Staatsblad
van het Koninkrijk der Nederlanden

Jaargang 2018

340

Besluit van 28 september 2018, houdende regels over de uitoefening van de bevoegdheid tot het binnendringen in een geautomatiseerd werk en het al dan niet met een technisch hulpmiddel onderzoek doen als bedoeld in de artikelen 126nba, eerste lid, 126uba, eerste lid, en 126zpa, eerste lid van het Wetboek van Strafvordering (Besluit onderzoek in een geautomatiseerd werk)

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

Op de voordracht van de Minister van Justitie en Veiligheid van 30 mei 2018, directie Wetgeving en Juridische Zaken, nr. 2280615;

Gelet op de artikelen 126nba, eerste en achtste lid, 126uba, eerste en derde lid, 126zpa, 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 van 26 juli 2018, nr. W16.18.0125/II);

Gezien het nader rapport van de Minister van Justitie en Veiligheid van 24 september 2018, directie Wetgeving en Juridische Zaken, nr. 2363828;

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;

c. *Landelijke eenheid:* Landelijke eenheid als bedoeld in artikel 3, eerste lid, van het Besluit beheer politie;

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 Justitie en Veiligheid;

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

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

h. *technisch team:* onderdeel van de Landelijke eenheid dat kan worden belast met de uitvoering van een bevel.

HOOFDSTUK 2 UITVOERING VAN EEN BEVEL 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 2°, 161sexies, aanhef en onder 1°, 177, eerste en tweede lid, 179, 182, eerste en tweede lid, onder 1°, 197a, eerste en tweede 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 OPSPORINGSAMBTE-NAREN

Artikel 3 Aanwijzing opsporingsambtenaren en 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 zijn werkgever worden aangewezen voor het binnendringen in een geautomatiseerd werk en het, al dan niet met een technisch hulpmiddel, verrichten van onderzoekshandelingen als bedoeld in de artikelen 126nba, eerste lid, 126uba, eerste lid, en 126zpa, eerste lid, van het Wetboek van Strafvordering.

2. Een op grond van het eerste lid aangewezen opsporingsambtenaar kan uitsluitend met de uitvoering van de in het eerste lid bedoelde bevoegdheid worden belast als hij lid is van een technisch team.

3. Een op grond van het eerste lid aangewezen opsporingsambtenaar kan door de korpschef worden aangewezen als lid van een technisch team indien hij heeft voldaan aan door Onze Minister aangewezen kwalificaties.

Artikel 4 Incidentele samenwerking

1. In afwijking van artikel 3, tweede lid, kan een op grond van artikel 3, eerste lid, aangewezen opsporingsambtenaar worden belast met de uitvoering van een bevel in een concrete zaak als hij deelnemer is aan een technisch team.

2. Een op grond van artikel 3, eerste lid, aangewezen opsporingsambtenaar kan door de korpschef worden aangewezen als deelnemer aan een technisch team voor de duur van de uitvoering van het bevel in een concrete zaak, indien hij naar het oordeel van de korpschef beschikt over specifieke kennis en vaardigheden, benodigd voor de uitvoering van dat bevel.

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

HOOFDSTUK 4 VASTLEGGING VAN GEGEVENS OVER DE UITVOERING VAN EEN BEVEL IN LOGBESTANDEN

Artikel 5 Logbestanden

1. Gedurende de uitvoering van een bevel worden doorlopend en automatisch gegevens in logbestanden vastgelegd over:

a. de handelingen die worden verricht ter uitvoering van een bevel;

b. de toegang tot een technisch hulpmiddel;

c. de gegevens die al dan niet met een technisch hulpmiddel op de technische infrastructuur worden vastgelegd ter uitvoering van een bevel:

d. het functioneren van de technische infrastructuur.

2. Indien de gegevens over de handelingen bedoeld in het eerste lid, onder a, naar hun aard niet automatisch kunnen worden vastgelegd legt een opsporingsambtenaar van een technisch team de handelingen handmatig vast.

Artikel 6 Vaststelling van onregelmatigheden

1. De in artikel 5 bedoelde vastlegging van gegevens in logbestanden 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 een onregelmatigheid heeft plaatsgevonden die van invloed is op de betrouwbaarheid en integriteit van de ter uitvoering van het bevel vastgelegde gegevens op een technische infrastructuur.

2. Indien een onregelmatigheid 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 logbestanden

1. De inhoud van de logbestanden wordt niet gewijzigd.

2. De logbestanden zijn uitsluitend toegankelijk voor door de korpschef aangewezen ambtenaren.

3. Bij de vastlegging van gegevens in logbestanden worden maatregelen getroffen om wijziging van de logbestanden of kennisneming hiervan door onbevoegden te voorkomen en achteraf te kunnen vaststellen of wijziging of kennisneming heeft plaatsgevonden.

HOOFDSTUK 5 TECHNISCHE EISEN AAN EEN TECHNISCH HULPMIDDEL VOOR HET VERRICHTEN VAN ONDERZOEKSHANDELINGEN

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 identificerende kenmerken van het geautomatiseerde werk 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, tegen wijziging van de geregistreerde gegevens en tegen 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 beveiligt de geregistreerde gegevens tijdens het transport naar een technische infrastructuur tegen wijziging van de geregistreerde gegevens en kennisneming van de geregistreerde gegevens door onbevoegden.

HOOFDSTUK 6 KEURING VAN EEN TECHNISCH HULPMIDDEL VOOR HET VERRICHTEN VAN ONDERZOEKSHANDELINGEN

Artikel 14 Voorafgaande keuring en herkeuring

1. Een technisch hulpmiddel wordt voorafgaand aan het gebruik ervan gekeurd 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 gestelde eisen, vindt voorafgaand aan het gebruik herkeuring plaats door een keuringsdienst van het gewijzigde technische hulpmiddel of van het gewijzigde onderdeel.

Artikel 15 Uitzonderingen op voorafgaande keuring en herkeuring

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

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 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 onderzoekingen die een beschermingsniveau bieden dat ten minste gelijkwaardig is aan het niveau dat met de nationale onderzoekingen wordt nagestreefd.

HOOFDSTUK 7 HET VERRICHTEN VAN ONDERZOEKSHANDELINGEN IN EEN GEAUTOMATISEERD WERK

Artikel 21 Uitvoering van een bevel

1. Indien de officier van justitie beveelt dat het verrichten van onderzoekshandelingen in een geautomatiseerd werk plaatsvindt met een technisch hulpmiddel wordt ter uitvoering van het bevel gebruik gemaakt van een goedgekeurd technisch hulpmiddel.
2. In afwijking van het eerste lid kan de officier van justitie bepalen dat, indien het onderzoeksbelang dit dringend vordert, een niet gekeurd technisch hulpmiddel wordt gebruikt. In dat geval vermeldt de officier van justitie in het bevel dat toepassing is gegeven aan artikel 21, tweede lid.
3. Indien ter uitvoering van een bevel gebruik wordt gemaakt van een niet gekeurd technisch hulpmiddel vermeldt de officier van justitie de uitkomst van de keuring of herkeuring na afloop van het gebruik in de processtukken.
4. In afwijking van het derde lid kan keuring of herkeuring na afloop van het gebruik achterwege blijven, indien de aard van het technische hulpmiddel zich naar het oordeel van de officier van justitie daartegen verzet. In dat geval vermeldt de officier van justitie in de processtukken dat toepassing is gegeven aan artikel 21, vierde lid, en vermeldt hij welke aanvullende waarborgen zijn getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de met het technisch hulpmiddel vastgelegde gegevens te garanderen.
5. Indien de officier van justitie beveelt dat het verrichten van onderzoekshandelingen in een geautomatiseerd werk plaatsvindt zonder een technisch hulpmiddel worden ter uitvoering van het bevel de onderzoekshandelingen verricht die zijn omschreven in het bevel en worden procedurele waarborgen getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de tijdens het onderzoek vast te leggen gegevens te garanderen.

Artikel 22 Toegang tot een technisch hulpmiddel

1. De korpschef wijst één of meer ambtenaren aan die zijn belast met de centrale registratie van de toegang tot 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;

e. een aanduiding van de opsporingsambtenaar van een technisch team die om toegang verzoekt.

Artikel 23 Plaatsing van een technisch hulpmiddel

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.

4. Indien bij de plaatsing van een technisch hulpmiddel een onregelmatigheid plaatsvindt, maakt de opsporingsambtenaar hiervan melding in het proces-verbaal.

Artikel 24 Onderzoekshandelingen verrichten

1. Het verrichten van onderzoekshandelingen in een geautomatiseerd werk vindt plaats door een opsporingsambtenaar van een technisch team.

2. De opsporingsambtenaar maakt proces-verbaal op van het verrichten van onderzoekshandelingen, dat aan de officier van justitie wordt gezonden.

3. Indien bij het verrichten van onderzoekshandelingen een onregelmatigheid plaatsvindt, maakt de opsporingsambtenaar hiervan melding in het proces-verbaal.

Artikel 25 Verwijdering van een technisch hulpmiddel

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 26 Niet of niet volledige verwijdering van een technisch hulpmiddel

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.

Artikel 27 Vastlegging van gegevens op een technische infrastructuur

1. De vastlegging van de tijdens het onderzoek al dan niet door een technisch hulpmiddel geregistreerde gegevens vindt plaats op een technische infrastructuur.

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

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

Artikel 28 Betrouwbaarheid en integriteit van een technische infrastructuur

1. De inhoud van de op een technische infrastructuur vastgelegde gegevens wordt niet gewijzigd.

2. De vastgelegde gegevens zijn uitsluitend toegankelijk voor door de korpschef aangewezen ambtenaren.

3. Bij de vastlegging van gegevens worden maatregelen getroffen om wijziging van de vastgelegde gegevens of kennisneming van de vastgelegde gegevens hiervan door onbevoegden te voorkomen en achteraf te kunnen vaststellen of wijziging of kennisneming hiervan heeft plaatsgevonden.

HOOFDSTUK 8 VERSTREKKING VAN TER UITVOERING VAN EEN BEVEL VASTGELEGDE GEGEVENS

Artikel 29 Verstrekking en bewerking van vastgelegde gegevens

1. De ter uitvoering van een bevel op een technische infrastructuur vastgelegde gegevens, bedoeld in artikel 27, worden verstrekt aan een opsporingsambtenaar die is belast met het opsporingsonderzoek.

