan een opsporingsambtenaar als bedoeld in de artikelen 141, onder b, c en d, en 142 van het Wetboek van Strafvordering die geen lid is van een technisch team door de korpschef worden aangewezen voor het binnendringen in een geautomatiseerd werk en het, al dan niet met een technisch hulpmiddel, onderzoek doen, bedoeld in de artikelen 126nba, eerste lid, 126uba, eerste lid, en 126zpa, eerste lid, van het Wetboek van Strafvordering, indien hij naar het oordeel van de korpschef beschikt over specifieke kennis en vaardigheden, benodigd voor de uitvoering van een bevel.
2. Indien een opsporingsambtenaar als bedoeld in het eerste lid wordt aangewezen wordt hij als deelnemer toegevoegd aan een technisch team en wordt hij tijdens de uitvoering van het bevel begeleid door een lid van een technisch team.

Hoofdstuk 4 Geautomatiseerde vastlegging van gegevens over de uitvoering van een bevel

Artikel 5 Vastlegging van gegevens

Gedurende de uitvoering van een bevel worden doorlopend en automatisch gegevens vastgelegd over de verrichte onderzoekshandelingen en het functioneren van de technische infrastructuur.

Artikel 6 Vaststelling van onregelmatigheden

1. De vastlegging van gegevens, bedoeld in artikel 5, vindt op zodanige wijze plaats dat zowel tijdens de periode, vermeld in het bevel, waarbinnen aan het bevel uitvoering moet worden gegeven als na afloop daarvan kan worden vastgesteld of tijdens die periode een handeling of bewerking heeft plaatsgevonden die van invloed is op de betrouwbaarheid en integriteit van de ter uitvoering van het bevel vastgelegde gegevens.
2. Indien een handeling of bewerking als bedoeld in het eerste lid wordt geconstateerd maakt een opsporingsambtenaar van een technisch team daarvan proces-verbaal op, dat aan de officier van justitie wordt gezonden.

Artikel 7 Betrouwbaarheid en integriteit gegevens

1. De inhoud van de vastgelegde gegevens, bedoeld in artikel 5, wordt niet bewerkt.
2. De vastgelegde gegevens zijn uitsluitend toegankelijk voor door de korpschef aangewezen ambtenaren.
3. Bij de vastlegging van gegevens worden maatregelen getroffen om wijziging of kennisneming van de ter uitvoering van een bevel vastgelegde gegevens door onbevoegden te voorkomen en achteraf te kunnen vaststellen of wijziging of kennisneming hiervan heeft plaatsgevonden.

Hoofdstuk 5 Technische eisen met betrekking tot een technisch hulpmiddel

Artikel 8 Gerichte werking

Een technisch hulpmiddel is zodanig ingericht dat de werking ervan kan worden beperkt tot de in het bevel vermelde functionaliteit of functionaliteiten.

Artikel 9 Gerichte detectie en registratie

1. Een technisch hulpmiddel detecteert en registreert uitsluitend gegevens ten behoeve van de in het bevel vermelde functionaliteit of functionaliteiten.
2. Een technisch hulpmiddel dat een functionaliteit of functionaliteiten bevat ten behoeve van het opnemen van telecommunicatie detecteert en registreert uitsluitend de communicatie die

plaatsvindt met gebruikmaking van één of meer nummers van de individuele gebruiker of gebruikers op wie het bevel betrekking heeft.

Artikel 10 Betrouwbaarheid en integriteit

1. Een technisch hulpmiddel registreert gegevens op zodanige wijze dat de inhoud van de geregistreerde gegevens identiek is aan de inhoud van de gedetecteerde gegevens.
2. Een technisch hulpmiddel is beveiligd tegen wijziging van de werking hiervan en tegen wijziging en kennisneming van de geregistreerde gegevens door onbevoegden.

Artikel 11 Herleidbaarheid

Een technisch hulpmiddel voorziet de geregistreerde gegevens van een uniek gegeven.

Artikel 12 Datum en tijd

Een technisch hulpmiddel voorziet de geregistreerde gegevens van de datum en tijd waarop de registratie plaatsvindt.

Artikel 13 Transport

1. Een technisch hulpmiddel transporteert de geregistreerde gegevens automatisch naar een technische infrastructuur.
2. Een technisch hulpmiddel beveiligd de geregistreerde gegevens tijdens het transport naar een technische infrastructuur tegen wijziging of kennisneming hiervan door onbevoegden.

Hoofdstuk 6 Keuring van een technisch hulpmiddel

Artikel 14 Voorafgaande keuring en herkeuring

1. Voordat een technisch hulpmiddel wordt ingezet ter uitvoering van een bevel wordt het goedgekeurd door een keuringsdienst.
2. Een technisch hulpmiddel wordt uitsluitend goedgekeurd indien het voldoet aan de in de artikelen 8 tot en met 13 gestelde eisen.
3. Indien een technisch hulpmiddel of een onderdeel hiervan zodanig wijzigt dat redelijkerwijs kan worden aangenomen dat de werking niet langer voldoet aan de in de artikelen 8 tot en met 13 genoemde eisen, vindt voorafgaand aan de inzet van het technische hulpmiddel herkeuring plaats door een keuringsdienst van het gewijzigde technische hulpmiddel of van het gewijzigde onderdeel.
4. In afwijking van het derde lid kan de herkeuring na afloop van de inzet plaatsvinden indien de wijziging van de werking van een technisch hulpmiddel of een onderdeel hiervan zodanig kort voor de inzet van het technische hulpmiddel plaatsvindt dat voorafgaande herkeuring niet mogelijk is.

Artikel 15 Inzet zonder voorafgaande keuring

1. Indien het onderzoeksbelang dit dringend vordert, kan de officier van justitie bepalen dat een technisch hulpmiddel wordt ingezet ondanks het feit dat niet of niet geheel wordt voldaan aan artikel 14, eerste lid.
2. De officier van justitie vermeldt in het bevel dat toepassing is gegeven aan het eerste lid.
3. Na afloop van de inzet wordt het technische hulpmiddel of een niet gekeurd onderdeel hiervan alsnog gekeurd door een keuringsdienst, tenzij de aard van het technische hulpmiddel of het niet gekeurde onderdeel hiervan zich naar het oordeel van de officier van justitie daartegen verzet.

Artikel 16 Keuringsdienst

1. Onze Minister wijst een onderdeel van de Landelijke eenheid aan als keuringsdienst.
2. Onze Minister kan één of meer andere organisaties aanwijzen als keuringsdienst.
3. Bij ministeriële regeling kunnen regels worden gesteld over de aanwijzing van de keuringsdienst, bedoeld in het eerste lid.
4. Indien Onze Minister voornemens is één of meer andere organisaties aan te wijzen als keuringsdienst worden hierover bij ministeriële regeling regels gesteld.

Artikel 17 Keuringsprotocol

1. Een keuringsdienst legt de wijze van keuring vast in een keuringsprotocol.
2. Een keuringsprotocol behoeft voorafgaande goedkeuring door Onze Minister.

Artikel 18 Keuringsrapport

1. De korpschef biedt een technisch hulpmiddel ter keuring aan bij een keuringsdienst.
2. Een keuringsdienst legt de resultaten van de keuring vast in een keuringsrapport.
3. Het keuringsrapport van een goedgekeurd technisch hulpmiddel vermeldt ten minste:
 - a. dat het technische hulpmiddel voldoet aan de artikel 8 tot en met 13 gestelde eisen;
 - b. een referentienummer;
 - c. een omschrijving van de werking van het technische hulpmiddel;
 - d. een aanduiding van de functionaliteit of functionaliteiten van het technische hulpmiddel;
 - e. relevante verplichte vervangende procedurele waarborgen waarmee voldaan kan worden aan één of meer eisen, bedoeld in de artikelen 8 tot en met 13;
 - f. relevante informatie met betrekking tot de werking van een functionaliteit of functionaliteiten van het technische hulpmiddel;
 - g. de periode waarvoor de keuring geldt, zolang de werking van het technische hulpmiddel ongewijzigd is.

Artikel 19 Registratie van keuringsrapporten

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

Artikel 20 Wederzijdse erkenningsclausule

1. Met technische hulpmiddelen als bedoeld in dit besluit worden gelijkgesteld technische hulpmiddelen die rechtmatig zijn vervaardigd of in de handel zijn gebracht in een andere lidstaat van de Europese Unie of in een staat, niet zijnde een lidstaat van de Europese Unie, die partij is bij een tot een douane-unie strekkend Verdrag, dan wel rechtmatig zijn vervaardigd in een staat die partij is bij een tot een vrijhandelszone strekkend Verdrag dat Nederland bindt, en die voldoen aan eisen die een beschermingsniveau bieden dat ten minste gelijkwaardig is aan het niveau dat met de nationale eisen wordt nagestreefd.
2. Met een keuringsrapport als bedoeld in dit besluit wordt gelijkgesteld een verklaring van goedkeuring, afgegeven door een onafhankelijke keuringsinstelling in een andere lidstaat van de Europese Unie dan wel in een staat, niet zijnde een lidstaat van de Europese Unie, die partij is bij een daartoe strekkend of mede daartoe strekkend Verdrag dat Nederland bindt, welke verklaring is afgegeven op basis van onderzoeken die een beschermingsniveau bieden dat ten minste gelijkwaardig is aan het niveau dat met de nationale onderzoeken wordt nagestreefd.

Hoofdstuk 7 Toegang tot en plaatsing van een technisch hulpmiddel

Artikel 21 Toegang

1. De korpschef wijst één of meer ambtenaren aan die zijn belast met de centrale registratie van de toegang tot goedgekeurde technische hulpmiddelen.
2. Een met registratie belaste ambtenaar verschaft, na ontvangst van een kopie van het bevel, een met plaatsing belaste opsporingsambtenaar toegang tot een technisch hulpmiddel.
3. De toegang tot een technisch hulpmiddel wordt verleend voor de in het bevel vermelde periode waarbinnen aan het bevel uitvoering moet worden gegeven.
4. Een met registratie belaste ambtenaar registreert ten minste:
 - a. een aanduiding van het technische hulpmiddel waartoe toegang wordt verleend;
 - b. het tijdstip van toegangverlening;
 - c. de in het bevel vermelde aanduidingen van de aard en functionaliteit van een technisch hulpmiddel;
 - d. de in het bevel vermelde periode waarbinnen aan het bevel uitvoering moet worden gegeven.

Artikel 22 Plaatsing

1. De plaatsing van een technisch hulpmiddel in een geautomatiseerd werk vindt plaats door een opsporingsambtenaar van een technisch team.
2. De opsporingsambtenaar beperkt bij de plaatsing van een technisch hulpmiddel de werking ervan tot de in het bevel vermelde functionaliteit of functionaliteiten.
3. De opsporingsambtenaar maakt proces-verbaal op van de plaatsing, dat aan de officier van justitie wordt gezonden.

Hoofdstuk 8 Inzet van een technisch hulpmiddel

Artikel 23 Inzet

1. De inzet van een technisch hulpmiddel in een geautomatiseerd werk vindt plaats door een opsporingsambtenaar van een technisch team.
2. De opsporingsambtenaar maakt proces-verbaal op van de inzet, dat aan de officier van justitie wordt gezonden.

Artikel 24 Technische infrastructuur

De vastlegging van de door een technisch hulpmiddel geregistreerde gegevens vindt plaats op een technische infrastructuur.

Artikel 25 Betrouwbaarheid en integriteit

1. De inhoud van de op een technische infrastructuur vastgelegde gegevens wordt niet bewerkt.
2. De vastgelegde gegevens zijn uitsluitend toegankelijk voor door de korpschef aangewezen ambtenaren.
3. Bij de vastlegging van gegevens worden maatregelen getroffen om wijziging of kennisneming van de vastgelegde gegevens door onbevoegden te voorkomen en achteraf te kunnen vaststellen of wijziging of kennisneming hiervan heeft plaatsgevonden.

Artikel 26 Herleidbaarheid

Een technische infrastructuur is zodanig ingericht dat bij de vastlegging van gegevens het door een technisch hulpmiddel geregistreerde unieke gegeven wordt herkend.

Artikel 27 Datum en tijd

Een technische infrastructuur is zodanig ingericht dat bij de vastlegging van gegevens de datum en tijd van de vastlegging worden geregistreerd.