2. Indien het ter uitvoering van het bevel of ten behoeve van het opsporingsonderzoek nodig is om een selectie te maken uit op een technische infrastructuur vastgelegde gegevens, voert een opsporingsambtenaar van een technisch team een bewerking uit met gebruikmaking van een kopie van de op grond van artikel 27 vastgelegde gegevens. De bewerkte gegevens worden verstrekt aan een opsporingsambtenaar die is belast met het opsporingsonderzoek.

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

HOOFDSTUK 9 WIJZIGING OVERIGE WET- EN REGELGEVING

Artikel 30 Wijziging Besluit politiegegevens

Het Besluit politiegegevens wordt als volgt gewijzigd:

1. Artikel 4:2, eerste lid, onderdeel o, vervalt.

2. Aan artikel 4:3, eerste lid, onderdeel a, 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 10 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.

Het advies van de Afdeling advisering van de Raad van State wordt met de daarbij behorende stukken openbaar gemaakt door publicatie in de Staatscourant.

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

Wassenaar, 28 september 2018

Willem-Alexander

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus

Uitgegeven de *negende* oktober 2018

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus

stb-2018-340
ISSN 0920 - 2064
's-Gravenhage 2018

NOTA VAN TOELICHTING

I. Algemeen

1. Inleiding

De Wet computercriminaliteit III[1] (hierna: de wet) versterkt het juridische instrumentarium voor de opsporing en vervolging van computercriminaliteit. De wet 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). Aan de officier van justitie wordt de bevoegdheid toegekend 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 verrichten van onderzoekshandelingen is noodzakelijk geworden door de voortschrijdende techniek en het wijdverbreide gebruik van geautomatiseerde werken voor communicatie en de verwerking en opslag van gegevens.

De wet 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 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 verrichten van onderzoekshandelingen met een technisch hulpmiddel (artikel 126ee Sv). Het onderhavige besluit geeft uitvoering aan deze bepalingen.

Ter uitvoering van het regeerakkoord 2017–2021 vindt twee jaren na inwerkingtreding evaluatie van de wet plaats. Bij deze wetsevaluatie wordt het onderhavige besluit betrokken.

---

[1] Wet van 27 juni 2018 tot wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III) (Stb. 322).

Naast voornoemde delegatiegrondslagen biedt de wet een facultatieve grondslag om bij algemene maatregel van bestuur nadere regels te stellen over de toepassing van de bevoegdheid 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, maar wordt gedacht aan uitwerking van het opsporingsbeleid in een Aanwijzing van het College van procureurs-generaal op grond van artikel 130, zesde lid, van de Wet op de rechtelijke organisatie.

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

Op grond van de wet mag de bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk en doen van onderzoek worden ingezet in geval van verdenking van een misdrijf waarvoor voorlopige hechtenis is toegelaten, dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert en indien het onderzoeksbelang dit dringend vordert (artikelen 126nba/uba, eerste lid). De bevoegdheid wordt binnen de kring van de misdrijven waarvoor voorlopige hechtenis mogelijk is nader ingekaderd, afhankelijk van de aard van de te verrichten onderzoekshandelingen. Voor de inzet van de bevoegdheid met het oog op het vastleggen van gegevens of het ontoegankelijkmaken van gegevens (artikelen 126nba/uba, eerste lid, onder d en e) geldt gelet op de mate van inbreuk die hiermee wordt gemaakt op de persoonlijke levenssfeer een zwaarder verdenkingscriterium. De inzet hiervan kan uitsluitend plaatsvinden bij een verdenking van een misdrijf waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaren of meer is gesteld of dat bij . algemene maatregel van bestuur is aangewezen en dat dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert. In hoofdstuk 2 van dit besluit worden de misdrijven met een lager wettelijk strafmaximum dan acht jaren gevangenisstraf waarvoor de bevoegdheid mag worden ingezet 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 in beginsel een duidelijk maatschappelijk belang is bij de beëindiging van de strafbare situatie en de vervolging van de daders. Bij een licht delictscenario kan de afweging in een concrete zaak ertoe leiden dat wordt afgezien van de inzet van de bevoegdheid. De toenemende digitalisering van de maatschappij en de ontwikkelingen in de cyberomgeving drukken een groot stempel op de aard van vele criminaliteitsvormen en leiden tot nieuwe veiligheidsrisico's.[2] Het aantal gevallen van computercriminaliteit groeit.[3] De vrijwel onbeperkte schaalbaarheid van aanvallen zorgt ervoor dat het voor criminelen interessant is zich toe te leggen op computercriminaliteit,

---

[2] In het Jaarbericht 2016 van het OM (https://www.om.nl/actueel/@98932/jaarbericht-2016/, p. 5) worden veelvoorkomende delicten als phishing en internetoplichting, genoemd, maar ook reële cyberdreigingen die zijn gericht op de ondermijning van politiek en bestuur en het saboteren van maatschappelijk vitale diensten, systemen en processen.

[3] Cybersecuritybeeld Nederland 2017 van het Nationaal Cyber Security Centrum (NCSC) (https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-2017.html, p. 7)

waarbij ICT niet alleen het middel, maar ook het doelwit is. Beroepscriminelen richten zich in steeds grotere mate op grote bedrijven, met als doel financieel gewin. 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 leiden tot ernstige economische schade en tot ontwrichting en vernietiging van vitale infrastructuren, zoals energiecentrales, vervoersnetwerken en overheidsnetwerken.

Spionage vindt toenemende mate plaats met digitale middelen. Statelijke actoren intensiveren hun activiteiten en hebben zich de afgelopen tijd ook gericht op digitale beïnvloeding van democratische processen voor geopolitiek gewin.[4]

Ook op andere criminaliteitsterreinen maken (beroeps)criminelen steeds vaker gebruik van digitale technieken.[5] Digitale technologie kan een rol spelen in elk stadium van strafbaar handelen, zowel bij de voorbereiding, de uitvoering als de afronding van misdrijven. Zo kunnen sociale media dienen als ontmoetingsplaats, het darkweb als handelsplaats en kan financiering plaatsvinden met behulp van bitcoins. Steeds betere encryptietechnieken zorgen voor een toenemende afscherming van illegale handelingen en activiteiten. Geavanceerde digitale technieken zijn in toenemende mate voor iedereen toegankelijk en te gebruiken zonder veel voorkennis. Daarnaast ontwikkelen deze technieken zich snel, waardoor de modus operandus van criminelen snel kan veranderen. 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. Zedendelinquenten verplaatsen hun activiteiten naar het digitale domein en benaderen online jonge kinderen voor seksuele doeleinden. 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.

Door het gebruik van digitale technieken worden deze misdrijven aan het zicht onttrokken, waardoor de maatschappelijke veiligheid vermindert. Via de toepassing van de binnendring- en onderzoekbevoegdheid kan rechtstreeks toegang worden verkregen tot de gegevens op het geautomatiseerde werk, kan heimelijk en op afstand digitaal bewijs van strafbare feiten worden veiliggesteld en kunnen criminele activiteiten worden stopgezet. Hiermee wordt bijgedragen aan een effectieve aanpak van criminaliteit 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 criminaliteit.

---

[4] Idem.

[5] In het Nationaal dreigingsbeeld georganiseerde criminaliteit 2017 van de Nationale Politie https://www.politie.nl/nieuws/2017/juni/1/11-digitale-ontwikkelingen-wijzigen-crimineel-landschap.html, p. 237 e.v.) wordt gewezen op de steeds sterkere verweving tussen computercriminaliteit en gedigitaliseerde criminaliteit en traditionele vormen van criminaliteit.

3. Het onderzoek in een geautomatiseerd werk

3.1. Algemeen

Het onderzoek in een geautomatiseerd werk bestaat uit verschillende fasen. De eerste fase betreft het op afstand heimelijk binnendringen in het geautomatiseerde werk. Als deze fase wordt bedoeld wordt dit omschreven als: het binnendringen in een geautomatiseerd werk. De tweede fase betreft het – al dan niet met een technisch hulpmiddel – verrichten van bepaalde onderzoekshandelingen in het geautomatiseerde werk waarin is binnengedrongen waarmee gegevens kunnen worden vastgelegd die kunnen dienen als bewijs in een strafzaak. Als deze fase wordt bedoeld dan wordt dit omschreven als: het verrichten van onderzoekshandelingen. Het op afstand heimelijk binnendringen in een geautomatiseerd werk en het verrichten van bepaalde onderzoekshandelingen tezamen wordt in het vervolg van deze nota van toelichting aangeduid als: (het uitvoeren van) onderzoek in een geautomatiseerd werk.

In de hoofdstukken 3 tot en met 8 van het onderhavige besluit worden ter uitvoering van de wet nadere regels gesteld over het onderzoek in een geautomatiseerd werk. Het betreft ten eerste regels over de deskundigheid en autorisatie van de opsporingsambtenaren die onderzoek doen in een geautomatiseerd werk en de samenwerking met andere opsporingsambtenaren (hoofdstuk 3). Het betreft ten tweede regels over de vastlegging van gegevens ter uitvoering van een bevel (hoofdstuk 4). Vervolgens worden regels gesteld over de technische eisen aan en keuring van een technisch hulpmiddel voor het verrichten van onderzoekshandelingen (hoofdstukken 5 en 6). Ten slotte worden regels gesteld over het verrichten van onderzoekshandelingen in een geautomatiseerd werk en de verstrekking van tijdens het onderzoek verkregen gegevens (hoofdstukken 7 en 8).

De bestrijding van computercriminaliteit vraagt, in het licht van de snelle en voortdurende technologische ontwikkelingen, om enige flexibiliteit en abstractie van technische details. De regels in de hoofdstukken 3 tot en met 8 van dit besluit hebben gelet hierop een kaderstellend karakter. Er worden eisen gesteld aan de organisatie, inrichting en controleerbaarheid van het onderzoekproces. De uitwerking hiervan vindt plaats in de opsporingspraktijk (via handreikingen, mandaatbesluiten, keuringsprotocollen etc.).

3.2. Deskundigheid van opsporingsambtenaren

In hoofdstuk 3 van dit besluit worden regels gesteld over de opsporingsambtenaren die kunnen worden aangewezen voor het uitvoeren van 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 onderzoek in een geautomatiseerd werk, indien zij lid zijn van een technisch team.

De politie heeft behoefte aan de bevoegdheid met het oog op de uitvoering van de politietaak, 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 bijzondere opsporingsdiensten 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. Hieronder valt onder meer 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 categoraal zijn aangewezen door de Minister van Justitie en Veiligheid, worden belast met het uitvoeren van onderzoek in een geautomatiseerd werk. 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 Justitie en Veiligheid aangewezen kwalificaties, onder meer ten aanzien van kennis op het gebied van ICT. De opleidingseisen worden nader 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 uitvoeren van onderzoek in een geautomatiseerd werk wordt, in ieder geval gedurende de beginfase, de organisatie van de technische teams centraal belegd binnen de politieorganisatie. Binnen de Landelijke eenheid van de Nationale Politie worden één of meer technische teams ingericht die worden belast met het onderzoek in een geautomatiseerd werk. Deze teams voeren dit onderzoek uit ten behoeve van de politie, de Kmar en de bijzondere opsporingsdiensten.

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 doen van onderzoek in een geautomatiseerd werk, indien hij beschikt over specifieke kennis en vaardigheden die nodig zijn voor de uitvoering van een bevel in een concrete zaak. Dit staat ter beoordeling van de korpschef. Bij een positieve beoordeling wordt de opsporingsambtenaar op incidentele basis als deelnemer toegevoegd aan een technisch team voor de duur van het bevel en wordt hij gedurende de uitvoering van het bevel begeleid door een lid van een technisch team.

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 specifieke zaak wordt voorgesteld. Een projectplan kan afkomstig zijn van tactische rechercheteams 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 is betrokken 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 onderzoek in een geautomatiseerd werk.

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

Het onderzoek in een geautomatiseerd werk vindt plaats ter uitvoering van een bevel van de officier van justitie als bedoeld in de artikelen 126nba/uba/zpa Sv. Bij het binnendringen in een geautomatiseerd werk kan gebruik worden gemaakt van verschillende technieken. Daarbij is het gebruik van commerciële binnendringsoftware van derden waarvan niet duidelijk is of deze van bekende of onbekende kwetsbaarheden gebruik maakt beperkt tot het uiterste geval. Deze software kan alleen worden gebruikt wanneer minder ingrijpende middelen zoals het gebruik van inloggegevens, social engineering of bekende kwetsbaarheden niet toereikend zijn om heimelijk toegang te verkrijgen tot een geautomatiseerd werk. De regering wil de markt voor onbekende kwetsbaarheden niet bevorderen, dat zou negatieve gevolgen voor de veiligheid van het internet kunnen hebben. Het Regeerakkoord 2017–2021 beperkt bovendien het betreden van de markt voor commerciële binnendringsoftware die mogelijk gebruik maakt van onbekende kwetsbaarheden. In plaats daarvan wil de regering meer inzetten op de eigen ontwikkeling van methoden voor het binnendringen, daartoe zal de ontwikkeling van passende producten binnen de politie worden gestimuleerd. De beperking in het Regeerakkoord van het gebruik van software van derden zal leiden tot een grotere belasting van het technisch team van de Landelijke Eenheid dat met de uitvoering is belast en dat zelf passende methoden moet ontdekken en ontwikkelen, vooral in zaken waarin inzet zonder de aanschaf van software nodig is. Bij de toedeling van de financiële middelen voor de uitvoering van de bevoegdheid zal hiermee rekening worden gehouden. Niettemin is het gebruik van software die mogelijk gebruik maakt van onbekende kwetsbaarheden soms onvermijdelijk om ernstige criminaliteit te kunnen bestrijden. De aanschaf van dergelijke binnendringsoftware is in het Regeerakkoord 2017–2021 beperkt en zal slechts worden ingekocht in een specifieke zaak. De politie kan dan bijvoorbeeld een softwarepakket aanschaffen en/of op basis van de aanschaf van een licentie of gebruiksrecht enkel voor die zaak de software inzetten.

Als de officier van justitie bepaalt dat gebruik van binnendringsoftware van een externe leverancier noodzakelijk is, zal dit centraal in het OM worden getoetst alvorens in die specifieke zaak wordt overgaan tot aanschaf.

Verder geldt in voorkomende gevallen de procedure van artikel 126ffa Sv op grond waarvan de officier van justitie kan bevelen, na machtiging van de rechter-commissaris, dat de melding aan de producent van een onbekende kwetsbaarheid waarvan aannemelijk is dat die niet bekend is of niet kan worden verondersteld bekend te zijn bij de producent, kan worden uitgesteld.

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).

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.

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). Indien het verrichten van onderzoekshandelingen plaatsvindt zonder een technisch hulpmiddel worden de onderzoekshandelingen die worden verricht omschreven in het bevel.

Ter voorbereiding van het bevel stelt het technische team, 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, of en zo ja welke software van derden moet worden aangeschaft. 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. Bij de vordering tot machtiging worden de beoogde functionaliteiten van het technisch hulpmiddel en een overzicht van de werking van deze functionaliteiten aan de rechter-commissaris verstrekt. Het onderzoek in een geautomatiseerd werk kan worden uitgevoerd, zodra daartoe, na machtiging van de rechter-commissaris, een bevel is afgegeven door de officier van justitie. 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, na technische voorverkenningen en analyse daarvan, een plan van aanpak voor het binnendringen in het geautomatiseerd werk worden opgesteld. Het plan van aanpak wordt getest in een proefopstelling. Het daadwerkelijke binnendringen in het geautomatiseerde werk gaat volgens het vooraf geschreven plan van aanpak. Hierbij kunnen, zoals hiervoor is aangegeven, verschillende technieken worden gebruikt. Nadat het geautomatiseerde werk is binnengedrongen kunnen onderzoekshandelingen 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 worden verricht.

De gegevens die tijdens het verrichten van onderzoekshandelingen worden geregistreerd 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.

Na het onderzoek wordt het softwarepakket verwijderd of is de licentie verbruikt waardoor hergebruik niet meer mogelijk is. Wanneer in een toekomstige zaak het gebruik van binnendringsoftware van derden wederom is aangewezen, zal eerst de bruikbaarheid van de minder ingrijpende middelen worden beoordeeld en het daarvoor benodigde gehele toetsings- en beslissingsmodel doorlopen, voordat kan worden

overgegaan tot een (hernieuwde) aanschaf van een softwarepakket of van een nieuwe licentie.

De resultaten van het onderzoek worden door het technische team ter beschikking gesteld aan het tactische team. Indien het ter uitvoering van het bevel of ten behoeve van het opsporingsonderzoek nodig is om de gegevens te filteren, draagt het technische team zorg voor de selectie van onderzoeksgegevens, zodat binnen de categorieën van gegevens die in het bevel van de officier zijn opgenomen uitsluitend de gegevens die van belang zijn voor het opsporingsonderzoek ter beschikking komen van het tactische team. Bij de selectie van gegevens wordt gebruik gemaakt van een forensische kopie van de ter uitvoering van het bevel vastgelegde gegevens. Het technische team legt vast welke bewerkingen hebben plaatsgevonden met betrekking tot de op de forensische kopie vastgelegde gegevens.

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. De vastlegging van gegevens over de uitvoering van een bevel in logbestanden

Hoofdstuk 4 van dit besluit bevat regels over de vastlegging van gegevens over de uitvoering van een bevel. De digitale omgeving waarin het onderzoek in een geautomatiseerd werk plaatsvindt maakt het mogelijk om gedurende de inzet van de bevoegdheid 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 onregelmatigheid heeft plaatsgevonden die van invloed is op de betrouwbaarheid en integriteit van de ter uitvoering van het bevel geregistreerde en vastgelegde gegevens. Deze vorm van elektronische verslaglegging over de uitvoering van een bevel wordt ook wel aangeduid als «logging». Alle handelingen die tijdens het onderzoek in een geautomatiseerd werk plaatsvinden worden gelogd. Dit betreft zowel de handelingen die tijdens de voorbereidende fase, het binnendringen in een geautomatiseerd werk, worden verricht als ook de handelingen die gedurende de onderzoeksfase worden verricht. Ook het functioneren van de technische infrastructuur wordt gelogd.

Concreet kunnen vier niveaus van logging worden onderscheiden:

a) Inzetlogging: de logging die wordt uitgevoerd om de tijdens het onderzoek verrichte handelingen vast te leggen. Het betreft handelingen als het (automatisch) vastleggen van het beeldscherm en de toetsaanslagen van de opsporingsambtenaar van een technisch team, maar ook het vastleggen van de communicatie tussen de technische infrastructuur en het geautomatiseerde werk, het vastleggen van gebruikte scripts, softwareversies en het journaal van de opsporingsambtenaar. De inzetlogging zal zoveel mogelijk geautomatiseerd plaatsvinden. Voor zover dit technisch niet mogelijk is, wordt procedureel binnen de politieorganisatie vastgelegd dat handmatige logging plaatsvindt.

b) Bewijslogging: een subcategorie van de inzetlogging. Het betreft de vastlegging gedurende de onderzoeksfase van al dan niet door een technisch hulpmiddel geregistreerde gegevens, die kunnen dienen als bewijs in een strafzaak.

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

d) Authenticatie- en autorisatielogging: een subcategorie van systeemloggingen. Hiermee vindt controle op de toegang tot een technisch hulpmiddel plaats.

De logging is ten eerste en vooral bedoeld voor de interne controle van de tijdens de uitvoering van het bevel verrichte handelingen en het functioneren van de technische infrastructuur. Uitsluitend de bewijslogging kan, al dan niet in bewerkte vorm, aan het dossier in een strafzaak worden toegevoegd.

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 ter uitvoering van een bevel vergaarde gegevens, die kunnen dienen als bewijs in een strafzaak. Indien een onregelmatigheid plaatsvindt die van invloed is op de betrouwbaarheid en integriteit van de ter uitvoering van het bevel vastgelegde gegevens op een technische infrastructuur, dan maakt een opsporingsambtenaar van een technisch team hiervan proces-verbaal op, dat aan de officier van justitie wordt gezonden. De officier van justitie en de rechter beoordelen in hoeverre de geconstateerde onregelmatigheid afbreuk doet aan de bewijskracht van de gegevens. De Inspectie Justitie en Veiligheid (Inspectie JenV) kan in het kader van haar toezichthoudende taak met gebruikmaking van de logging onderzoek doen naar eventuele onregelmatigheden bij de uitvoering van het onderzoek in een geautomatiseerd werk.

3.5. Technische eisen aan en keuring van een technisch hulpmiddel voor het verrichten van onderzoekshandelingen

Het verrichten van onderzoekshandelingen 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 sofwareapplicatie 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 dienen als bewijs in een strafzaak. Gelet hierop is het essentieel dat gegevens die met een technisch hulpmiddel worden vergaard betrouwbaar, integer en herleidbaar zijn en dat het technische hulpmiddel zelf betrouwbaar en integer functioneert.