Hoofdstuk 9 Verwijdering van een technisch hulpmiddel

Artikel 28 Verwijdering

1. Een technisch hulpmiddel wordt verwijderd uit een geautomatiseerd werk zodra een bevel is uitgevoerd of uiterlijk zodra de periode, vermeld in het bevel, waarbinnen aan het bevel uitvoering moet worden gegeven is verlopen.
2. De verwijdering van een technisch hulpmiddel vindt plaats door een opsporingsambtenaar van een technisch team.
3. De opsporingsambtenaar maakt proces-verbaal op van de verwijdering, dat aan de officier van justitie wordt gezonden.

Artikel 29 Niet of niet volledige verwijdering

1. Indien een technisch hulpmiddel niet of niet volledig kan worden verwijderd uit een geautomatiseerd werk, beëindigt de met verwijdering belaste opsporingsambtenaar het transport van de door het technische hulpmiddel geregistreerde gegevens naar de technische infrastructuur.
2. 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.
3. De opsporingsambtenaar maakt proces-verbaal op van de niet of niet volledige verwijdering, dat aan de officier van justitie wordt gezonden.

Hoofdstuk 10 Wijziging overige wet- en regelgeving

Artikel 30 Wijziging Besluit politiegegevens

Aan artikel 4:3, eerste lid, onderdeel a, van het Besluit politiegegevens wordt, onder vervanging van de punt aan het slot door een puntkomma, een onderdeel toegevoegd, luidende:

- De inspectie, bedoeld in artikel 57, eerste lid, van de Wet veiligheidsregio's, met het oog op de uitvoering van de taken, bedoeld in artikel 65, eerste lid, van de Politiewet 2012 en op de uitvoering van een bevel, als bedoeld in de artikelen 126nba, eerste lid, 126uba, eerste lid en 126zpa, eerste lid, van het Wetboek van Strafvordering, door de ambtenaren, bedoeld in artikel 141, onderdeel d, en de personen, bedoeld in artikel 142, eerste lid, onderdeel b, van het Wetboek van Strafvordering.

Hoofdstuk 11 Slotbepalingen

Artikel 31 Inwerkingtreding

Dit besluit treedt in werking op een bij koninklijk besluit te bepalen tijdstip.

Artikel 32 Citeertitel

Dit besluit wordt aangehaald als: Besluit onderzoek in een geautomatiseerd werk.

Lasten en bevelen dat dit besluit met de daarbij behorende nota van toelichting in het Staatsblad zal worden geplaatst.

De Staatssecretaris van Veiligheid en Justitie,

NOTA VAN TOELICHTING

I. Algemeen

1. Inleiding

Het wetsvoorstel computercriminaliteit III (Kamerstukken I 2016/17 34 372, A) versterkt het juridische instrumentarium voor de opsporing en vervolging van computercriminaliteit. Het wetsvoorstel sluit aan bij de snelle ontwikkelingen van de technologie, het internet en de computercriminaliteit en zet de lijn voort die is ingezet met de Wet computercriminaliteit I (1993) en de Wet computercriminaliteit II (2006).

Het wetsvoorstel verleent de officier van justitie de bevoegdheid om, onder strikte voorwaarden, te bevelen dat een opsporingsambtenaar heimelijk en op afstand een geautomatiseerd werk dat in gebruik is bij een verdachte binnendringt en hierin, al dan niet met een technisch hulpmiddel, onderzoek doet met oog op bepaalde onderzoeksdoelen (artikelen 126nba, 126uba en 126zpa van het Wetboek van Strafvordering (Sv)). Deze onderzoeksdoelen betreffen: de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of van de gebruiker, de uitvoering van een bevel tot stelselmatige observatie, de uitvoering van een bevel tot het aftappen en opnemen van communicatie of opnemen van vertrouwelijke communicatie, de vastlegging van gegevens die in het geautomatiseerde werk zijn of worden opgeslagen en de ontoegankelijkmaking van gegevens. Het op afstand heimelijk binnendringen in een geautomatiseerd werk en het doen van onderzoek is noodzakelijk geworden door de voortschrijdende techniek en het wijdverbreide gebruik van geautomatiseerde werken voor communicatie en de verwerking en opslag van gegevens.

Het wetsvoorstel computercriminaliteit III bevat een aantal grondslagen om bij of krachtens algemene maatregel van bestuur regels te stellen over de uitoefening van deze bevoegdheid. Het betreft ten eerste de grondslag om de inzet van de bevoegdheid voor het doen van onderzoek waarbij het geautomatiseerde werk wordt binnengedrongen met het oog op twee specifieke onderzoeksdoelen, het vastleggen van gegevens die in het geautomatiseerde werk zijn of worden opgeslagen en het ontoegankelijk maken van gegevens, mogelijk te maken bij verdenking van bij algemene maatregel van bestuur aangewezen misdrijven (artikelen 126nba/126uba/126zpa, eerste lid, Sv). Het betreft ten tweede de mogelijkheid om nadere regels te stellen over de deskundigheid en autorisatie van de bij het onderzoek in een geautomatiseerd werk betrokken opsporingsambtenaren, de samenwerking met andere opsporingsambtenaren en de geautomatiseerde vastlegging van gegevens ter uitvoering van een bevel van de officier van justitie (artikel 126nba, achtste lid, onder a en b, Sv, dat van overeenkomstige is verklaard in de artikelen 126uba/126zpa, derde lid, Sv). Ten derde kunnen nadere regels gesteld worden over verschillende aspecten met betrekking tot het doen van onderzoek met een technisch hulpmiddel (artikel 126ee Sv). Het onderhavige besluit geeft uitvoering aan deze bepalingen.

Naast voornoemde delegatiegrondslagen biedt het wetsvoorstel een facultatieve grondslag om bij algemene maatregel van bestuur nadere regels te stellen over de toepassing van de binnendringen- en onderzoeksbevoegdheid in gevallen waarin niet bekend is waar de gegevens zijn opgeslagen (artikel 126nba, negende lid, Sv, dat van overeenkomstige toepassing is verklaard in de artikelen 126uba/126zpa, derde lid, Sv). Vooralsnog wordt van deze mogelijkheid geen gebruik gemaakt; de uitwerking hiervan vindt plaats in een Aanwijzing van het College van procureurs-generaal.

2. Toepassing van de bevoegdheid met het oog op het vastleggen van gegevens of het ontoegankelijkmaken van gegevens

Op grond van het wetsvoorstel computercriminaliteit III mag de bevoegdheid tot het binnendringen in een geautomatiseerd werk en doen van onderzoek met het oog op het vastleggen van gegevens of het ontoegankelijkmaken van gegevens, gelet op de mate van inbreuk die hiermee wordt gemaakt op de persoonlijke levenssfeer, in beginsel uitsluitend worden toegepast bij een verdenking van een misdrijf waarop naar de wettelijke omschrijving een

gevangenisstraf van acht jaren of meer is gesteld. Bij algemene maatregel van bestuur kunnen echter andere misdrijven met een lagere wettelijke strafbedreiging worden aangewezen (artikelen 126nba/126uba/126zpa, eerste lid, onder c, Sv). In hoofdstuk 2 van dit besluit worden deze misdrijven aangewezen. Het betreft misdrijven die worden gepleegd met een geautomatiseerd werk en die een geautomatiseerd werk als doelwit hebben (computercriminaliteit in enge zin) en ernstige commune misdrijven die in toenemende mate met behulp van een geautomatiseerd werk worden gepleegd (gedigitaliseerde criminaliteit) waarbij vaak geen ander aanknopingspunt is voor de opsporing dan via het geautomatiseerde werk waarmee het misdrijf wordt gepleegd. Voor alle aangewezen misdrijven geldt dat er een duidelijk maatschappelijk belang is bij de beëindiging van de strafbare situatie en de vervolging van de daders.

De toenemende digitalisering van de maatschappij leidt tot nieuwe veiligheidsrisico's en nieuwe mogelijkheden voor criminelen. Het aantal gevallen van computercriminaliteit waarbij computers niet alleen als middel worden ingezet, maar ook doelwit zijn, neemt toe. Van computercriminaliteit gaan grote dreigingen uit, zoals gevaar voor maatschappelijke ontwrichting en voor het vertrouwen in het financieel-economische systeem. Dat risico is onder meer aan de orde bij aanvallen via zogenoemde botnets, waarbij controle op afstand over een aanzienlijk aantal computers tot stand wordt gebracht door deze door middel van gerichte cyberaanvallen te besmetten met kwaadaardige software. Het netwerk van computers dat de botnet vormt kan worden ingezet om een grootschalige cyberaanvallen uit te voeren. Deze aanvallen kunnen vleiden tot ernstige economische schade en tot ontwrichting en vernietiging van vitale infrastructuren, zoals energiecentrales, vervoersnetwerken en overheidsnetwerken.

Ook op andere criminaliteitsterreinen maken criminelen steeds vaker gebruik van digitale technieken. Beroepscriminelen schermen hun activiteiten af door geavanceerde technische middelen in te zetten, wat het opsporingsonderzoek en de bewijsvergaring complex maakt. Ondermijnende criminaliteit, zoals witwassen, fraude en corruptie waarbij criminelen voor hun activiteiten gebruik maken van legale structuren en goederen, verplaatst zich naar het virtuele domein en ontwricht het maatschappelijk vertrouwen. Grootschalige financiële fraude wordt steeds vaker door technisch zeer capabele criminelen gepleegd. Zedenmisdrijven, zoals het verleiden of aanzetten van een minderjarige tot webcamseks, worden steeds vaker online gepleegd. De gevolgen hiervan kunnen indringend, ingrijpend en langdurig zijn en hebben niet alleen impact op het slachtoffer, maar ook op de omgeving en de samenleving als geheel.

Inzet van de binnendring- en onderzoeksbevoegdheid met het oog op het veiligstellen van digitaal bewijs voor voornoemde strafbare feiten en het stopzetten van criminele activiteiten draagt bij aan een effectieve aanpak van cybercrime en aan een veilig digitaal domein. Door de aanwijzing van misdrijven bij algemene maatregel van bestuur kan flexibel worden ingespeeld op de snelle ontwikkelingen in de cybercriminaliteit.

3. De uitvoering van een bevel van de officier van justitie

3.1. Het onderzoek in een geautomatiseerd werk

In dit besluit worden nadere regels gesteld over het onderzoek in een geautomatiseerd werk ter uitvoering van een bevel van de officier van justitie als bedoeld in de artikelen 126nba/uba/zpa Sv. Onder onderzoek in een geautomatiseerd werk wordt in deze toelichting verstaan: het op afstand en heimelijk binnendringen in een geautomatiseerd werk en het verrichten van bepaalde onderzoekshandelingen. Het binnendringen in een geautomatiseerd werk is het voorbereidende deel van het onderzoek. In de daarop volgende onderzoeksfase worden al dan niet met een technisch hulpmiddel onderzoekshandelingen verricht met het oog op bepaalde onderzoekdoelen en gegevens vastgelegd.

Bij het binnendringen in een geautomatiseerd werk kan gebruik worden gemaakt van verschillende technieken. In beginsel wordt gebruik gemaakt van zwakheden bij de gebruiker of kwetsbaarheden die bekend zijn bij de producent van het geautomatiseerde werk of de software. In het uitzonderlijke geval dat gebruik wordt gemaakt van een kwetsbaarheid waarvan aannemelijk is dat die niet bekend is of kan worden verondersteld bekend te zijn, kan de officier van justitie op grond van het wetsvoorstel computercriminaliteit III bevelen, na machtiging van de rechter-commissaris, dat de melding hiervan aan de producent wordt uitgesteld (artikel 126ffa

Sv).

De onderzoeksdoelen met het oog waarop onderzoek kan worden gedaan betreffen:

- a. de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of van de gebruiker, zoals de identiteit of locatie, en de vastlegging daarvan;
- b. de uitvoering van een bevel tot stelselmatige observatie;
- c. de uitvoering van een bevel tot het aftappen en opnemen van communicatie of opnemen van vertrouwelijke communicatie;
- d. de vastlegging van gegevens die in het geautomatiseerde werk zijn of worden opgeslagen;
- e. de ontoegankelijkmaking van gegevens.

Het bevel van de officier bevat de onderzoeksdoelen met het oog waarop het bevel wordt afgegeven (artikelen 126nba/126uba, tweede lid, onder e, Sv en 126zpa, tweede lid, onder c, Sv). Als het gaat om de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker, de vastlegging van gegevens of de ontoegankelijkmaking van gegevens dient het bevel een duidelijke omschrijving van de te verrichten handelingen te bevatten. Ook wordt in het bevel tot uitdrukking gebracht ten aanzien van welk deel van het geautomatiseerde werk en welke categorie van gegevens aan het bevel uitvoering wordt gegeven (artikelen 126nba/126uba/126zpa, tweede lid, onder f, Sv). Verder dient in het bevel een aanduiding van de aard en functionaliteit van het technische hulpmiddel te worden opgenomen (artikelen 126nba/126uba, tweede lid, onder d, en 126zpa, tweede lid, onder b, Sv).

Het wetsvoorstel computercriminaliteit III bevat grondslagen om bij of krachtens algemene maatregel van bestuur regels te stellen over het onderzoek in een geautomatiseerd werk. Het betreft ten eerste de deskundigheid en autorisatie van de bij het binnendringen in een geautomatiseerd werk en het verrichten van onderzoekshandelingen betrokken opsporingsambtenaren en de samenwerking met andere opsporingsambtenaren (artikel 126nba, achtste lid, onder a, Sv, dat van overeenkomstige toepassing wordt verklaard in de artikelen 126uba/126zpa, derde lid, Sv). Het betreft ten tweede verschillende organisatorische, procedurele en technische eisen met betrekking tot de onderzoeksfase waarin gegevens worden vastgelegd. Hierbij gaat het om de geautomatiseerde vastlegging van gegevens ter uitvoering van een bevel van de officier van justitie (artikel 126nba, achtste lid, onder b, Sv, dat van overeenkomstige toepassing wordt verklaard in de artikelen 126uba/126zpa, derde lid, Sv) en diverse aspecten met betrekking tot het doen van onderzoek met behulp van een technisch hulpmiddel (artikel 126ee Sv). 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. Door eisen te stellen aan onderzoeksproces en de verantwoording hiervan ontstaat een gegevensspoor dat herleidbaar is.

Bij het stellen van regels over het onderzoek in een geautomatiseerd werk is een zekere mate van techniekonafhankelijkheid in acht genomen. Techniek verandert snel en cybercriminaliteit ook. De bestrijding van cybercriminaliteit vraagt om enige flexibiliteit en abstractie van technische details. Het besluit heeft gelet hierop een kaderstellend karakter. Er worden eisen gesteld aan de organisatie, inrichting en controleerbaarheid van het onderzoeksproces. De uitwerking hiervan vindt plaats in de opsporingspraktijk, aan de hand van onder meer OM-aanwijzingen, (keurings)protocollen, handreikingen en mandaatbesluiten. De Inspectie Veiligheid en Justitie (hierna: Inspectie VenJ) houdt toezicht op de naleving van de regels die zijn neergelegd in het Wetboek van Strafvordering en in het onderhavige besluit bij de uitvoering van het onderzoek in een geautomatiseerd werk door opsporingsambtenaren.

3.2 Deskundigheid van opsporingsambtenaren

In hoofdstuk 3 van dit besluit worden regels gesteld over de opsporingsambtenaren die kunnen worden aangewezen voor het onderzoek in een geautomatiseerd werk, hun deskundigheid en de samenwerking tussen opsporingsambtenaren. 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. Op grond van het besluit kunnen opsporingsambtenaren van de politie, de Koninklijke marechaussee (Kmar) en de bijzondere opsporingsdiensten, en buitengewone

opsporingsambtenaren, bedoeld in artikel 141 Sv onder b, c en d, en 142 Sv door de korpschef worden aangewezen voor het binnendringen in een geautomatiseerd werk en al dan niet met behulp van een technisch hulpmiddel onderzoek doen, indien zij lid zijn van een technisch team. De politie heeft behoefte aan de bevoegdheid met het oog op de uitvoering van de politietaken, bedoeld in artikel 3 van de Politiewet 2012, namelijk de opsporing van computercriminaliteit en vormen van commune criminaliteit, waarbij geen andere aanknopingspunten zijn voor de opsporing van het misdrijf dan het gebruikte geautomatiseerde werk. Bij de Kmar bestaat de behoefte aan deze bevoegdheid met het oog op de uitvoering van de in artikel 4 van de Politiewet 2012 genoemde politietaken. Bij de FIOD/ECD bestaat behoefte aan deze bevoegdheid met het oog op de strafrechtelijke handhaving van de rechtsorde op bepaalde beleidsterreinen, bedoeld in artikel 3 van de Wet op de bijzondere opsporingsdiensten, te weten de opsporing van fraude en witwassen.

In verband met de behoefte aan specifieke expertise op het gebied van ICT kunnen naast de in artikel 141 Sv bedoelde opsporingsambtenaren ook buitengewone opsporingsambtenaren, bedoeld in artikel 142 Sv, die categoriaal zijn aangewezen door de Minister van Veiligheid en Justitie, worden belast met het binnendringen in een geautomatiseerd werk en het doen van onderzoek. Hun opsporingsbevoegdheid strekt zich uit tot de in de categorale aanwijzing aangeduide feiten. De kwaliteit van een technisch team wordt geborgd door middel van opleidingseisen. Een opsporingsambtenaar kan lid worden van een technisch team, indien hij heeft voldaan aan door de Minister van Veiligheid en Justitie aangewezen kwalificaties, onder meer ten aanzien van kennis op het gebied van ICT. De opleidingseisen worden nader worden uitgewerkt in een ministeriële regeling, die tegelijk met dit besluit in werking treedt.

Gelet op de bijzondere expertise en de technische voorzieningen die nodig zijn voor het 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.

Incidentele samenwerking tussen leden van een technisch team en andere opsporingsambtenaren is mogelijk, het besluit bevat hiervoor een voorziening. Een opsporingsambtenaar die geen lid is van een technisch team kan worden aangewezen voor het binnendringen in een geautomatiseerd werk en doen van onderzoek, indien hij beschikt over specifieke kennis en vaardigheden die nodig zijn voor de uitvoering van het onderzoek in een geautomatiseerd werk in het kader van een individueel opsporingsonderzoek. Dit staat ter beoordeling van de korpschef. Bij een positieve beoordeling wordt de opsporingsambtenaar op incidentele basis als deelnemer toegevoegd aan een technisch team en wordt hij gedurende het de uitvoering van het bevel begeleid door een lid van een technisch team.

3.3 Taakverdeling en functiescheiding gedurende het opsporingsonderzoek

Gedurende het opsporingsonderzoek, dat plaatsvindt onder het gezag van de officier van justitie, is er sprake van een strikte taakverdeling en functiescheiding. 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 en behoren niet tot het tactische team. Het tactische team is belast met het uitvoeren van het operationele onderzoek.

De voorbereiding van het onderzoek in een geautomatiseerd werk start met een projectvoorstel van een tactisch team aan de officier van justitie, waarin het onderzoek in een concrete zaak wordt voorgesteld. Een projectplan kan afkomstig zijn van tactische researcheteams van de politie, van de Kmar of van een bijzondere opsporingsdienst. Het projectplan bevat onder meer een beschrijving van de verdachte, de verdenking, de noodzaak om de onderzoeksbevoegdheid toe te passen en de gewenste resultaten van de toepassing van de bevoegdheid.

Vervolgens vraagt de officier van justitie een technisch team om advies over de haalbaarheid van het onderzoek. Voor de inschatting, beheersing en beperking van de risico's voor het geautomatiseerde werk is de deskundigheid van de opsporingsambtenaren van het technische team van essentieel belang. Omdat het technische team niet betrokken is bij het operationele onderzoek van het tactische team kan het niet worden beïnvloed bij het maken van afwegingen

met betrekking tot de haalbaarheid en de wijze van uitvoering van het binnendringen in en het verrichten van onderzoekshandelingen in een geautomatiseerd werk.

Het technische team stelt op basis van de intakegegevens en overige relevante gegevens een rapport haalbaarheidsonderzoek op voor de officier van justitie. Hierin wordt het plan van aanpak voor de uitvoering van een onderzoek in het geautomatiseerde werk uitgewerkt. In het rapport wordt onder meer opgenomen welke bevelen nodig zijn en welk technisch hulpmiddel moet worden gebruikt. De officier van justitie gebruikt het rapport haalbaarheidsonderzoek 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.

Het onderzoek in een geautomatiseerd werk kan worden uitgevoerd, zodra daartoe een bevel is afgegeven door de officier van justitie. Het onderzoek is voorbehouden aan de opsporingsambtenaren van een technisch team. In de hoofdstukken 3, 7, 8 en 9 van dit besluit wordt de taakverdeling uitgewerkt.

Na afgifte van een bevel zal een technisch team eerst voorverkenningen uitvoeren. Na analyse daarvan wordt een plan van aanpak voor het binnendringen in het geautomatiseerd werk opgesteld. Het plan van aanpak wordt getest in een proefopstelling.

Het daadwerkelijke onderzoek in het geautomatiseerde werk bestaat uit een voorbereidende fase en een onderzoekfase. De voorbereidende fase omvat het binnendringen in het geautomatiseerde werk volgens het vooraf geschreven plan van aanpak. Hierbij kunnen, zoals hiervoor is aangegeven, verschillende technieken worden gebruikt. De onderzoeksfase bestaat uit het uitvoeren van onderzoekshandelingen in een geautomatiseerd werk. De onderzoekshandelingen kunnen worden verricht met behulp van een technisch hulpmiddel, een softwareapplicatie die gegevens detecteert, registreert en transporteert. Het gebruik van een technisch hulpmiddel is echter niet strikt noodzakelijk: onderzoekshandelingen kunnen ook ad hoc en handmatig plaatsvinden.

De tijdens een onderzoek in een geautomatiseerd werk met een technisch hulpmiddel geregistreerde gegevens worden automatisch vastgelegd op een technische infrastructuur van een technisch team. De vastgelegde gegevens zijn uitsluitend toegankelijk voor de door de korpschef aangewezen ambtenaren. Tactische opsporingsambtenaren hebben geen toegang tot de gegevens. De technische infrastructuur is beveiligd tegen wijziging van de vastgelegde gegevens en kennisneming hiervan door onbevoegden.

De resultaten van het onderzoek worden door het technische team ter beschikking gesteld aan het tactische team. Zo nodig kan het technische team, op basis van technische criteria, zorgdragen voor voorafgaande filtering van de onderzoeksgegevens, zodat binnen de categorieën van gegevens die in het bevel van de officier zijn opgenomen uitsluitend die gegevens die van belang zijn voor het opsporingsonderzoek ter beschikking komen van het tactische team. Bij het opnemen van vertrouwelijke communicatie of het opnemen van telecommunicatie of de vastlegging van gegevens die in het geautomatiseerde werk zijn of worden opgeslagen, zoals email-verkeer, 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. In dat geval wordt uitsluitend het email-verkeer waarvan de email-adressen zijn opgenomen op een vooraf opgestelde lijst ter beschikking gesteld van het tactische onderzoeksteam. In het bevel dient melding te worden gemaakt van het feit dat binnen de categorie van gegevens waarvoor het bevel wordt afgegeven uitsluitend die onderzoeksgegevens die van belang zijn voor het opsporingsonderzoek ter beschikking worden gesteld van het tactische team.

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. Afhankelijk van het verloop van het onderzoek kan de grens tussen het technisch optreden en het tactisch optreden verschillen, maar de samenwerking zal dusdanig plaatsvinden dat het tactisch team geen enkele invloed kan uitoefenen op het binnendringen in het geautomatiseerde werk en de plaatsing, inzet en verwijdering van een technisch hulpmiddel.

3.4. Vastlegging van gegevens over de uitvoering van een bevel (logging)

De digitale omgeving waarin het onderzoek in een geautomatiseerd werk plaatsvindt maakt het

mogelijk om gedurende de onderzoeksfase doorlopend en automatisch gegevens vast te leggen over de uitvoering van het bevel van de officier van justitie. Hierdoor kan zowel tijdens de uitvoering van bevel van de officier als na afloop hiervan worden vastgesteld of een handeling of bewerking heeft plaatsgevonden die van invloed is op de betrouwbaarheid en integriteit van de vastgelegde gegevens. Deze vorm van elektronische verslaglegging over de uitvoering van een bevel wordt ook wel aangeduid als "logging".