De wijze waarop het binnendringen plaatsvindt, bijvoorbeeld de wijze van het omzeilen van de beveiliging van een geautomatiseerd werk, maakt geen deel uit van het keuringsproces. In het geval binnendringsoftware wordt ingekocht wordt het functioneren hiervan in een testomgeving gecontroleerd.

In de hoofdstukken 5 en 6 van dit besluit worden regels gesteld over technische hulpmiddelen waarmee onderzoekshandelingen worden verricht in een geautomatiseerd werk. Deze regels hebben betrekking op de technische eisen waaraan technische hulpmiddelen moeten voldoen en de voorafgaande goedkeuring hiervan. 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 in hoofdstuk 5 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.

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. De integriteit van de met een technisch hulpmiddel verkregen gegevens, waarmee gedoeld 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. 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.

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 de wet wordt het mogelijk om deze bevoegdheden uit te oefenen nadat op afstand heimelijk 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 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.

Hoofdstuk 6 van het besluit bevat regels over de voorafgaande keuring van een technisch hulpmiddel. Voordat een technisch hulpmiddel wordt gebruikt ter uitvoering van een bevel, dient het goedgekeurd te zijn door een keuringsdienst. Bij de keuring wordt getoetst of het hulpmiddel voldoet aan de in hoofdstuk 5 gestelde technische eisen. Als bij het verrichten van onderzoekshandelingen gebruik wordt gemaakt van een goedgekeurd hulpmiddel mag er vanuit worden gegaan dat aan de wettelijke eisen omtrent de betrouwbaarheid, integriteit en herleidbaarheid van de gegevens is voldaan.

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 in het besluit 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 Justitie en Veiligheid.

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 sofwareapplicaties van verschillende producenten te betrekken of deze zelf binnen de politieorganisatie te (laten) ontwerpen, mits aan de wettelijke vereisten voor keuring wordt voldaan. Conform de afspraken in het Regeerakkoord 2017–2021 zal de politie binnendringsoftware van derden die mogelijk gebruik maakt van onbekende kwetsbaarheden alleen aanschaffen als daar in een specifieke zaak een noodzaak toe bestaat. In de praktijk kan het voorkomen dat er gebruik wordt gemaakt van één softwarepakket dat bestaat uit onderdelen voor het verrichten van onderzoekshandelingen (een technisch hulpmiddel) en onderdelen voor het binnendringen van een geautomatiseerd werk. Deze software kan met het oog op de keuring van het technische hulpmiddel worden aangeschaft voordat dit nodig is in een specifieke zaak. Dit is noodzakelijk omdat de keuring enige tijd in beslag kan nemen en na een besluit om dergelijke software te gebruiken om binnen te dringen, deze snel ingezet moet kunnen worden. Het gebruik van software op basis van een licentie biedt de mogelijkheid om een demonstratieversie van de software te keuren voordat de software in een specifieke zaak kan worden ingezet om binnen te dringen. Indien inzet om binnen te dringen aan de orde is, dient alsnog een aparte licentie daarvoor te worden aangeschaft. Het gebruik van commerciële binnendringsoftware van derden is een uiterste middel. De wijze waarop het binnendringen plaatsvindt, bijvoorbeeld de wijze van het omzeilen van de beveiliging van een geautomatiseerd werk, maakt geen deel uit van het keuringsproces. In het geval binnendringsoftware wordt ingekocht wordt het functioneren in een testomgeving gecontroleerd. Tevens wordt in de procedure rondom de inzet van de bevoegdheid aandacht besteed aan de risico's voor het te onderzoeken geautomatiseerd werk, waaronder schade aan derden.

De ervaring leert dat producenten van software veelvuldig gebruik maken van software updates ter verbetering van het product. Indien de werking van een technisch hulpmiddel of een onderdeel hiervan door een software update zodanig wijzigt dat niet meer wordt voldaan aan de technische eisen vindt herkeuring plaats van het technische hulpmiddel of van het gewijzigde onderdeel hiervan. De Inspectie JenV houdt toezicht op de naleving van de technische eisen en de keuringsprocedure.

3.6. Het verrichten van onderzoekshandelingen in een geautomatiseerd werk

Het besluit stelt in hoofdstuk 7 procedurele en organisatorische eisen aan onderzoekshandelingen die al dan niet met een technisch hulpmiddel in een geautomatiseerd werk worden verricht. Er worden regels gesteld over de uitvoering van het bevel, de toegang tot, de plaatsing, het gebruik en de verwijdering van technische hulpmiddelen. De gegevens die bij het verrichten van onderzoekshandelingen, al dan niet met een technisch hulpmiddel worden verkregen dienen automatisch worden te worden 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.

Ter uitvoering van een bevel van de officier van justitie wordt in beginsel steeds gebruik gemaakt van een vooraf goedgekeurd technisch hulpmiddel. Een uitzondering op deze hoofdregel is mogelijk als het onderzoeksbelang dringend vordert dat gebruik wordt gemaakt van een hulpmiddel dat zich naar zijn aard niet leent voor voorafgaande goedkeuring. Hierbij kan worden gedacht aan op maat gemaakte software, zoals een script dat is geschreven door een technisch team en dat «semi-handmatig» wordt ingezet. In dat geval vermeldt de officier van justitie in het bevel dat gebruik wordt gemaakt van een niet gekeurd hulpmiddel. Na afloop vindt alsnog keuring plaats, tenzij de aard van het hulpmiddel zich naar het oordeel van de officier hiertegen verzet. In dat geval vermeldt de officier van justitie in de processtukken dat is afgezien van keuring en vermeldt hij welke aanvullende waarborgen zijn getroffen om de betrouwbaarheid, integriteit en de herleidbaarheid van de vastgelegde gegevens te garanderen. Ook als onderzoekshandelingen zonder goedgekeurd hulpmiddel worden verricht, dienen de verkregen gegevens te worden vastgelegd op een technische infrastructuur. Tevens dienen alle handelingen die ter uitvoering van het bevel worden verricht te worden 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 in een geautomatiseerd werk kunnen worden ingezien of worden overgenomen ten behoeve van het vaststellen van de identiteit van het geautomatiseerde werk. De vraag of het gebruik van een technisch hulpmiddel noodzakelijk is, is onder meer afhankelijk van de aard van de inzet, de aard van het geautomatiseerde werk en de vraag of de gegevens zonder gebruik van een technisch hulpmiddel als rechtmatig bewijs kunnen worden aangemerkt. Indien de officier van justitie beveelt dat het onderzoek in een geautomatiseerd werk plaatsvindt zonder technisch hulpmiddel wordt het onderzoek uitgevoerd aan de hand van de in het bevel omschreven onderzoekshandelingen en worden procedurele waarborgen getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de tijdens het onderzoek vast te leggen gegevens te garanderen. De advisering van de officier van justitie hieromtrent vindt plaats door het technische team. De officier vermeldt in de processtukken welke procedurele waarborgen zijn getroffen om de betrouwbaarheid, integriteit en de herleidbaarheid van de vastgelegde gegevens te garanderen.

De Inspectie JenV houdt toezicht op de naleving van de regels omtrent het verrichten van onderzoekshandelingen in een geautomatiseerd werk.

3.7. Verstrekking van ter uitvoering van een bevel vastgelegde gegevens

De ter uitvoering van een bevel al dan niet met een technisch hulpmiddel op een technische infrastructuur vastgelegde gegevens kunnen door het technische team worden verstrekt aan het tactische team. 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. Indien het ten behoeve van de uitvoering van het bevel of ten behoeve van het opsporingsonderzoek nodig is om een selectie te maken uit de op een de technische infrastructuur vastgelegde gegevens, dan kan het technische team een bewerking uitvoeren met gebruikmaking van een forensische kopie van de gegevens. In dat geval legt het technische team vast welke bewerkingen hebben plaatsgevonden.

De verantwoording in een strafzaak vindt plaats via 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 opsporingsmethodieken en -middelen. Deze belangen kunnen een minder gedetailleerde verantwoording rechtvaardigen. Als bij het verrichten van onderzoekshandelingen in een geautomatiseerd werk gebruik wordt gemaakt van een goedgekeurd technisch hulpmiddel mag er vanuit worden gegaan dat aan de wettelijke eisen met betrekking tot betrouwbaarheid, integriteit en herleidbaar van de gegevens is voldaan. In dat geval kan in het proces-verbaal van de inzet worden volstaan met verwijzing naar het keuringsnummer, waardoor de samenstelling van het hulpmiddel ter bescherming van de opsporingsbelangen kan worden afgeschermd. Indien de onderzoekshandelingen zonder (goedgekeurd) technisch hulpmiddel zijn verricht, vermeldt de officier van justitie in de processtukken welke procedurele waarborgen zijn getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de vastgelegde gegevens te kunnen garanderen.

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

4. Gegevensverwerking

De gegevens die ter uitvoering van een bevel van de officier van justitie op een technische infrastructuur worden vastgelegd zijn persoonsgegevens die worden verwerkt in het kader van de uitoefening van de politietaak, als bedoeld in de artikelen 3 en 4, eerste lid, van de Wet politiegegevens (Wpg). De toepasselijkheid van de Wpg geldt voor zowel de ter uitvoering van een bevel vastgelegde gegevens, de door een technisch team bewerkte gegevens, de door een tactisch team verwerkte gegevens als de vastgelegde gegevens over de uitvoering van een bevel in logbestanden.

Op grond van de Wpg geldt een gedifferentieerd regime wat betreft de bewaartermijnen. Afhankelijk van het specifieke doel van de verwerking kan de bewaartermijn verschillen. Doorgaans zullen de gegevens worden verwerkt 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 (art. 14, eerste lid, Wpg).

Op grond van het Wetboek van Strafvordering geldt een speciale regeling voor de processen-verbaal en andere voorwerpen waaraan gegevens kunnen worden ontleend die zijn verkregen door observatie, 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). Deze regeling geldt als een «lex specialis» ten opzichte van de regeling van de Wpg. 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 over de uitvoering van een bevel, die worden vastgelegd in logbestanden, worden verwerkt met het oog op de opsporing van strafbare feiten en vallen, zoals hierboven reeds aangegeven, eveneens onder het regime 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 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.

Ten behoeve van de voorbereiding van de wet is een Privacy impact Assessment (PIA) v die als bijlage bij voornoemde memorie van toelichting is gevoegd (bijlage bij Kamerstukken II 2015/16, 34 372, nr. 3).