In hoofdstuk 4 van dit besluit worden regels gesteld over de logging. Gedurende de uitvoering van een bevel worden gegevens over onderzoekshandelingen die worden verricht doorlopend en automatisch worden vastgelegd. Onder de logging van de onderzoekshandelingen valt ook de vastlegging van de gegevens die door een technisch hulpmiddel worden geregistreerd, de zogenaamde bewijslogging. De bewijslogging dient plaats te vinden op een technische infrastructuur van een technisch team. Het functioneren van de technische infrastructuur wordt eveneens doorlopend en automatisch gelogd.

De logging dient zodanig te zijn ingericht dat op basis hiervan kan worden vastgesteld of en zo ja wanneer een onregelmatigheid heeft plaatsgevonden, die van invloed is op de betrouwbaarheid en integriteit van de tijdens de onderzoeksfase vergaarde gegevens. Indien dat het geval is, maakt de opsporingsambtenaar van een technisch team hiervan proces-verbaal op, dat aan de officier van justitie wordt gezonden, zodat de officier van justitie en de rechter kunnen bepalen in hoeverre de geconstateerde onregelmatigheid afbreuk doet aan de bewijskracht van de tijdens het onderzoek vastgelegde gegevens.

Het voorbereidende deel van het onderzoek, het binnendringen in een geautomatiseerd werk, behoeft niet te worden gelogd, omdat de handelingen die in dit deel van het onderzoek plaatsvinden niet van invloed zijn op de betrouwbaarheid en de integriteit van het bewijs. Als in een strafzaak vragen zouden rijzen over de wijze van binnendringen, is het aan de rechter om hierover te oordelen. Zo nodig kan een rechter overgaan tot het horen van de betrokken opsporingsambtenaar of kan hij een deskundige raadplegen.

De logging is ten eerste en vooral bedoeld voor de interne controle van de tijdens de onderzoeksfase verrichte handelingen. Daarnaast maakt de bewijslogging het mogelijk om de met een technisch hulpmiddel geregistreerde gegevens achteraf te verantwoorden in een strafzaak. Die verantwoording vindt plaats aan de hand van de processen-verbaal en andere voorwerpen waaraan gegevens kunnen worden ontleend die voor het onderzoek in de zaak van betekenis zijn (artikel 126aa Sv). De officier van justitie houdt bij het samenstellen van het strafdossier rekening met bijzondere belangen zoals de afscherming van methodieken en middelen. Deze belangen kunnen een minder gedetailleerde verantwoording rechtvaardigen. Als bij het verrichten van onderzoekshandelingen in een geautomatiseerd werk gebruik gemaakt wordt van een gekeurd technisch hulpmiddel zal in het proces-verbaal van de inzet worden verwezen naar het keuringsnummer, waardoor de samenstelling van het hulpmiddel ter bescherming van de opsporingsbelangen, kan worden afgeschermd.

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

3.5. Het doen van onderzoek met een gekeurd technisch hulpmiddel

3.5.1. Algemeen

Het doen van onderzoek in een geautomatiseerd werk met het oog op in het bevel van de officier van justitie opgenomen onderzoeksdoelen kan plaatsvinden met een technisch hulpmiddel. Een technisch hulpmiddel is een softwareapplicatie die functionaliteiten bevat waarmee gegevens kunnen worden gedetecteerd, geregistreerd en getransporteerd. Het transport van de geregistreerde gegevens vindt plaats naar een technische infrastructuur, een opslaglocatie in beheer van de politie, waarop de gegevens worden vastgelegd. De vastgelegde gegevens kunnen als bewijs dienen in een strafzaak. Gelet hierop is het essentieel dat de gegevens betrouwbaar,

integer en herleidbaar zijn.

In de hoofdstukken 5 tot en met 9 van dit besluit worden regels gesteld over technische hulpmiddelen waarmee onderzoek wordt gedaan in een geautomatiseerd werk. Deze regels hebben ten eerste betrekking op de technische eisen waaraan technische hulpmiddelen moeten voldoen en de voorafgaande goedkeuring hiervan. Ten tweede worden regels gesteld over de toegang tot, plaatsing, inzet en verwijdering van technische hulpmiddelen en de vastlegging van met een technisch hulpmiddel geregistreerde gegevens op een technische infrastructuur binnen de politieorganisatie.

Het verrichten van onderzoekshandelingen in een geautomatiseerd werk kan plaatsvinden met het oog op bestaande bijzondere opsporingsbevoegdheden. Het betreft de stelselmatige observatie, het opnemen van communicatie of van vertrouwelijke communicatie (artikelen 126g, 126o, 126zd, eerste lid, onder a, 126l, 126m, 126s, 126t of 126zg Sv). Het Besluit technische hulpmiddelen strafvordering stelt eisen aan de "traditionele" technische hulpmiddelen die daarbij worden ingezet, zoals een camera of een richtmicrofoon.

Op grond van het wetsvoorstel computercriminaliteit III wordt het mogelijk om deze bevoegdheden uit te oefenen nadat heimelijk en op afstand is binnengedrongen in een geautomatiseerd werk. In het onderhavige besluit worden eisen gesteld aan technische hulpmiddelen die worden gebruikt bij de inzet van de bestaande bijzondere opsporingsbevoegdheden in het kader van een onderzoek in een geautomatiseerd werk. Alsdan en gelden specifieke eisen voor de inzet van een technisch hulpmiddel, die zijn toegesneden op het gebruik in een digitale omgeving. Hieruit vloeit voort dat niet voldaan hoeft te worden aan de eisen van het Besluit technische hulpmiddelen strafvordering wat betreft de eisen met betrekking tot de 'traditionele' technische hulpmiddelen.

3.5.2. Technische eisen

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 eisen aan een technisch hulpmiddel. Een technisch hulpmiddel moet in staat zijn om gegevens op zodanige wijze te registreren dat de inhoud identiek is aan de in een geautomatiseerd werk gedetecteerde gegevens. Ook moet een technisch hulpmiddel geregistreerde gegevens kunnen voorzien van de datum en tijd van de registratie. Verder moet een technisch hulpmiddel de geregistreerde gegevens kunnen voorzien van een uniek kenmerk, dat bij vastlegging van de gegevens op de opslaglocatie wordt herkend, zodat de herkomst van de gegevens te allen tijde kan worden vastgesteld.

De integriteit van de met een technisch hulpmiddel vergaarde gegevens, waarmee bedoeld wordt op de zekerheid dat een gegeven niet is gewijzigd of hiervan onbevoegd kennis is genomen, wordt geborgd door eisen te stellen aan de beveiliging van een technisch hulpmiddel en de door een technisch hulpmiddel geregistreerde en getransporteerde gegevens. Naast technische eisen aan het technische hulpmiddel stelt het besluit ook eisen met betrekking tot de kwaliteit van de technische infrastructuur waarop de met een technisch hulpmiddel geregistreerde gegevens worden vastgelegd.

Om de rechtmatigheid van de inzet van een hulpmiddel te kunnen garanderen vereist het besluit dat een technisch hulpmiddel zodanig is ingericht dat het mogelijk is om uitsluitend de in het bevel van de officier van justitie aangegeven functionaliteit(en) van een technisch hulpmiddel in te schakelen en uitsluitend gegevens te detecteren en registeren ten behoeve van deze functionaliteit.

3.5.3. Keuring

Voordat een technisch hulpmiddel wordt ingezet, dient het goedgekeurd te worden door een keuringsdienst. Als bij het verrichten van onderzoekshandelingen gebruik wordt gemaakt van een goedgekeurd hulpmiddel mag er vanuit worden gegaan dat aan de wettelijke eisen is voldaan. Een onderdeel van de Landelijke eenheid van de Nationale Politie, de keuringsdienst van de Dienst landelijke operationele samenwerking, is momenteel belast met de keuring van de traditionele technische hulpmiddelen die worden ingezet bij stelselmatige observatie, het opnemen van vertrouwelijke communicatie en het opnemen van telecommunicatie. Deze keuringsdienst wordt

eveneens aangewezen voor de keuring van technische hulpmiddelen die gebruikt worden voor het verrichten van onderzoekshandelingen in een geautomatiseerd werk. Het besluit bevat de mogelijkheid om andere organisaties als keuringsdienst aan te wijzen. Om de kwaliteit en consistentie van de keuring te waarborgen stelt een keuringsdienst een keuringsprotocol op. Een keuringsprotocol behoeft de voorafgaande goedkeuring van de Minister van Veiligheid en Justitie. Van de keuring wordt een rapport opgemaakt, waarin bij goedkeuring wordt vermeld dat het technische hulpmiddel voldoet aan de technische eisen die het besluit stelt. Bij de goedkeuring wordt aan het technische hulpmiddel een referentienummer toegekend. Dit referentienummer kan gedurende het opsporingsonderzoek worden gebruikt om het hulpmiddel aan te duiden zodat de samenstelling van het hulpmiddel, ter bescherming opsporingsbelangen, kan worden afgeschermd. De mogelijkheid bestaat om softwareapplicaties van verschillende producenten te betrekken of deze zelf binnen de politieorganisatie te (laten) ontwerpen, mits aan de wettelijke vereisten voor keuring wordt voldaan. De ervaring leert dat producenten van software veelvuldig gebruik maken van softwareupdates ter verbetering van het product. Indien de werking van een technisch hulpmiddel of een onderdeel hiervan door een softwareupdate zodanig wijzigt dat niet meer wordt voldaan aan de technische eisen vindt herkeuring plaats van het technische hulpmiddel of van het gewijzigde onderdeel hiervan.

3.6. Het doen van onderzoek zonder goedgekeurd technisch hulpmiddel

Het is denkbaar dat bij het verrichten van onderzoekshandelingen technische hulpmiddelen, worden gebruikt die zich naar hun aard niet lenen voor voorafgaande goedkeuring. Hierbij kan worden gedacht aan op maat gemaakte software, zoals een script dat is geschreven door een technisch team en dat "semi-handmatig" wordt ingezet. Indien het onderzoeksbelang dit dringend vordert kan de officier van justitie bepalen dat een niet gekeurd technisch hulpmiddel wordt ingezet. Na afloop van het onderzoek kan alsnog goedkeuring plaatsvinden, tenzij de aard van het hulpmiddel zich naar het oordeel van de officier hiertegen verzet. De betrouwbaarheid, integriteit en herleidbaarheid van de vastgelegde gegevens zullen dan op andere wijze moeten worden geborgd. Ook als onderzoekshandelingen zonder goedgekeurd hulpmiddel plaatsvinden worden de verrichte onderzoekshandelingen en het functioneren van de technische infrastructuur gelogd. In bepaalde gevallen kunnen onderzoekshandelingen beter handmatig worden verricht, zodat het gebruik van een technisch hulpmiddel achterwege kan blijven. Hierbij kan worden gedacht aan de situatie dat gegevens direct na het binnendringen kunnen worden ingezien of worden overgenomen ten behoeve van het vaststellen van de identiteit van het geautomatiseerde werk. De vraag of de inzet van een technisch hulpmiddel noodzakelijk is, is onder meer afhankelijk van de aard van de inzet, de aard van het geautomatiseerde werk en de vraag of de gegevens zonder inzet van een technisch hulpmiddel als rechtmatig bewijs kunnen worden aangemerkt. De advisering van de officier van justitie hieromtrent vindt plaats door het technische team.

4. Bewaartermijnen

De gegevens die al dan niet met een technisch hulpmiddel ter uitvoering van een bevel van de officier worden vastgelegd vallen onder een gedifferentieerd regime wat betreft de bewaartermijnen. De processen-verbaal en andere voorwerpen waaraan gegevens kunnen worden ontleend die zijn verkregen door observatie, het opnemen van vertrouwelijke communicatie en het opnemen van telecommunicatie met behulp van een technisch hulpmiddel worden door de officier van justitie, voor zover die niet bij de processtukken zijn gevoegd, ter beschikking gehouden van het onderzoek (artikel 126cc, eerste lid, Sv). 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. De procedure is uitgewerkt in het Besluit bewaren en vernietigen niet-gevoegde stukken.

De gegevens die zijn verkregen door de toepassing van de bevoegdheid met het oog op andere onderzoekshandelingen en al dan niet met een technisch hulpmiddel zijn gegenereerd vallen onder het regime van de Wet politiegegevens (Wpg). Afhankelijk van het specifieke doel van de verwerking kan de bewaartermijn verschillen. Doorgaans zullen de gegevens worden verwerkt met het oog op de ten behoeve van een onderzoek met het oog op de handhaving van de rechtsorde in een bepaald geval (artikel 9, eerste lid, Wpg). 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 als bedoeld in het eerste lid of een nieuwe verwerking als bedoeld in artikel 10 Wpg. Na afloop van deze termijn worden de gegevens verwijderd (artikel 9, derde lid, Wpg). 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. 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 kunnen in dat geval nodig blijven voor het vervolg van het onderzoek en voor het geval dat het team opnieuw bijeen wordt geroepen vanwege nieuwe aanknopingspunten. 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. Daarna kunnen de gegevens niet meer nodig zijn voor het doel van het onderzoek en moeten zij worden verwijderd (Kamerstukken II 2005/06, 30 327, nr. 3, blz. 45/46). 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.

De logging wordt bewaard met het oog op de verantwoording van de verrichte onderzoekshandelingen en het functioneren van de technische infrastructuur waarop de met een technisch hulpmiddel geregistreerde gegevens worden vastgelegd. Deze gegevens worden verwerkt met het oog op de opsporing van strafbare feiten en vallen eveneens onder de reikwijdte van de Wpg. Dit betekent dat de gegevens doorgaans moeten worden verwijderd zodra deze niet langer noodzakelijk zijn voor het doel van het onderzoek. Dit geldt in zijn algemeenheid voor de logging van gegevens, dus ook voor de logging met betrekking tot het verrichten van onderzoekshandelingen met het oog op observatie, het opnemen van vertrouwelijke communicatie of het opnemen van telecommunicatie met behulp van een technisch hulpmiddel.

5. Systeemtoezicht

De Inspectie VenJ houdt toezicht op het functioneren van het wettelijke systeem rond de uitvoering van een bevel tot onderzoek in een geautomatiseerd werk. De Inspectie VenJ is belast met het toezicht op de taakuitvoering door de politie op grond van artikel 57, eerste lid, onderdeel d, van de Wet veiligheidsregio's. Artikel 126nba, zevende lid, Sv, (dat van overeenkomstige toepassing is verklaard in de artikelen 126uba/126zpa, derde lid, Sv) bepaalt dat het door de Inspectie uitgeoefende toezicht zich mede uitstrekt over de uitvoering van een bevel tot het binnendringen in een geautomatiseerd werk en onderzoek doen door de opsporingsambtenaren van de bijzondere opsporingsdiensten, bedoeld in artikel 141, onderdeel d, Sv en de buitengewone opsporingsambtenaren, bedoeld in artikel 142, eerste lid, onderdeel b, Sv.

Het toezicht van de Inspectie VenJ heeft betrekking op de naleving van de wettelijke regels die zijn neergelegd in het Wetboek van Strafvordering en het onderhavige besluit en omvat zowel de gevallen die in het kader van de door de officier van justitie ingestelde strafvervolging van een verdachte aan het oordeel van de rechter worden voorgelegd als gevallen die niet tot strafvervolging leiden. Concreet zal het systeemtoezicht van de Inspectie VenJ betrekking hebben op aspecten als de autorisatie 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. De inspecteurs beschikken over de bevoegdheden voor het toezicht op de naleving op grond van de Algemene wet bestuursrecht (Awb) (artikel 57, derde lid, Wet veiligheidsregio's, artikelen 5:12 tot en met 5:20 Awb).

De Inspectie VenJ werkt op basis van een werkprogramma dat jaarlijks wordt vastgesteld. Voor de invulling van het toezicht zullen naar verwachting de volgende vormen worden gebruikt: doorlichting, thematisch onderzoek en incidentonderzoek. Na afloop van een onderzoek wordt een rapport opgesteld. Het vastgestelde inspectierapport wordt aan de Minister van Veiligheid en Justitie aangeboden en door de Minister openbaar gemaakt.

Om de verhouding tussen taakuitoefening door de Inspectie VenJ en het verstrekkingenregime van de Wpg te verhelderen past dit besluit het Besluit politiegegevens aan. Daarmee wordt de verplichting tot verstrekking van politiegegevens in het kader van de toezichthoudende taak van de Inspectie VenJ expliciet wettelijk vastgelegd.

6. Europeesrechtelijke aspecten

Het vrij verkeer van goederen en diensten binnen de Europese Unie brengt met zich dat lidstaten in de nationale wetgeving geen eisen aan goederen en keuringen mogen stellen die leiden tot beperking van het vrije verkeer tussen de lidstaten. De technische eisen die in het besluit worden gesteld aan de technische hulpmiddelen waarmee onderzoekshandelingen in een geautomatiseerd werk worden verricht en de voorgeschreven keuring kunnen worden aangemerkt als een inbreuk op het vrije verkeer. Daarom is een wederzijdse erkenningsclausule opgenomen voor hulpmiddelen en keuringen.

Dit besluit biedt de mogelijkheid om naast de keuringsdienst van de Landelijke eenheid van de Nationale Politie andere keuringsdiensten aan te wijzen voor de keuring van technische hulpmiddelen. Als van deze mogelijkheid gebruik wordt gemaakt, dan worden hierover bij ministeriële regeling regels gesteld. Afhankelijk van de gekozen systematiek kan sprake zijn van een dienst van algemeen economisch belang of een niet-economische dienst van algemeen belang. Bij het opstellen van de ministeriële regeling zal dan toetsing plaatsvinden aan de daarvoor geldende EU-kaders, zoals de richtlijn 2006/123/EG van het Europees Parlement en de Raad van de Europese Unie van 12 december 2006 betreffende diensten op de interne markt (PbEU L 376) (Dienstenrichtlijn).

Het ontwerpbesluit is op **PM** gemeld aan de Europese Commissie onder richtlijn 2015/1535/EU (richtlijn van het Europees Parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende diensten van de informatiemaatschappij (codificatie van richtlijn 98/34/EG en 98/48/EG, 'de notificatierichtlijn')).

7. Financiële gevolgen

Het is de verwachting dat de nieuwe opsporingsbevoegdheid niet leidt tot structurele toename van de totale opsporingsinspanning. De uitvoering van het onderzoek in een geautomatiseerd werk vindt plaats bij een onderdeel van de Landelijke eenheid van de Nationale Politie. De Nationale Politie ontvangt jaarlijks een bijzondere bijdrage van €13,8 miljoen voor de digitale professionalisering en vernieuwing van de organisatie, onder meer ter bestrijding van cybercrime. De aanschaf en implementatie van ICT-hulpmiddelen ter voorbereiding op de invoering van het onderzoek in een geautomatiseerd werk geschiedt uit dit budget. De personeels- en IV-capaciteit en de structurele kosten voor beheer en onderhoud komen ten laste van de algemene begroting van de politie. Aan de begroting van de politie is bij najaarsnota structureel een bedrag toegevoegd voor de aanpak van cybercrime. Voor 2017 bedraagt de bijdrage € 1,4 miljoen, voor 2018 en verdere jaren € 1,5 miljoen. Deze bijdragen zijn bedoeld voor de versterking van personele en materiële capaciteit door opleiding en ICT-middelen en – tools. Voor zover het besluit leidt tot werklastgevolgen bij het openbaar ministerie en de rechtspraak worden de kosten gedekt binnen het reguliere budget.

8. Adviezen

PM.

II. Artikelsgewijze toelichting

Hoofdstuk 1 Algemene bepalingen

Artikel 1 Definities

Artikel 1 bevat een definitiebepaling van een aantal relevante begrippen in het besluit. Het meest gebruikte begrip is het begrip "technisch hulpmiddel" (onderdeel g). Hieronder wordt verstaan: softwareapplicatie die gegevens detecteert, registreert en transporteert en waarmee onderzoekshandelingen worden verricht ter uitvoering van een bevel. Onder bevel (onderdeel a) wordt verstaan: een bevel van de officier van justitie als bedoeld in de artikelen 126nba, eerste lid, 126uba, eerste lid, en 126zpa, eerste lid, Sv. Op grond van het wetsvoorstel computercriminaliteit III kan het doen van onderzoek al dan niet met een technisch hulpmiddel plaatsvinden. Van doen van onderzoek zonder technisch hulpmiddel is sprake als bij het onderzoek geen gebruik wordt gemaakt van software die gegevens detecteert, registreert en transporteert.

Een "onderzoekshandeling" is een handeling van een opsporingsambtenaar van een technisch team die met het oog op een onderzoeksdoel als bedoeld in de artikelen 126nba, eerste lid, a tot en met e, 126uba, eerste lid, onder a tot en met e, en 126zpa, eerste lid, Sv wordt verricht ter uitvoering van een bevel. Gedurende de uitvoering van een bevel vindt doorlopende en automatische vastlegging van gegevens plaats over de verrichte onderzoekshandelingen. Met de definitie van "technische infrastructuur" (onderdeel h) wordt bedoeld op de opslaglocatie voor de met een technisch hulpmiddel geregistreerde gegevens. Uit deze definitie, in combinatie met de definitie van "technisch team" (onderdeel i), vloeit voort dat de vastlegging van geregistreerde gegevens dient plaats te vinden op een technische voorziening binnen de politieorganisatie. Deze eis wordt gesteld om de betrouwbaarheid en integriteit van de door een technisch hulpmiddel geregistreerde gegevens te borgen en onbevoegde wijziging of kennisneming hiervan te voorkomen. In de definitie van "technisch team" is de centrale plaatsing van dit team als herkenbaar onderdeel binnen de Landelijke eenheid tot uitdrukking gebracht.

Hoofdstuk 2 Toepassing van de bevoegdheid met het oog op het vastleggen van gegevens of het ontoegankelijkmaken van gegevens

Artikel 2 Aanwijzing misdrijven

In dit artikel wordt een aantal ernstige misdrijven aangewezen waarvoor de binnendring- en onderzoeksbevoegdheid met het oog op de vastlegging van gegevens en ontoegankelijkmaking van gegevens kan worden toegepast. Het betreft misdrijven die met of met behulp van een geautomatiseerd werk worden gepleegd waarop een wettelijke strafbedreiging van minder dan acht jaren gevangenisstraf staat, maar die niettemin dermate ernstig zijn dat er een duidelijk maatschappelijk belang is bij de beëindiging van de strafbare situatie en de vervolging van de daders.

De eerste categorie van misdrijven die worden aangewezen zijn computermisdrijven in enge zin, waarbij het misdrijf met een geautomatiseerd werk wordt gepleegd of betrekking heeft op een geautomatiseerd werk. Deze misdrijven zijn verspreid opgenomen in het Wetboek van Strafrecht. Het betreft in de eerste plaats de strafbaarstellingen van computervredereuk, waaronder het gebruik van een botnet (artikelen 138ab Sr) en van ernstige "spam" of "bombing" (artikel 138b Sr), die zijn opgenomen in de Titel over de misdrijven tegen de openbare orde (Boek II, Titel V). Het wetsvoorstel computercriminaliteit III voegt hieraan strafbaarstellingen inzake het overnemen en helen van gegevens (artikelen 138c en 139g) toe, deze misdrijven worden eveneens aangewezen. Ook de bepalingen uit deze Titel over het aftappen of opnemen van gegevens (artikel 139d) zijn relevant, voor zover het gaat om het aftappen en opnemen van computergegevens. Daarnaast gaat het om de artikelen 161, eerste lid, 161bis en 161sexies, waarin de vernieling van geautomatiseerde werken en werken voor de vitale infrastructuur strafbaar is gesteld. Deze strafbepalingen maken onderdeel uit van Boek II, Titel VII, misdrijven waardoor de algemene veiligheid van personen of goederen in gevaar wordt gebracht. Ook Boek II, Titel XXVII (vernieling) bevat enkele computermisdrijven. Het betreft de artikelen 350a, 350c en 350d (beschadiging van computergegevens), deze misdrijven worden eveneens aangewezen voor de toepassing van de bevoegdheid.