In het advies van de Autoriteit Persoonsgegevens over het besluit is opgemerkt dat implementatie van de Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad inhoudelijk geen invloed heeft op dit besluit.

5. Toezicht

De Inspectie JenV houdt toezicht op het functioneren van het wettelijke systeem rond de uitvoering van een bevel tot onderzoek in een geautomatiseerd werk. De Inspectie JenV 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. De Inspectie JenV heeft een onafhankelijke positie binnen de departementale structuur. 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 tot de uitvoering van een bevel 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 JenV 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 JenV 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 logging over de uitvoering van een bevel speelt een belangrijke rol bij het toezicht. Daarnaast kan ook steekproefsgewijs toezicht plaatsvinden tijdens het binnendringen in een geautomatiseerd werk en het doen van onderzoek in de praktijk. De Inspectie JenV 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 Justitie en Veiligheid aangeboden en door de Minister openbaar gemaakt.

Om de verhouding tussen taakuitoefening door de Inspectie JenV 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 JenV expliciet wettelijk vastgelegd.

6. Rechtsbescherming

Het Wetboek van Strafvordering kent geen specifieke regeling voor vergoeding van strafvorderlijke schade als gevolg van toepassing van bijzondere opsporingsbevoegdheden, zoals de bevoegdheid tot onderzoek in een geautomatiseerd werk. In voorkomende gevallen kunnen benadeelden zich wenden tot politie en het openbaar ministerie. Een verzoek om schade wordt vaak afgehandeld door deze instanties zelf, op basis van het civiele recht. In bepaalde gevallen kan een minnelijke schikking worden getroffen. Ook kan uit coulance een vergoeding worden toegekend. Komt het niet tot een vergelijk tussen de benadeelde en de betrokken instantie, dan kan een civielrechtelijke procedure worden gestart.

Een gewezen verdachte die schade heeft geleden door strafvorderlijk overheidsoptreden kan zich ook (rauwelijks) tot de civiele rechter wenden met een vordering op basis van een onrechtmatige overheidsdaad (artikel 6:162 BW). De civiele rechter ziet echter in beginsel geen grondslag voor de vergoeding van de strafvorderlijke schade indien de betrokkene onherroepelijk is veroordeeld. In dat geval ziet de rechter onvoldoende aanleiding om het strafvorderlijk optreden als een onrechtmatige daad in civielrechtelijke zin te beoordelen. Er bestaat wel een mogelijkheid tot schadevergoeding in verband met strafrechtelijk optreden jegens de gewezen verdachte dat vanaf het begin als onrechtmatig moet worden beoordeeld of als dit optreden achteraf als onrechtmatig moet worden bestempeld. Het eerste is aan de orde als er geen sprake was van een redelijk vermoeden van schuld of bij strijd met de maatschappelijke zorgvuldigheid, bijvoorbeeld bij schending van de beginselen van proportionaliteit en subsidiariteit, of fundamentele vereisten. Dit oordeel laat een eventuele veroordeling terzake van het strafbare feit onverlet. Het laatste is aan de orde als de strafzaak niet met een bewezenverklaring eindigt en uit de uitspraak van de strafrechter of anderszins uit de stukken

blijkt van het ongefundeerd zijn van de verdenking waarop het optreden berustte.

Wanneer een onschuldige derde schade heeft geleden vanwege het strafvorderlijk optreden, ook als dit rechtmatig heeft plaatsgevonden, dan kan de derde aanspraak maken op schadevergoeding. In de jurisprudentie van de Hoge Raad is aanvaard dat gevolgen van overheidshandelen die buiten het normale maatschappelijke risico of het normale bedrijfsrisico vallen en op een beperkte groep burgers drukken, gelijkelijk over de gemeenschap dienen te worden verdeeld. Uit deze regel vloeit voort dat het toebrengen van zodanige onevenredige schade bij een op zichzelf rechtmatige overheidshandeling jegens de betrokkene onrechtmatig is (ECLI:NL:HR:2001, AB 0801, NJ 2003,615).

7. 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 onderzoek in een geautomatiseerd werk wordt gedaan 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 7 juni 2018 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»)). De notificatie heeft niet geleid tot opmerkingen van de Europese Commissie en van andere lidstaten.

8. 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 (NP). De NP 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.

Het College van procureurs-generaal (College van PG's) heeft geen advies uitgebracht over de werklastgevolgen. Voor zover het besluit leidt tot werklastgevolgen bij het openbaar ministerie, worden de kosten gedekt binnen het reguliere budget.

De Raad voor de rechtspraak (RvdR) heeft in zijn advies over het ontwerp-besluit opgemerkt dat het besluit mogelijk gevolgen heeft voor de werklast, maar dat er op dit moment geen aanknopingspunten worden gezien om hiervan een adequate inschatting te maken. Voor zover het besluit leidt tot werklastgevolgen bij de rechtspraak worden de kosten gedekt binnen het reguliere budget. Indien zou blijken dat er sprake is van een grotere werklastverzwaring, kan deze worden meegenomen in de driejaarlijkse onderhandelingen tussen de RvdR en het ministerie van Justitie en Veiligheid.

De Inspectie JenV heeft in het advies over het ontwerp-besluit opgemerkt dat structurele financiering ten behoeve van extra capaciteit nodig is en dat pas als definitieve uitwerking (handreikingen etc.) in de opsporingspraktijk heeft plaatsgevonden een concrete inschatting kan worden gemaakt van de gevolgen voor het toezicht.

De beperking in het Regeerakkoord 2017–2021 van het gebruik van software van derden zal leiden tot een grotere belasting van het technisch team van de Landelijke Eenheid dat met de uitvoering is belast en dat zelf passende hulpmiddelen moet ontdekken en ontwikkelen, vooral in zaken waarin inzet zonder de aanschaf van software nodig is. Bij de toedeling van de financiële middelen voor de uitvoering van het wetsvoorstel CCIII wordt hiermee rekening gehouden. In het regeerakkoord is opgenomen dat vanaf 2019 jaarlijks additioneel € 10 miljoen is voorzien voor de uitvoering van de wet. Dit bedrag zal onder andere worden besteed aan capaciteit, opleiding en ICT bij de Landelijke Eenheid. Daarnaast wordt aanvullend geïnvesteerd in de toezichtstaak van de Inspectie JenV, capaciteit voor leiding en toezicht op de opsporingsonderzoeken bij het OM, in de rechterlijke macht en de Kmar.

9. Adviezen

9.1. Algemeen

Een ontwerp van het besluit is ter consultatie voorgelegd aan de volgende organisaties: het College van PG's, de NP, de Autoriteit persoonsgegevens (AP) (op grond van artikel 35, tweede lid, Wet politiegegevens juncto 51, tweede lid van de Wet bescherming persoonsgegevens), de Nederlandse Orde van Advocaten (NOvA), de RvdR (op grond van artikel 95 van de Wet op de rechterlijke organisatie), de Nederlandse Vereniging voor rechtspraak (NVvR), het Platform Bijzondere Opsporingsdiensten (Platform BOD) en de Inspectie JenV. Met uitzondering van het College van PG's, dat te kennen heeft gegeven zich aan te sluiten bij het advies van de NP, en het ministerie van Defensie hebben alle geconsulteerde instanties een advies uitgebracht. Tevens heeft internetconsultatie plaatsgevonden over het besluit. Naar aanleiding hiervan zijn acht reacties ontvangen, waaronder vijf reacties van particulieren en drie reacties van organisaties (van KPN, T-Mobile en Bits of Freedom (BoF)). Hieronder worden de hoofdlijnen uit de ontvangen adviezen besproken. Op de overige onderwerpen wordt op de daartoe geëigende plaatsen in (het artikelsgewijze deel van) deze nota van toelichting ingegaan.

Een ontwerp van het besluit is tevens aangeboden aan beide Kamers der Staten-Generaal. Naar aanleiding hiervan heeft een schriftelijk overleg plaatsgevonden in de Tweede Kamer (Kamerstukken II 2017/18, 34 372, nr. 27). De Eerste Kamer heeft het ontwerpbesluit betrokken bij het nader voorlopig verslag over de wet. De vragen van de Eerste Kamer zijn beantwoord in de nadere memorie van antwoord (Kamerstukken I 2017/18, 34 372, nr. G).

9.2. De toepassing van de bevoegdheid met het oog op het vastleggen van gegevens of het ontoegankelijkmaken van gegevens

In de adviezen van het Platform BOD, de RvdR en de NOvA zijn opmerkingen gemaakt over de reikwijdte van de toepassing van de bevoegdheid met het oog op het vastleggen van gegevens of het ontoegankelijk maken van gegevens en de in dat kader in artikel 2 van het besluit aangewezen misdrijven. Het Platform BOD pleit voor een verruiming van de lijst van misdrijven met categorieën misdrijven dan wel met specifieke delicten, waaronder ook enkele strafbepalingen uit bijzondere wetten. De RvdR wijst erop dat geen strafbepalingen uit bijzondere wetten zijn opgenomen in artikel 2 van het besluit. De NOvA acht de aanwijzing van misdrijven waarvoor de bevoegdheid kan worden toegepast in het besluit onwenselijk. Volgens de NOvA wordt de door de wetgever gegeven garantie dat de toepassing van de bevoegdheid beperkt zal blijven tot ernstige delicten waarbij het gebruik van een geautomatiseerd werk instrumenteel is door het besluit teniet gedaan. In het bijzonder wijst de NOvA erop dat de aanwijzing van het misdrijf «witwassen» surveillance van ieder persoon met niet onmiddellijk verklaarbaar bezit toelaat, hetgeen opsporingsinstanties in staat stelt om als «bijvangst» het leven van een persoon in wie interesse bestaat in kaart te brengen. Ook vreest de NOvA voor een snel uitdijende lijst van delicten.

De ontvangen adviezen hebben niet geleid tot aanpassing van de aanwijzing van misdrijven in artikel 2. Voor zover in het advies van de NOvA beperking van de toepassing van de bevoegdheid wordt bepleit tot bij wet aangewezen misdrijven wordt opgemerkt dat dit in het licht van het huidige criminaliteitsbeeld te beperkend zou zijn voor de opsporingspraktijk. Het wettelijk vereiste van een «dringend onderzoeksbelang» brengt mee dat de inzet van de bevoegdheid in een concreet geval dient te voldoen aan de vereisten van proportionaliteit en subsidiariteit. Dit vormt tevens onderdeel van de voorafgaande toetsing door de rechter-commissaris. De afweging bij de lichtere delictscenario's van voornoemde strafbaarstellingen, waaronder witwassen, die noodzakelijkerwijs algemeen zijn geformuleerd, kan ertoe leiden dat wordt afgezien van de toepassing van de bevoegdheid.