De tweede categorie van misdrijven betreft ernstige commune misdrijven met een grote maatschappelijke impact die in toenemende mate worden gepleegd met behulp van een geautomatiseerd werk. Bij deze vormen van gedigitaliseerde criminaliteit is het geautomatiseerde werk waarvan gebruik wordt gemaakt bij het plegen van het misdrijf vaak het enige aanknopingspunt voor de opsporing. Aangewezen worden diverse ernstige ondermijnende misdrijven die strafbaar zijn gesteld in verschillende titels van het Wetboek van Strafrecht (Boek II, Titel V, misdrijven tegen de openbare orde, Titel VIII, misdrijven tegen het openbaar gezag Titel XII, valsheid in geschrifte, Titel XXXA Witwassen), te weten de rekrutering voor terrorisme (artikelen 131 en 205 Sr), het deelnemen aan een criminele organisatie (artikel 140 Sr), mensensmokkel (artikel 197a Sr) corruptie (artikelen 177, 179, 182, 200 Sr), fraude (artikelen 225, 226, 227, 231, 231a, 232 Sr) en witwassen (artikel 420bis Sr). Ook spionagemisdrijven (artikelen 98, 98c Sr), waarmee een inbreuk wordt gemaakt op de veiligheid van de staat (Boek II, Titel I), worden in toenemende mate langs digitale weg gepleegd. Hetzelfde geldt voor het plaatsen van een valse bom of het doen van een valse bommelding (artikel 142 Sr, Boek II, Titel V), waarmee een ernstige inbreuk wordt gemaakt op de openbare orde en waardoor overheidsdiensten in hun functioneren worden belemmerd. Ook zedenmisdrijven met minderjarigen (artikelen 240b, 247, 248a en 248e Sr, Boek II, Titel XIV,) en het misdrijf stalking (artikel 285b Sr, Titel XVIII), waarmee een inbreuk wordt gemaakt op de seksuele dan wel persoonlijke levenssfeer van een ander, vinden steeds vaker online plaats. Voor een effectieve bestrijding van voornoemde ernstige strafbare feiten zijn digitale opsporingsmogelijkheden onontbeerlijk. Door toepassing van de bevoegdheid met het oog het vastleggen dan wel ontoegankelijk maken van gegevens kan digitaal bewijs worden vergaard voor het gepleegde strafbare feit en kunnen criminele activiteiten worden beëindigd.

Hoofdstuk 3 Deskundigheid van opsporingsambtenaren

Artikel 3 Lidmaatschap van een technisch team

Artikel 3 regelt dat het binnendringen in een geautomatiseerd werk en het al dan niet met een technisch hulpmiddel onderzoek doen is voorbehouden aan de door de korpschef aangewezen opsporingsambtenaren van de politie, de Kmar, de bijzondere opsporingsdiensten en buitengewoon opsporingsambtenaren, bedoeld in artikel 141 Sv onder b, c en d, en 142 Sv, die lid zijn van een technisch team. Door het onderzoek in een geautomatiseerd werk voor te behouden aan deskundigen van een technisch team wordt de kwaliteit en de professionaliteit van dit onderzoek geborgd.

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 Kmar en de bijzondere opsporingsdiensten. Opsporingsambtenaren kunnen lid worden van een technisch team, indien zij voldoen aan door de Minister van Veiligheid en Justitie bepaalde kwalificaties. De kwalificaties waaraan een lid van een technisch team moet voldoen worden uitgewerkt in een ministeriële regeling. Een lid van een technisch team zal onder meer moeten beschikken over voldoende kennis en vaardigheden met betrekking tot ICT en kennis over het juridisch kader waarbinnen het onderzoek in een geautomatiseerd werk plaatsvindt. Ook vaardigheden met betrekking het opmaken van processen-verbaal zullen deel uitmaken van de opleidingseisen. Het lidmaatschap van een technisch team is een specialistische functie, het doorlopen van de volledige politieopleiding is gelet hierop niet nodig. De leden van het technische team zullen naar verwachting vooral zogenaamde zij-instromers zijn.

De opsporingsambtenaren van een technisch team behoren niet tot het tactische team dat is belast met het tactische onderzoek. Deze functiescheiding vermindert het risico op tunnelvisie. Het toezicht op de naleving van de deskundigheidseisen maakt onderdeel uit van het systeemtoezicht van de Inspectie VenJ.

Artikel 4 Incidentele samenwerking

Artikel 4 biedt een voorziening voor de incidentele samenwerking tussen opsporingsambtenaren. Een opsporingsambtenaar van de politie, de Kmar, de bijzondere opsporingsdiensten of een buitengewoon opsporingsambtenaar die geen lid is van een technisch team kan door de korpschef

worden aangewezen voor het binnendringen in een geautomatiseerd werk en doen van onderzoek als hij beschikt over specifieke kennis en vaardigheden die nodig zijn voor de uitvoering van een bevel in een individueel opsporingsonderzoek. 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. De korpschef beoordeelt of een opsporingsambtenaar beschikt over voldoende specifieke kennis en vaardigheden voor het onderzoek. De korpschef kan deze bevoegdheid desgewenst mandateren aan het hoofd van het onderdeel van de Landelijke eenheid waar de technische teams worden ondergebracht. Om de kwaliteit en professionaliteit van het onderzoek te borgen bepaalt artikel 4 dat een opsporingsambtenaar die op ad hoc basis deelneemt aan een technisch team gedurende de uitvoering van het onderzoek wordt begeleid door een lid van een technisch team.

Hoofdstuk 4 Geautomatiseerde vastlegging van gegevens over de uitvoering van een bevel (logging)

Artikelen 5 tot en met 7 Vastlegging van gegevens, vaststelling onregelmatigheden en betrouwbaarheid en integriteit gegevens

Artikel 5 bepaalt dat alle onderzoekshandelingen die gedurende de uitvoering van een bevel van de officier van justitie worden verricht en het functioneren van de technische infrastructuur van een technisch team doorlopend en geautomatiseerd worden vastgelegd. Dit wordt ook wel logging genoemd. Er wordt gelogd op het niveau van de autorisatie, op het niveau van de verrichte onderzoekshandelingen en op het niveau van de werking van het systeem. Ter aanvulling op de automatische logging kan ook handmatige verslaggeving plaatsvinden over de uitvoering van een bevel, bijvoorbeeld in de vorm van een journaal. Zowel onderzoekshandelingen die met een technisch hulpmiddel plaatsvinden als onderzoekshandelingen waarbij de inzet van een technisch hulpmiddel achterwege blijft worden gelogd. Hierdoor zal steeds inzichtelijk zijn welke handelingen gedurende de onderzoeksfase door het technische team zijn verricht en is controle op de uitvoering van het bevel van de officier van justitie mogelijk.

Onder de logging van de onderzoekshandelingen valt ook de vastlegging van gegevens van door een technisch hulpmiddel geregistreerde gegevens, de zogenaamde bewijslogging. De vastlegging van de geregistreerde gegevens dient ingevolge artikel 24 van dit besluit plaats te vinden op een technische infrastructuur van een technisch team. Op grond van artikel 6 moet zowel tijdens de onderzoeksfase als achteraf vastgesteld kunnen worden of zich gedurende de uitvoering van het bevel een onregelmatigheid heeft voorgedaan, die van invloed is op de betrouwbaarheid van de op de technische infrastructuur vastgelegde gegevens. Indien dat het geval is, wordt hiervan proces-verbaal opgemaakt, dat aan de officier van justitie wordt gezonden.

In artikel 7 worden eisen gesteld ter borging van de kwaliteit van de logging. De gelogde gegevens mogen niet worden bewerkt, zijn uitsluitend toegankelijk voor daartoe door de korpschef geautoriseerde ambtenaren en moeten beveiligd zijn tegen wijziging of onbevoegde kennisneming. Het voorbereidende deel van het onderzoek, het binnendringen in een geautomatiseerd werk, behoeft niet te worden gelogd, omdat de handelingen die in dit deel van het onderzoek plaatsvinden niet van invloed zijn op de betrouwbaarheid en de integriteit van het bewijs. De gelogde gegevens moeten worden verwijderd zodra deze niet langer noodzakelijk zijn voor het doel van het onderzoek. Toezicht op de naleving van de regels over de logging vindt plaats door de Inspectie VenJ.

De logging dient ten eerste en vooral ter interne controle van de uitvoering van het bevel van de officier van justitie. Daarnaast kunnen door middel van de logging de verrichte onderzoekshandelingen worden verantwoord. De gedurende een opsporingsonderzoek verrichte opsporingshandelingen en de hiermee vergaarde gegevens worden neergelegd in een proces-verbaal (artikel 152 Sv). De officier van justitie voegt de processen-verbaal en andere voorwerpen die gegevens bevatten die voor het onderzoek in de zaak van betekenis zijn bij de processtukken (artikel 126aa Sv). In het geval in een strafzaak 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, kan aan de hand van de logging hierover verantwoording worden afgelegd.

Hoofdstuk 5 Technische eisen met betrekking tot een technisch hulpmiddel

Hoofdstuk 5 bevat de technische eisen waaraan een technisch hulpmiddel moet voldoen. Als bij de uitvoering van een bevel van de officier van justitie gebruik wordt gemaakt van een goedgekeurd technisch hulpmiddel mag er vanuit worden gegaan dat aan de wettelijke eisen is voldaan. In hoofdstuk 6 van dit besluit worden regels gesteld over de keuringsprocedure.

Artikelen 8 en 9 Gerichtte werking, gerichte detectie en registratie

De artikelen 8 en 9 stellen eisen aan de inrichting en werking van een technisch hulpmiddel. De eerste eis betreft de gerichte werking van een technisch hulpmiddel (artikel 8). Het verrichten van onderzoekshandelingen met behulp van een technisch hulpmiddel in een geautomatiseerd werk vindt plaats binnen de grenzen van het bevel van de officier van justitie. Het bevel bevat (onder meer) een aanduiding van de aard en functionaliteit(en) van het technische hulpmiddel.

Softwareapplicaties met behulp waarvan onderzoekshandelingen in een geautomatiseerd werk worden verricht beschikken naar hun aard vaak over verschillende functionaliteiten. Om te waarborgen dat de onderzoekshandelingen binnen de grenzen van het bevel van de officier van justitie worden verricht, bepaalt artikel 8 van het besluit dat een technisch hulpmiddel zodanig is ingericht dat de werking ervan kan worden beperkt tot de in het bevel vermelde functionaliteit of functionaliteiten. Hierbij kan worden gedacht aan functionaliteiten als het opnemen van geluid, het maken van screenshots, het vastleggen van toetsaanslagen of het doorzoeken van bepaalde bestandsmappen en het vastleggen van gegevens hieruit.

Bij de keuring wordt getoetst of een technisch hulpmiddel instellingen bevat waarmee de werking van een technisch hulpmiddel kan worden beperkt tot een bepaalde functionaliteit of tot bepaalde functionaliteiten. De keuringsdienst stelt bij de keuring een handleiding op voor het gebruik van een hulpmiddel, waarin wordt aangegeven welke instellingen bij gebruik van een technisch hulpmiddel voor een bepaalde functionaliteit moeten worden aangevinkt. Bij de plaatsing van een technisch hulpmiddel wordt hierover verantwoording afgelegd in een proces-verbaal (artikel 22 van het besluit).

De in artikel 9 gestelde eis ligt in het verlengde van artikel 8. Een technisch hulpmiddel moet in staat zijn uitsluitend gegevens te detecteren en te registreren ten behoeve van de in het bevel vermelde functionaliteit of functionaliteiten. De eis in artikel 8, tweede lid, is overgenomen uit artikel 11 van het Besluit technische hulpmiddelen strafvordering en heeft betrekking op technische hulpmiddelen die worden ingezet ten behoeve van het opnemen van telecommunicatie. Het technische hulpmiddel dient in staat te zijn om uitsluitend van een vooraf opgegeven nummer de telecommunicatie op te nemen.

Artikelen 10, 11 en 12 Betrouwbaarheid en integriteit, herleidbaarheid, datum tijd

De in de artikelen 10 tot en met 12 gestelde technische eisen strekken ertoe de betrouwbaarheid, integriteit en herleidbaarheid van de met een technisch hulpmiddel geregistreerde gegevens te garanderen. Een technisch hulpmiddel detecteert gegevens in het geautomatiseerde werk, registreert de gedetecteerde gegevens en transporteert de gegevens naar de technische infrastructuur van het technisch team. Omdat de met een technisch hulpmiddel vastgelegde gegevens kunnen dienen als bewijs in een strafzaak, is het van essentieel belang dat de betrouwbaarheid en integriteit van de gegevens vaststaan en dat de gegevens herleidbaar zijn. Dit kan allereerst worden bereikt door te eisen dat de inhoud van de gegevens die door een technisch hulpmiddel worden geregistreerd identiek is aan de inhoud van de gegevens die worden gedetecteerd in het geautomatiseerde werk. Dit wordt geregeld in artikel 10, eerste lid. Met gedetecteerde gegevens wordt bedoeld op de gegevens die een technisch hulpmiddel waarneemt in een te onderzoeken geautomatiseerd werk. Een voorbeeld is het lezen van een bestand op een computer van een verdachte. Van geregistreerde gegevens is sprake als het technische hulpmiddel de gedetecteerde gegevens overneemt uit het geautomatiseerde werk. De eis heeft betrekking op de inhoud van de gegevens. Niet is van belang op welke wijze de metadata worden geregistreerd. Als de in het geautomatiseerde werk gedetecteerde gegevens door het technische hulpmiddel in een ander format worden geregistreerd (een voorbeeld is een SMS die op een mobiel apparaat

als PDU is opgeslagen en die door een technisch hulpmiddel in ASCII coding wordt geregistreerd) zal na de vastlegging van de gegevens op de technische infrastructuur de omzetting van het format met een applicatie moeten worden uitgelokt. Bij de keuring zal worden gekeurd of het technische hulpmiddel een voorziening bevat om de inhoud van de geregistreerde gegevens zichtbaar te maken.