In reactie op het advies van het Platform BOD waarin is verzocht om uitbreiding van de toepassing van de bevoegdheid tot diverse (al dan niet commune) delicten wordt opgemerkt dat hiervoor geen aanleiding wordt gezien in het licht van het verwachtingspatroon met betrekking tot de inzet van de bevoegdheid gedurende de eerste jaren na de inwerkingtreding van de wet. De reikwijdte van de bevoegdheid zal deel uitmaken van de wetsevaluatie, die voorzien is binnen twee jaren na inwerkingtreding van de wet. Alsdan zal worden bezien in hoeverre de aanwijzing van misdrijven waarvoor de bevoegdheid toegepast mag worden met het oog op het overnemen of ontoegankelijkmaken van gegevens, in het licht van de opgedane ervaringen, uitbreiding behoeft. Tussentijdse toevoeging van misdrijven ligt in het licht van deze korte evaluatietermijn niet in de rede.

9.3. De vastlegging van gegevens over de uitvoering van een bevel in logbestanden

In de adviezen van de NP, de Inspectie JenV en in de reacties van BoF en KPN is voorgesteld om de loggingplicht uit te breiden tot de voorbereidende fase van het onderzoek: het binnendringen in een geautomatiseerd werk. Naar aanleiding van deze adviezen is de verplichting om gegevens vast te leggen over de uitvoering van een bevel in artikel 5 van het besluit uitgebreid tot de alle handelingen die worden verricht ter uitvoering van een bevel. Dit omvat mede de handelingen die worden verricht om een geautomatiseerd werk binnen te dringen. Hiermee wordt bereikt dat de

Inspectie van JenV meer handvaten krijgt voor het toezicht op het binnendringen in een geautomatiseerd werk en het verantwoord gebruik van binnendringsoftware hierbij.

De NP heeft in het advies over het ontwerpbesluit tekstvoorstellen gedaan over het onderscheid tussen de verschillende vormen van logging van gegevens over de uitvoering van een bevel, die zijn overgenomen in paragraaf 3.3 van deze nota van toelichting.

In het advies van de AP is geconstateerd dat het vastleggen van gegevens over de uitvoering van een bevel in logbestanden mede naar aanleiding van de ontvangen adviezen is uitgebreid tot de handelingen die worden verricht om een geautomatiseerd werk binnen te dringen. De AP heeft te kennen gegeven ten aanzien van dit punt geen inhoudelijke opmerkingen meer te hebben.

9.4. Technische eisen aan en keuring van een technisch hulpmiddel voor het verrichten van onderzoekshandelingen

In de (internet)consultatieronde zijn diverse opmerkingen gemaakt over de technische eisen aan en de keuring van een technisch hulpmiddel waarmee onderzoekshandelingen worden verricht in een geautomatiseerd werk. Het advies van de NP, de RvdR en de NVvR om in artikel 9 van het besluit, waarin technische eisen worden gesteld aan het hulpmiddel bedoeld voor het opnemen van telecommunicatie, niet uit te gaan van een nummer maar een techniekonafhankelijke formulering te gebruiken is overgenomen.

De adviezen van BoF en KPN om niet alleen technische hulpmiddelen die worden gebruikt voor het doen van onderzoek, maar ook hulpmiddelen die worden gebruikt bij het binnendringen te onderwerpen aan een voorafgaande keuring met het oog op het voorkomen van schade van derden, zijn niet overgenomen. Het functioneren van de binnendringsoftware wordt in een testomgeving gecontroleerd. In de procedure rondom de inzet van de software wordt aandacht besteed aan de risico's voor het te onderzoeken geautomatiseerd werk, waaronder schade aan derden. Voorafgaand aan de inzet stelt het technische team een rapport haalbaarheidsonderzoek op ten behoeve van de officier van justitie, waarin het plan van aanpak voor de uitvoering van een onderzoek in het geautomatiseerde werk is uitgewerkt. De inschatting van de beheersing en beperking van de risico's van het onderzoek is hiervan een onderdeel.

De AP heeft in het advies geconstateerd dat deze nadere onderbouwing voldoende duidelijkheid geeft omtrent de controle op de binnendringsoftware.

De NOvA heeft opgemerkt dat het onmogelijk is voor een verdachte om de betrouwbaarheid en integriteit van het met een technisch hulpmiddel vergaard bewijsmateriaal effectief te controleren, omdat een verdachte enkel aan de hand van het keuringsnummer kan nagaan dat het middel op enig moment ergens betrouwbaar is bevonden. De NOvA stelt zich op het standpunt dat een rechter hiervoor niet kan compenseren. Als bij het verrichten van onderzoekshandelingen in een geautomatiseerd werk gebruik wordt gemaakt van een goedgekeurd technisch hulpmiddel mag er vanuit worden gegaan dat aan de wettelijke eisen met betrekking tot betrouwbaarheid, integriteit en herleidbaarheid van de gegevens is voldaan. In dat geval wordt in het proces-verbaal van de inzet verwezen naar het keuringsnummer, waardoor de samenstelling van het hulpmiddel, ter bescherming van de opsporingsbelangen, kan worden afgeschermd. Anders dan de NOVA ben ik van mening dat de onafhankelijke rechterlijke toetsing van het gebruik van het technische hulpmiddel en het hiermee verkregen bewijsmateriaal voldoende waarborgen biedt voor effectieve controle in een concrete zaak. Indien er tijdens de behandeling van een strafzaak twijfels zouden rijzen over de betrouwbaarheid en de integriteit van het tijdens het onderzoek vergaarde bewijs,

kan de zittingsrechter de volledige informatie opvragen of een deskundige raadplegen.

9.5. Het verrichten van onderzoekshandelingen in een geautomatiseerd werk

In de (internet)consultatieronde zijn diverse opmerkingen gemaakt over het verrichten van onderzoekshandelingen in een geautomatiseerd werk al dan niet met gekeurde technische hulpmiddelen. Mede in reactie op het advies van de RvdR dat de informatievoorziening aan de rechter(commissaris) over de toelaatbaarheid van het gebruik van een technisch hulpmiddel verbetering behoeft is het gebruik van een niet (vooraf) gekeurd technisch hulpmiddel geëxpliciteerd in een nieuw artikel 21 van het besluit. In de nota van toelichting wordt op diverse plaatsen ingegaan op de informatieverstrekking aan de rechter(commissaris) over het gebruik van een technisch hulpmiddel ter uitvoering van een bevel.

Het advies van BoF om in het besluit vast te leggen dat de officier van justitie bij het gebruik van een niet gekeurd technisch hulpmiddel dient aan te geven welke aanvullende waarborgen zijn getroffen om te garanderen dat de gegevens betrouwbaar, integer en herleidbaar zijn is overgenomen. Dit wordt eveneens geregeld in het nieuwe artikel 21.

Het advies van BoF om de uitzonderingen omtrent het gebruik van niet dan wel achteraf goedgekeurde technische hulpmiddelen te beperken is niet overgenomen. Dit zou te belemmerend zijn voor de opsporingspraktijk. In de nota van toelichting zijn de uitzonderingsgevallen waarin keuring achterwege kan blijven verduidelijkt.

In het advies van T-Mobile is gevraagd naar de gevolgen van het verrichten van onderzoekshandelingen in een mobiel apparaat en het mogelijk verhoogde datagebruik van de gebruiker als gevolg hiervan. Voorts heeft T-mobile opgemerkt dat het niet duidelijk is of het bij de inzet van de bevoegdheid uitsluitend gaat over het geautomatiseerde werk van de verdachte of ook over de infrastructuur van de internetproviders en in hoeverre de continuïteit van deze infrastructuur mogelijk in het geding is. Meer specifiek heeft T-Mobile gevraagd in hoeverre maatregelen kunnen worden opgelegd aan het verlenen van toegang aan een geautomatiseerd werk van een verdachte van buitenaf en of hiervoor enige vorm van gegevensdeling nodig is, gelet op het feit dat in sommige gevallen het IP-adres wordt gedeeld tussen verschillende personen.

In reactie hierop wordt opgemerkt dat de politie maatregelen neemt om de kans dat het onderzoek wordt onderkend zoveel mogelijk te beperken. Welke maatregelen het betreft, kan in verband met de geheimhouding van opsporingsmethoden niet worden gemeld. T-mobile heeft terecht opgemerkt dat het vanuit technisch oogpunt lastig kan zijn om een geautomatiseerd werk te identificeren via een IP-adres. Daarom laat de wet ruimte om een andere wijze van identificatie te gebruiken. De technische wijze waarop een geautomatiseerd werk wordt geïdentificeerd is maatwerk.

T-Mobile heeft verzocht toe te lichten hoe in het geval van het verrichten van onderzoekshandelingen met gebruikmaking van zelfgemaakte scripts wordt geborgd dat dit professioneel gebeurt en hoe voorkomen wordt dat systemen in hun werking belemmerd worden, ook in het geval van reconaissance (scannen). In reactie hierop wordt opgemerkt dat de politie een professionele organisatie is en dat het verrichten van onderzoekshandelingen is voorbehouden aan aangewezen deskundige opsporingsambtenaren van een technisch team.

9.6. Verstrekking van ter uitvoering van het bevel vastgelegde gegevens

In de ontvangen adviezen zijn verschillende opmerkingen gemaakt over de verstrekking van gegevens die gedurende het verrichten van onderzoekshandelingen in een geautomatiseerd werk worden verkregen. De RvdR heeft opgemerkt dat onvoldoende onderscheid wordt gemaakt tussen ruwe gegevens en bewerkte gegevens. Ook heeft de RvdR het belang van het bewaard blijven van de ruwe gegevens en het belang van een transparante verslaglegging over de bewerking van gegevens benadrukt. De NVvR heeft geadviseerd om te bepalen aan wie en onder welke voorwaarden gegevens kunnen worden uitgegeven. De NOvA heeft opgemerkt dat het inherent aan digitaal verkregen gegevens is dat zij gemakkelijk gedeeld en verwerkt kunnen worden en dat het zorgwekkend is dat het besluit niets regelt over de noodzaak om automatische verwerking te beperken.

De ontvangen adviezen hebben geleid tot aanpassing van het besluit en de nota van toelichting. In het besluit is in een nieuw artikel 29 opgenomen waarin de verstrekking en bewerking van ter uitvoering van een bevel vastgelegde gegevens wordt geregeld. De nota van toelichting is aangevuld met een paragraaf (3.7) waarin de procedure voor de verdere verwerking van tijdens het onderzoek vergaarde gegevens en de bewerking van de gegevens wordt toegelicht.

Tevens is paragraaf 4 van deze nota van toelichting (gegevensverwerking) aangevuld op het punt van de bewaartermijnen van ruwe en bewerkte gegevens.

9.7. Overige opmerkingen

In verschillende ontvangen adviezen zijn opmerkingen gemaakt over onderwerpen die weliswaar betrekking hebben op het onderzoek in een geautomatiseerd werk, maar geen regeling vinden in het onderhavige besluit. Deze opmerkingen worden hieronder worden besproken.

In het advies van de NOvA is opgemerkt dat de bevoegdheid tot onderzoek in een geautomatiseerd werk op diverse punten in strijd zou zijn met het Europees Verdrag voor de Rechten van de Mens en de fundamentele vrijheden (EVRM) en in het bijzonder met artikel 8 van het EVRM dat het recht op eerbiediging van de persoonlijke levenssfeer beschermt. Het onderhavige besluit stelt regels over de uitwerking van de bevoegdheid, de grondslag voor de bevoegdheid is neergelegd in de wet. Wat betreft de juridische houdbaarheid van de nieuwe opsporingsbevoegdheid wordt verwezen naar de parlementaire geschiedenis bij de wet (Kamerstukken 32 372, in het bijzonder de memorie van toelichting (Kamerstukken II 2015/16 nr. 3, paragraaf 2.9.1), waarin uitgebreid wordt ingegaan op de beoordeling van de bevoegdheid in het licht van het recht op bescherming van de persoonlijke levenssfeer als neergelegd in artikel 10 van de Grondwet en artikel 8 van het EVRM.

De RvdR en de NOvA hebben opgemerkt dat de uitwerking van de stapsgewijze aanpak met betrekking tot de situatie waarin niet bekend is waar de gegevens zijn opgeslagen bij algemene maatregel van bestuur zou moeten plaatsvinden en niet bij Aanwijzing van het College van procureurs-generaal. De RvdR is van mening dat door uitwerking bij Aanwijzing op bescheiden wijze invulling wordt gegeven aan de verantwoordelijkheden voor interstatelijke opsporing en geeft in overweging om nader in te gaan op de vraag onder welke condities het binnendringen in een (vermoedelijk) zich in het buitenland bevindend geautomatiseerd werk toelaatbaar wordt geacht. De NOvA heeft opgemerkt dat het hier om gevoelige gevallen gaat, waarin datavergaring plaatsvindt bij (onder meer) personen die niet aan enig strafbaar handelen gelinkt kunnen

worden, en dat een dergelijke inbreuk op de burgerrechten voorzienbaar en kenbaar bij wet dient te zijn.

De wet maakt het mogelijk voor de officier van justitie om te bevelen dat onderzoek wordt gedaan in een geautomatiseerd werk dat in gebruik is bij een verdachte of, in het geval van een redelijk vermoeden van betrokkenheid bij het in georganiseerd verband beramen of plegen van misdrijven of in het geval van aanwijzingen van een terroristisch misdrijf, dat in gebruik is van een persoon. In de memorie van toelichting bij de wet (paragraaf 2.8.3) is uitgebreid ingegaan op de voorwaarden waaronder zelfstandig optreden in het geval de feitelijke locatie van gegevens redelijkerwijs niet te achterhalen valt aan de orde kan zijn. Hierbij gaat het om de situatie dat wel bekend is dat een geautomatiseerd werk in gebruik is bij een verdachte of een persoon, maar niet bekend is wat de feitelijke locatie is van het geautomatiseerde werk, waardoor de staat die betrokken is bij de opslag of verwerking van de gegevens niet kan worden bepaald en geen rechtshulp kan worden gevraagd. In een dergelijke situatie hanteert de officier van justitie een stapsgewijze aanpak voor het onderzoek in een geautomatiseerd werk.

De afweging om over te gaan tot zelfstandig optreden in een concrete zaak is onderdeel van de uitvoering van taken en bevoegdheden door het openbaar ministerie. Gelet hierop gaat vooralsnog de voorkeur uit naar uitwerking van de voorwaarden waaronder hiertoe kan worden overgegaan in een Aanwijzing van het College van procureurs-generaal. De criteria voor een stapsgewijze aanpak hebben betrekking op de inspanning die is vereist om de identiteit en locatie van een geautomatiseerd werk te achterhalen, de ernst van het strafbare feit, de mate van betrokkenheid van de Nederlandse rechtsorde (betrokkenheid van Nederlandse slachtoffers of de Nederlandse infrastructuur), de aard van de te verrichten opsporingshandelingen (worden gegevens alleen overgenomen of ook ontoegankelijk gemaakt) en de risico's voor het geautomatiseerde werk. Als bekend is dat de gegevens niet in Nederland zijn opgeslagen, vermeldt de officier van justitie dit in het bevel, zodat de rechter-commissaris hierover controle kan uitoefenen. In beginsel zal worden gestart met een beperkt eerste bevel met als onderzoeksdoel het bepalen van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker hiervan. Als verdergaande handelingen nodig zijn zal waar mogelijk worden volstaan met het overnemen van de opgeslagen gegevens, zodat de beschikkingsmacht van de rechthebbende niet wordt beperkt. Als bekend is, of in de loop van het onderzoek bekend wordt, dat de gegevens zich in een andere rechtsmacht bevinden dan ligt een verzoek om rechtshulp voor de hand, waarbij aan de bevoegde buitenlandse autoriteiten verantwoording kan worden afgelegd over de handelingen die zijn verricht en de afwegingen die daarbij zijn gemaakt.

De AP heeft geconstateerd dat de nota van toelichting, mede naar aanleiding van de ontvangen adviezen, is uitgebreid met de onderbouwing van de keuze om vooralsnog af te zien van regeling bij algemene maatregel van bestuur. De AP heeft ten aanzien van dit punt geen inhoudelijke opmerkingen meer.

KPN heeft gevraagd of informatie over onbekende kwetsbaarheden bij bekendmaking ook met partijen die behoren tot de vitale infrastructuur kan worden gedeeld zodat zij, wanneer nodig, tijdig hun infrastructuur en bedrijfsmiddelen kunnen beveiligen. Het Nationaal Cyber Security Centrum (NCSC) zal, als zij geïnformeerd wordt over een kwetsbaarheid, partijen binnen de doelgroep van de rijksoverheid en vitale sectoren informeren. Het NCSC zal, indien mogelijk, de verkregen informatie over kwetsbaarheden in samenspraak met de betrokkenen gebruiken om kennis verder te delen met de ICT-community, bijvoorbeeld door het openbaar maken van een deel van de informatie, het schrijven of

bijwerken van een factsheet of whitepaper of het gericht informeren van organisaties.

Ook heeft KPN gesuggereerd om, wanneer het binnendringen en het verrichten van onderzoekshandelingen plaatsvindt in de infrastructuur, diensten of producten van telecom- of internetproviders, de providers hiervan te notificeren, zodat deze bedrijven inzicht krijgen in eventuele kwetsbaarheden. In reactie hierop wordt allereerst opgemerkt dat het binnendringen in een geautomatiseerd werk van vitale sectoren zeer onwaarschijnlijk wordt geacht, onder meer omdat de desbetreffende organisaties in beginsel zelf benaderd kunnen worden om de voor de opsporing relevante gegevens te overleggen. Het binnendringen in een dergelijk geautomatiseerd werk kan echter niet bij voorbaat worden uitgesloten, bijvoorbeeld in het geval dat deze dienstverleners zelf zijn geïnfiltreerd door een kwaadwillende partij. Voor zover bij het binnendringen van een geautomatiseerd werk in een specifieke zaak gebruik wordt gemaakt van onbekende kwetsbaarheden kan de officier van justitie uitsluitend op grond van een zwaarwegend opsporingsbelang en na machtiging van de rechter-commissaris bevelen dat het bekend maken van een onbekende kwetsbaarheid wordt uitgesteld (126ffa Sv).

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 f). 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. Een «onderzoekshandeling» (onderdeel d) 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. Het betreft 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. Op grond van de wet kan het verrichten van onderzoekshandelingen al dan niet met een technisch hulpmiddel plaatsvinden. Van het verrichten van onderzoekshandelingen zonder technisch hulpmiddel is sprake als geen gebruik wordt gemaakt van software die gegevens detecteert, registreert en transporteert. Bij het verrichten van onderzoekshandelingen wordt in beginsel gebruik gemaakt van een vooraf goedgekeurd technisch hulpmiddel.

De RvdR heeft gevraagd in hoeverre is doordacht dat alleen softwareapplicaties een technisch hulpmiddel als bedoeld in het besluit kunnen zijn. Volgens de RvdR is het denkbaar dat ook met behulp van slimme hardware-ingrepen, of met apparatuur die een mix van hard- en softwarelementen bevat, heimelijk informatie kan worden verkregen. In reactie hierop wordt opgemerkt dat het verrichten van onderzoekshandelingen op grond van de artikelen 126nba/zpa/uba Sv mogelijk is nadat op afstand is binnengedrongen in een geautomatiseerd werk. Indien niet op afstand met behulp van hardware onderzoekshandelingen worden

verricht in een geautomatiseerd werk, dan wordt gebruikt gemaakt van de «traditionele» bijzondere opsporingsbevoegdheden.

T-mobile is van mening dat het begrip «technisch hulpmiddel» eng wordt gedefinieerd en wijst erop dat bij hacking niet alleen gebruik wordt van «standaard» software en bijbehorende payloads, maar ook van slimheid/scripts/own codes van hackers. In reactie hierop wordt opgemerkt dat onder technisch hulpmiddel uitsluitend de software wordt verstaan die wordt gebruikt voor het verrichten van onderzoekshandelingen. Voor zover er bij het binnendringen in een geautomatiseerd werk gebruik wordt gemaakt van software, wordt deze software niet gekeurd. Het binnendringen wordt gedaan door daartoe opgeleide deskundige opsporingsambtenaren van een technisch team. Met de definitie van «technische infrastructuur» (onderdeel g) wordt gedoeld op de opslaglocatie voor de gegevens die gedurende de uitvoering van een bevel worden vastgelegd en die kunnen dienen als een bewijs in een strafzaak. Uit deze definitie, in combinatie met de definitie van «technisch team» (onderdeel h), vloeit voort dat de vastlegging van gegevens dient plaats te vinden op een technische voorziening binnen de politieorganisatie. Deze eis wordt gesteld om de betrouwbaarheid en integriteit van het verkregen bewijsmateriaal te borgen en onbevoegde wijziging of kennisneming hiervan te voorkomen. In de definitie van «technisch team» is de centrale plaatsing van dit team als herkenbaar onderdeel binnen de Landelijke eenheid tot uitdrukking gebracht. De ophanging van de technische teams wordt betrokken bij de evaluatie van de wet die twee jaren na inwerkingtreding plaatsvindt.