Artikel 10, tweede lid, vereist dat een technisch hulpmiddel beveiligd is tegen wijziging van de werking ervan en tegen de wijziging en kennisneming van geregistreerde gegevens door onbevoegden. Hierbij dient te worden opgemerkt dat in de ICT nooit volledige garanties tegen beïnvloeding van buitenaf kunnen worden gegeven. Wel kan die beïnvloeding zo moeilijk mogelijk worden gemaakt. Bij de keuring wordt getoetst of er beveiligingsmaatregelen aanwezig zijn die beïnvloeding van een technisch hulpmiddel van buitenaf naar de stand van de techniek zo goed mogelijk tegengaan. Hierbij kan worden gedacht aan het aanwezig zijn van authenticatiemaatregelen voor de communicatie met het technische hulpmiddel.

Als een technisch hulpmiddel niet constant met de technische infrastructuur communiceert – het zal in de praktijk regelmatig voorkomen dat een verdachte offline is - dan kan een vorm van tussenopslag nodig zijn. Gelet hierop dient een technisch hulpmiddel beveiligd te zijn tegen wijziging van geregistreerde gegevens en kennisneming hiervan door onbevoegden. Hierbij kan naar de huidige stand van de techniek worden gedacht aan maatregelen als versleuteling van de gegevens met een digitale handtekening. Hierdoor wordt bereikt dat de door een technisch hulpmiddel geregistreerde gegevens na de registratie niet meer leesbaar en toegankelijk zijn. Om te waarborgen dat de gegevens afkomstig zijn van het ter uitvoering van een bevel van de officier geplaatste technische hulpmiddel wordt in artikel 11 de eis gesteld dat een technisch hulpmiddel een uniek gegeven toevoegt aan de geregistreerde gegevens. Uit dit gegeven moet de relatie met het geplaatste technische hulpmiddel blijken. Hierbij kan worden gedacht aan een code die bij de plaatsing aan het technisch hulpmiddel is toegevoegd. De technische infrastructuur moet in staat zijn om bij de vastlegging van de geregistreerde gegevens het unieke gegeven te herkennen. Op deze wijze kan een herleidbaar gegevensspoor worden gecreëerd.

Artikel 12 vereist dat een technisch hulpmiddel de geregistreerde gegevens voorziet van de datum en tijd van de registratie. Hierdoor wordt inzichtelijk op welk moment een onderzoekshandeling heeft plaatsgevonden. De eis van datum- en tijdregistratie betekent niet dat er doorlopend datum- en tijdregistratie moet plaatsvinden gedurende de inzet van een technisch hulpmiddel. Artikel 12 staat er niet aan de in de weg dat een technisch hulpmiddel uitsluitend gegevens registreert als er gegevens van het te onderzoeken geautomatiseerde werk worden ontvangen. De strekking van de eis is dat zodra er gegevens worden geregistreerd door een technisch hulpmiddel er zekerheid bestaat over de datum en het tijdstip van de gegevensregistratie door het technische hulpmiddel. Door middel van de logging van de onderzoekshandelingen en het functioneren van de technische infrastructuur kan controle plaatsvinden op het functioneren van een technisch hulpmiddel. Indien zich gedurende de inzet van een technisch hulpmiddel onregelmatigheden voordoen die van invloed zijn op de kwaliteit van de vastgelegde gegevens kan hierover verantwoording worden afgelegd aan de hand van de logging.

Artikel 13 Transport geregistreerde gegevens

Op grond van artikel 13, eerste lid, van het besluit dient een technisch hulpmiddel zodanig te zijn ingericht dat geregistreerde gegevens automatisch worden getransporteerd naar een technische infrastructuur, die in beheer is bij een technisch team. Deze eis wordt gesteld om onbevoegde toegang van derden tot de met een technisch hulpmiddel geregistreerde gegevens te voorkomen. De keuring van een technisch hulpmiddel strekt zich uit tot het transport naar de opslaglocatie. De technische infrastructuur waarop de vastlegging van met een technisch hulpmiddel geregistreerde gegevens plaatsvindt wordt niet gekeurd. Om de integriteit van de op de technische infrastructuur vastgelegde gegevens te borgen dienen de geregistreerde gegevens tijdens het transport beveiligd te zijn tegen wijziging en kennisneming door onbevoegden (tweede lid). Bij de beoordeling van deze eis kunnen de wijze van beveiliging van de werking van een technisch hulpmiddel en de wijze van beveiliging van de geregistreerde gegevens worden betrokken.

Hoofdstuk 6 Keuring van een technisch hulpmiddel

Artikelen 14 en 15 Voorafgaande goedkeuring, herkeuring en keuring achteraf

Uitgangspunt is bij de inzet gebruik wordt gemaakt van een vooraf goedgekeurd technisch hulpmiddel. Dit wordt geregeld in artikel 14, eerste lid, van het besluit. Een technisch hulpmiddel kan uitsluitend worden goedgekeurd als het voldoet aan de artikelen 8 tot en met 13 gestelde eisen (tweede lid). Dit wordt beoordeeld tijdens de keuring. Artikel 14, derde lid, bevat regels over de herkeuring van technische hulpmiddelen. Herkeuring is aan de orde als de werking van een gekeurd technisch hulpmiddel of een onderdeel hiervan zodanig wijzigt dat redelijkerwijs kan worden aangenomen dat het hulpmiddel niet langer voldoet aan de in de artikelen 8 tot en met 13 gestelde eisen. De herkeuring zal naar zijn aard vooral gericht zijn op de gewijzigde onderdelen van de software, die door de producent meestal in een zogenaamd "change log" worden omschreven. In het geval dat een software update zodanig kort voor de inzet van een technisch hulpmiddel plaatsvindt dat geen herkeuring heeft kunnen plaatsvinden, biedt het besluit de mogelijkheid van herkeuring achteraf (vierde lid).

Van het uitgangspunt van een voorafgaande keuring kan worden afgeweken indien een dringend onderzoeksbelang daartoe noodzaakt. Deze uitzondering is geregeld in artikel 15. Hierbij kan worden gedacht aan de situatie dat keuring voorafgaand aan de inzet teveel tijd zou vergen. Het moet dan gaan om situaties waarin het belang van het onderzoek de inzet van het desbetreffende technische hulpmiddel dringend vordert. Bij deze afweging zal de officier van justitie nagaan of het beoogde technische hulpmiddel naar verwachting zal voldoen aan de in de artikel 8 tot en met 13 gestelde technische eisen. In het bevel van de officier van justitie wordt expliciet vermeld dat een niet gekeurd technisch hulpmiddel wordt ingezet (tweede lid).

Als hoofdregel geldt dat een technisch hulpmiddel dat niet vooraf is goedgekeurd, na afloop van de inzet alsnog ter keuring aan de keuringsdienst wordt aangeboden (derde lid). Indien naar het oordeel van de officier van justitie de aard van een technisch hulpmiddel zich tegen keuring achteraf verzet, kan hij bepalen dat een technisch hulpmiddel niet ter keuring wordt aangeboden. Hierbij kan worden gedacht aan de situatie van een speciaal op maat gemaakt technisch hulpmiddel. Wanneer het technische hulpmiddel specifiek is aangepast aan de omgeving waarin de inzet heeft plaatsgevonden, kan het problematisch zijn om bij een keuring dezelfde situatie na te bootsen. Met name bij op maat gemaakte software die tijdens het verrichten van onderzoekshandelingen nog moet worden aangepast aan de omstandigheden, kan het onuitvoerbaar zijn om de omstandigheden waarbinnen de inzet plaats heeft gevonden te reproduceren en het ingezette technische hulpmiddel daarop te keuren. Indien de officier van justitie besluit om, gelet op de aard van het technische hulpmiddel, keuring achteraf achterwege te laten, dient hij de noodzakelijke procedurele maatregelen te treffen om rechterlijke controle op de inzet mogelijk te maken. Hierbij kan worden gedacht aan een uitgebreide omschrijving van de functionele specificaties van het op maat gemaakte technische hulpmiddel in het proces-verbaal, het vooraf en achteraf maken van een forensische kopie of het audiovisueel vastleggen van het onderzoeksproces. Daarnaast kunnen een digitale kopie van de software en de broncode bij het proces-verbaal worden gevoegd. De aanvullende procedurele eisen van de officier van justitie kunnen de rechtmatigheid van de inzet waarborgen en voorkomen dat er twijfel ontstaat over de betrouwbaarheid, integriteit en herleidbaarheid van de gegenereerde gegevens. Ook onderzoekshandelingen die zonder gekeurd technisch hulpmiddel worden verricht worden gelogd, evenals het functioneren van de technische infrastructuur. In geval van twijfel kan zo nodig via de logging verantwoording worden afgelegd over de verrichte handelingen en het vergaarde bewijsmateriaal.

Artikelen 16 tot en met 19 Keuringsdienst, keuringsprotocol, keuringsrapport

In de artikelen 16 tot en met 19 van dit besluit wordt de keuringsprocedure omschreven. Artikel 16 stelt regels over de aanwijzing van keuringsdiensten. De keuring van technische hulpmiddelen zal primair worden opgedragen aan een onderdeel van de Landelijke eenheid, thans de keuringsdienst van de Dienst Landelijke Operationele Samenwerking (eerste lid). 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. Bij ministeriële regeling kunnen regels worden

gesteld over de aanwijzing van de keuringdienst van de Landelijke eenheid (derde lid). De mogelijkheid bestaat om een andere organisatie aan te wijzen als keuringsdienst (tweede lid). Als van deze mogelijkheid gebruik wordt gemaakt worden hierover bij ministeriële regeling regels gesteld (vierde lid). Afhankelijk van de gekozen systematiek kan sprake zijn van een dienst van algemeen economisch belang of een niet-economische dienst van algemeen belang. Bij het opstellen van de ministeriële regeling zal toetsing aan de geldende EU-kaders plaatsvinden. De keuring van technische hulpmiddelen wordt uitgevoerd op basis van een keuringsprotocol waarin de wijze waarop de keuring plaatsvindt wordt vastgelegd (artikel 17). Daarnaast kunnen in het keuringsprotocol de criteria worden opgenomen die bij de keuring worden gehanteerd. Het keuringsprotocol wordt in samenspraak tussen de keuringsdienst en het openbaar ministerie opgesteld. Een keuringsprotocol behoeft voorafgaande goedkeuring van de Minister van Veiligheid en Justitie. Het is niet wenselijk dat de keuringsdiensten bij keuring van soortgelijke technische hulpmiddelen verschillende keuringsprotocollen hanteren. Indien andere keuringsdiensten worden aangewezen, zal de keuringsdienst van de Landelijke eenheid een coördinerende rol worden toebedeeld bij het opstellen en het gebruik van keuringsprotocollen. De keuring is gericht op die onderdelen van het technische hulpmiddel die van belang zijn voor de detectie, registratie en het transport van gegevens naar een technische infrastructuur. Om de consistentie en de kwaliteit van de keuring te waarborgen wordt de keuring uitgevoerd op basis van voornoemd keuringsprotocol. Artikel 18, eerste lid, bepaalt dat de korpschef een technisch hulpmiddel ter keuring kan aanbieden bij een keuringsdienst. Van de keuring wordt een rapport opgemaakt, waarin de bevindingen van de keuringsdienst worden vastgelegd (tweede lid). De keuring vindt proefondervindelijk plaats. Bij goedkeuring van een technisch hulpmiddel wordt vermeld dat het hulpmiddel voldoet aan de in de artikelen 8 tot en met 13 vermelde eisen (derde lid, onderdeel a). In het keuringsrapport wordt aan een technisch hulpmiddel een uniek keuringsnummer toegekend (derde lid, onderdeel b). In de processen-verbaal die gedurende het opsporingsonderzoek worden opgesteld kan naar dit keuringsnummer worden verwezen. Op deze wijze kan het gebruik van het middel afgeschermd worden ter bescherming van opsporingsbelangen, terwijl de rechter en de verdediging de zekerheid hebben dat het ingezette technische hulpmiddel voldoet aan de wettelijke eisen. Het keuringsrapport bevat verder een omschrijving van de werking van een technisch hulpmiddel en een aanduiding van de functionaliteit of functionaliteiten van het hulpmiddel (derde lid, onderdelen c en d). Bij het opstellen van het rapport haalbaarheidsonderzoek ter advisering van de officier van justitie kan het technische team zich hierop baseren. In het derde lid, onderdeel e, wordt de mogelijkheid gecreëerd om te voldoen aan een of meer in het besluit gestelde technische eisen via het stellen van procedurele waarborgen bij de keuring. De huidige keuringspraktijk heeft uitgewezen dat hieraan behoefte bestaat. Een voorbeeld betreft het ontbreken van een technisch geborgde datum/tijd functie. Dat kan worden opgelost door in een keuringsrapport verplichte procedurele waarborgen te stellen, waardoor materieel aan de technische eisen kan worden voldaan. In de processen-verbaal over de opsporingshandelingen kan hierover verantwoording worden afgelegd. In het keuringsrapport wordt ook melding gemaakt van relevante informatie met betrekking tot de werking van een functionaliteit of functionaliteiten van een technisch hulpmiddel, zoals relevante informatie ten behoeve van de plaatsing, inzet of verwijdering van het technische hulpmiddel (derde lid, onderdeel f). Het rapport van een keuringsdienst bevat de periode waarvoor de keuring geldt zolang de werking hiervan ongewijzigd is (derde lid, onderdeel g). Indien de werking van een technisch hulpmiddel of een onderdeel hiervan zodanig wijzigt dat niet meer voldaan wordt aan de in dit besluit gestelde technische eisen, dient herkeuring plaats te vinden (artikel 14, tweede lid). 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. In artikel 19 wordt geregeld dat de keuringsdienst van de Landelijke eenheid een centrale registratie bijhoudt van de eigen keuringsrapporten en, indien aanwezig, van de keuringsrapporten van andere keuringsdiensten.

Artikel 20 Wederzijdse erkenning

Het beginsel van vrij verkeer van goederen en diensten binnen de Europese Unie brengt met zich

dat lidstaten in de nationale wetgeving geen eisen aan goederen en keuringen mogen stellen die leiden tot beperking van het vrije verkeer tussen de lidstaten. De technische eisen die het besluit stelt aan technische hulpmiddelen en de door het besluit voorgeschreven keuring van technische hulpmiddelen kunnen worden opgevat als een inbreuk op het vrije verkeer. Daarom is in dit artikel een wederzijdse erkenningsclausule opgenomen voor goederen en keuringen.

Hoofdstuk 7 Toegang tot en plaatsing van een technisch hulpmiddel

Artikelen 21 en 22 Toegang en plaatsing van een technisch hulpmiddel

Artikel 21 bepaalt dat de toegang tot technische hulpmiddelen centraal wordt geregistreerd. De korpschef wijst één of meer ambtenaren aan die met de registratie zijn belast. Na vertoon van het bevel van de officier van justitie met daarin een aanduiding van de aard en functionaliteit van het technische hulpmiddel verschaft een met registratie belaste ambtenaar toegang tot een technisch hulpmiddel ten behoeve van de plaatsing ervan. De toegang tot een technisch hulpmiddel wordt verleend voor de periode die nodig is voor de uitvoering van het bevel.

De plaatsing van een technisch hulpmiddel vindt plaats door een opsporingsambtenaar van een technisch team (artikel 22). Dit kan een op grond van de artikelen 3 of 4 van dit besluit aangewezen lid van of deelnemer aan een technisch team zijn.

Het technisch team zal in de praktijk eerst een voorverkenning opstellen. Na analyse daarvan wordt een plan van aanpak voor het binnendringen opgesteld dat wordt getest in een proefopstelling. Nadat is binnengedrongen in het geautomatiseerde werk wordt het technische hulpmiddel geplaatst. Het tweede lid vereist dat bij de plaatsing van een technisch hulpmiddel uitsluitend de in het bevel van de officier van justitie aangeduide functionaliteiten worden ingeschakeld. Hierover dient verantwoording te worden afgelegd in een proces-verbaal. Bij de plaatsing kan het technische hulpmiddel van een uniek gegeven worden voorzien, waarmee de relatie tussen het geplaatste technische hulpmiddel en de met het hulpmiddel vastgelegde gegevens op een technische infrastructuur kan worden aangetoond. De Inspectie VenJ en houdt toezicht op de naleving van de toegang- en plaatsingprocedures en de vereiste autorisaties.

Hoofdstuk 8 Inzet van een technisch hulpmiddel

Artikelen 23 tot en met 27 Inzet van een technisch hulpmiddel en vastlegging van gegevens op een technische infrastructuur

In artikel 23 wordt geregeld dat de inzet van een technisch hulpmiddel plaatsvindt door een opsporingsambtenaar van een technisch team. Van de inzet wordt proces-verbaal opgemaakt. Tijdens de inzet kunnen afhankelijk van de ingeschakelde functionaliteit(en) verschillende soorten gegevens worden geregistreerd. De vastlegging van de geregistreerde gegevens vindt plaats op een technische infrastructuur. Dit betreft een technische voorziening van een technisch team, die is bedoeld voor de vastlegging van de met een technisch hulpmiddel geregistreerde gegevens (artikel 24). Om de betrouwbaarheid, integriteit en herleidbaarheid van de vastgelegde gegevens te borgen stelt het besluit eisen aan de inrichting van de technische infrastructuur waarop de gegevens worden vastgelegd (artikelen 25 tot en met 27 van het besluit). De gegevens mogen niet inhoudelijk worden bewerkt en dienen te worden beveiligd tegen wijziging en kennisneming hiervan door onbevoegden (artikel 25). De vastgelegde gegevens zijn uitsluitend toegankelijk voor de door de korpschef aangewezen ambtenaren. Tactische opsporingsambtenaren hebben geen toegang. De technische infrastructuur moet in staat zijn om het unieke gegeven dat door het technische hulpmiddel aan de geregistreerde gegevens is toegevoegd te herkennen (artikel 26). Zo kan de herkomst van de vastgelegde gegevens worden vastgesteld.

Bij de vastlegging van gegevens op de technische infrastructuur worden de datum en tijd geregistreerd (artikel 27). Hierdoor bestaat zekerheid over de datum en het tijdstip van de vastlegging. Het kan voorkomen dat de datum en tijd in de technische infrastructuur van de politie afwijken van de ingestelde datum en tijd van het te onderzoeken geautomatiseerd werk. Een technisch team heeft geen invloed op de datum en tijd die een verdachte heeft ingesteld in zijn computer of smartphone. Na overlegging van de onderzoeksresultaten door het technische team aan het tactische team kan het tactische team het tijdsverloop reconstrueren.

Via de logging kan controle worden uitgeoefend op de verrichte onderzoekshandelingen en het

functioneren van de technische infrastructuur. Zowel tijdens de uitvoering van een bevel als achteraf moet kunnen worden vastgesteld of wijziging dan wel onbevoegde kennisneming van de ter uitvoering van een bevel vastgelegde gegevens heeft plaatsgevonden. Indien een onregelmatigheid wordt vastgesteld die van invloed is op de kwaliteit van de met een technisch hulpmiddel geregistreerde gegevens dient hiervan proces-verbaal te worden opgemaakt door een opsporingsambtenaar van een technisch team. Dit proces-verbaal wordt aan de officier van justitie gezonden (artikel 6). De Inspectie VenJ houdt toezicht op de naleving van de regels en procedures omtrent de inzet van een technisch hulpmiddel en de vastlegging van gegevens op een beveiligde technische infrastructuur.

Hoofdstuk 9 Verwijdering van een technisch hulpmiddel

Artikelen 28 en 29 Verwijdering van een technisch hulpmiddel, beëindiging transport gegevens

Hoofdregel is dat een technisch hulpmiddel wordt verwijderd uit het te onderzoeken geautomatiseerde werk, nadat het onderzoeksdoel is bereikt of de periode waarvoor het bevel is afgegeven is verstreken (artikel 28). De verwijdering geschiedt door een opsporingsambtenaar van een technisch team. Sommige softwareapplicaties bieden de functionaliteit van een zelfstandige vernietiging van de software na verloop van een bepaalde, vooraf ingestelde, periode.

Vanuit de opsporing bestaat belang bij de verwijdering: bij voorkeur dient te worden voorkomen te dat het gebruik van het technische hulpmiddel bekend wordt. Niettemin kan het voorkomen dat een technisch hulpmiddel niet verwijderd kan worden, bijvoorbeeld omdat voor verwijdering soms meer beheerrechten nodig zijn dan voor de plaatsing. Als het hulpmiddel niet verwijderd kan worden, dan dient het transport van de gegevens te worden beëindigd. Dit wordt geregeld in artikel 29. Van de verwijdering van het technisch hulpmiddel dan wel het stopzetten van het transport van de gegevens wordt proces-verbaal opgemaakt, dat aan de officier van justitie wordt gezonden. Op basis van de logging kan worden gecontroleerd of de ontvangst van gegevens op de technische infrastructuur daadwerkelijk is beëindigd.

Indien de niet of niet volledige verwijdering van een technisch hulpmiddel risico's oplevert voor het onderzochte geautomatiseerde werk stelt het technisch team de officier van justitie hiervan in kennis en stelt het informatie beschikbaar ten behoeve van de volledige verwijdering. De officier van justitie stelt de beheerder van het geautomatiseerde werk daarvan in kennis.

De Inspectie VenJ houdt toezicht op de naleving op de juiste uitvoering van de verwijderingsprocedure.

Hoofdstuk 10 Wijziging overige wet- en regelgeving

Artikel 30 Wijziging Besluit politiegegevens

Artikel 30 strekt tot wijziging van artikel 4:3, eerste lid, van het Besluit politiegegevens. In de Wpg is geregeld dat de politie persoonsgegevens aan derden kan verstrekken met het oog op een zwaarwegend algemeen belang (artikel 18, eerste lid, Wpg). De personen en instanties aan wie, evenals de taak ten behoeve waarvan de politiegegevens worden verstrekt, worden aangewezen bij of krachtens algemene maatregel van bestuur. Dit is uitgewerkt in het Besluit politiegegevens. Om de verhouding tussen de taakuitoefening door de Inspectie VenJ en het verstrekkingenregime van de Wpg te verhelderen wordt artikel 4:3 van het Besluit politiegegevens aangepast en wordt de verplichting tot verstrekking van politiegegevens die worden verwerkt op grond van de artikelen 8, 9, 10 en 13 van de Wpg, ten behoeve van de toezichthoudende taak van de Inspectie VenJ expliciet vastgelegd.

De toezichthoudende taak van de Inspectie VenJ betreft het toezicht op de taakuitvoering door de politie (artikel 57, eerste lid, onderdeel d, Wet veiligheidsregio's) alsmede het onderzoek in een geautomatiseerd werk dat wordt gedaan door de opsporingsambtenaren van de bijzondere opsporingsdiensten en de buitengewone opsporingsambtenaren (artikel 126nba, zevende lid, Sv). De verplichting om gegevens te verstrekken met het oog op de uitvoering van de taken van de Inspectie VenJ omvat de politiegegevens die worden verwerkt ten behoeve van een onderzoek met het oog op de handhaving van de rechtsorde in een bepaald geval en de gegevens die worden verwerkt met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde (artikelen 9, eerste lid, en 10, eerste lid, onderdelen a en

c, Wpg). Het gaat hier om zachte gegevens, die binnen de politie worden verwerkt door onder meer de criminele inlichtingeneenheden en de regionale inlichtingendiensten.

Hoofdstuk 11 Inwerkingtreding

Artikelen 31 en 32 Citeertitel en inwerkingtreding

Dit besluit heeft als citeertitel "Besluit onderzoek in een geautomatiseerd werk" en treedt tegelijk in werking met het wetsvoorstel computercriminaliteit III. De datum van inwerkingtreding wordt bepaald op **PM**.

De Staatssecretaris van Veiligheid en Justitie,