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 misdrijven die een ernstige inbreuk op de rechtsorde kunnen opleveren aangewezen waarvoor de binnendring- en onderzoekbevoegdheid 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 ondergrens voor de aanwijzing betreft misdrijven waarvoor voorlopige hechtenis is toegelaten (artikelen 126nba/126uba, eerste lid, aanhef en onder en c, Sv, in samenhang bezien).

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 computervredebreuk, 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). De wet 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 Sr) zijn relevant, voor zover het gaat om het aftappen en opnemen van computergegevens. Daarnaast gaat het om de artikelen 161, eerste lid, 161bis, aanhef en onder 2°, en 161sexies Sr, 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 Sr (beschadiging van computergegevens), deze misdrijven worden eveneens aangewezen voor de toepassing van de bevoegdheid.

De tweede categorie van misdrijven die worden aangewezen zijn 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, 182Sr), 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 ontoegankelijkmaken van gegevens kan digitaal bewijs worden vergaard voor het gepleegde strafbare feit en kunnen criminele activiteiten worden beëindigd.

De afweging bij lichtere delictscenario's van aangewezen misdrijven kan ertoe leiden dat in een concreet geval wordt afgezien van de inzet van de bevoegdheid.

In de adviezen van de NOvA, de RvdR en het Platform BOD's zijn opmerkingen gemaakt over de reikwijdte van de toepassing van bevoegdheid met het oog op het vastleggen van gegevens of het ontoegankelijk maken van gegevens en de in dat kader in artikel 2 van het besluit aangewezen misdrijven. Deze opmerkingen zijn besproken in onderdeel 8.3 van deze toelichting en hebben om de daar genoemde redenen, niet geleid tot aanpassing van het artikel.

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 verrichten van onderzoekshandelingen is voorbehouden aan daartoe door hun werkgever 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. Een aangewezen opsporingsambtenaar kan de bevoegdheid uitsluitend uitoefenen als hij heeft voldaan aan door Onze Minister aangewezen kwalificaties en door de

korpschef is aangewezen als lid van een technisch team. 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. De kwalificaties waaraan een lid van een technisch team moet voldoen worden uitgewerkt in een ministeriële regeling, de Inspectie JenV zal worden geconsulteerd over de op te stellen 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 JenV.

De NP heeft opgemerkt dat de korpschef de leden van een technisch team niet kan aanwijzen, omdat hiervoor geen bevoegdheid zou bestaan. In de memorie van toelichting bij de wet (Kamerstukken II, 2015/16 34 372, nr 3, p. 24 en p.30) is opgemerkt dat de opsporingsambtenaren die door de korpschef zijn aangewezen en die ter zake deskundig zijn met de uitvoering van een bevel tot binnendringen in een geautomatiseerd werk en het verrichten van onderzoekshandelingen kunnen worden belast. In artikel 3 van dit besluit wordt hieraan invulling gegeven. In de tekst is verduidelijkt dat het bevoegd gezag de opsporingsambtenaren aanwijst die binnendringen in een geautomatiseerd werk en hierin al dan niet met een technisch hulpmiddel onderzoek doen. Vervolgens wordt geregeld dat aangewezen opsporingsambtenaren deze bevoegdheid uitsluitend kunnen uitoefenen als zij lid zijn van een technisch team en dat de korpschef aangewezen opsporingsambtenaren aanwijst als lid van een technisch team. In verband met de centrale positionering van een of meer technische teams bij de Landelijke eenheid dient de eindverantwoordelijkheid voor de technische teams, in ieder geval in de beginfase, bij de korpschef te liggen.

T-mobile heeft in de consultatiereactie de zorg uitgesproken dat kennis over de interne en complexe netwerken van de telecom providers niet is genoemd. In reactie hierop wordt opgemerkt dat actuele en uitgebreide kennis van ICT onderdeel uitmaakt van de kwalificaties waaraan de leden van een technisch team moeten voldoen. Om hun kennis actueel te houden zullen leden van een technisch team regelmatig bijscholingscursussen volgen.

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 deelname aan een technisch team als hij beschikt over specifieke kennis en vaardigheden die nodig zijn voor de uitvoering van een bevel in een individueel opsporingsonderzoek. De aanwijzing vindt plaats voor de duur van het bevel. 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 Vastlegging van gegevens over de uitvoering van een bevel

Artikel 5 Vastlegging van gegevens in logbestanden

Artikel 5 bepaalt dat alle handelingen 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 in logbestanden. Dit wordt ook wel logging genoemd. Alle handelingen die tijdens het onderzoek in een geautomatiseerd werk plaatsvinden worden gelogd. Dit betreft zowel de handelingen die tijdens de voorbereidende fase, het binnendringen in een geautomatiseerd werk, worden verricht als de handelingen die gedurende de onderzoeksfase worden verricht. Zowel onderzoekshandelingen die met een technisch hulpmiddel plaatsvinden als onderzoekshandelingen waarbij de inzet van een technisch hulpmiddel achterwege blijft worden vastgelegd in logbestanden. Ook het functioneren van de technische infrastructuur wordt gelogd. Samenvattend kunnen vier niveaus van logging worden onderscheiden: inzetlogging (eerste lid, onder a), bewijslogging (eerste lid, onder b), systeemlogging (eerste lid, onder c) en authenticatie- en autorisatielogging (eerste lid, onder d). De logging is ten eerste en vooral bedoeld voor de interne controle van de tijdens de uitvoering van het bevel verrichte handelingen en het functioneren van de technische infrastructuur. Uitsluitend de bewijslogging wordt, al dan niet in bewerkte vorm, aan het dossier in een strafzaak toegevoegd. De bewijslogging dient op grond van artikel 26 van het besluit plaats te vinden op een technische infrastructuur van een technisch team. Indien automatische logging technisch niet mogelijk is, vindt handmatige verslagging over de uitvoering van een bevel plaats, bijvoorbeeld in de vorm van een journaal (tweede lid).

De gelogde gegevens moeten op grond van de Wet politiegegevens worden verwijderd zodra deze niet langer noodzakelijk zijn voor het doel van het onderzoek. Toezicht op de naleving van de regels over de vastlegging in logbestanden vindt plaats door de Inspectie JenV. De AP is belast met het toezicht op de naleving van de Wet politiegegevens.

Artikel 6 Vaststelling van onregelmatigheden

Artikel 6 vereist dat de vastlegging in logbestanden op zodanige wijze geschiedt dat zowel tijdens de uitvoering van het bevel als achteraf kan worden vastgesteld of zich gedurende de uitvoering van het bevel een onregelmatigheid heeft voorgedaan, die van invloed is op de betrouwbaarheid van de met de onderzoekshandelingen verkregen gegevens. Indien dat het geval is, wordt hiervan proces-verbaal opgemaakt, dat aan de officier van justitie wordt gezonden.

In het geval in een strafzaak of in het kader van het toezicht door de Inspectie JenV twijfels ontstaan over de tijdens het onderzoek verrichte handelingen en/of de betrouwbaarheid van het hiermee vergaarde bewijs

kan aan de hand van de logging hierover verantwoording worden afgelegd.

Artikel 7 Betrouwbaarheid en integriteit logbestanden

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.

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

Hoofdstuk 5 Technische eisen aan een technisch hulpmiddel voor het verrichten van onderzoekshandelingen

Hoofdstuk 5 bevat de technische eisen waaraan een technisch hulpmiddel dat wordt gebruikt voor het verrichten van onderzoekshandelingen moet voldoen. Voorafgaand aan het gebruik van het technische hulpmiddel vindt keuring plaats aan de hand van deze eisen. De keuring richt zich daarbij op de betrouwbaarheid en integriteit van de uitvoering van de onderzoekshandelingen met een technisch hulpmiddel en de betrouwbaarheid, integriteit en herleidbaarheid van de verkregen gegevens, die kunnen dienen als bewijs in eens strafzaak. In hoofdstuk 6 van dit besluit worden regels gesteld over de keuringsprocedure. De Inspectie JenV en houdt toezicht op de naleving van de technische eisen en de keuringsprocedure.

Artikelen 8 en 9 Gerichte 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 procesverbaal (artikel 22 van het besluit).

De NP heeft in het advies over artikel 8 van het besluit opgemerkt dat dit artikel de mogelijkheid openhoudt om in bepaalde gevallen een technisch hulpmiddel te gebruiken waarvan de technische werking vanuit de aard van het hulpmiddel niet volledig beperkt kan worden tot de in het bevel vermelde functionaliteit of functionaliteiten in combinatie met selectie van de verkregen gegevens door het technische team. Artikel 29 van het besluit bevat een regeling over verstrekking en bewerking van gegevens aan een tactisch team.

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

De eis in artikel 9, tweede lid, is gebaseerd op artikel 11 van het Besluit technische hulpmiddelen strafvordering, dat betrekking heeft op technische hulpmiddelen die worden ingezet ten behoeve van het opnemen van telecommunicatie. Om digitale communicatievormen steeds minder via de traditionele nummers lopen is in plaats van «nummer» een techniekonafhankelijke formulering gebruikt. Hiermee wordt tegemoet gekomen aan de adviezen van de NP, de RvdR en de NVvR. Een technisch hulpmiddel mag uitsluitend de communicatie die plaatsvindt met gebruikmaking van één of meer identificerende kenmerken van het geautomatiseerde werk van de individuele gebruiker of gebruikers op wie het bevel betrekking heeft registreren.

Artikelen 10, 11 en 12 Betrouwbaarheid en integriteit, herleidbaarheid, datum en 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 gedoeld 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. In

gevallen waarbij technische hulpmiddelen worden gebruikt die gegevens extraheren die in de cloud zijn opgeslagen nadat bijvoorbeeld een gebruikersnaam en wachtwoord zijn verkregen vinden detectie en registratie pas plaats in het technisch hulpmiddel zelf. Een voorbeeld is een technisch hulpmiddel waarmee een mailbox van een verdachte wordt gelezen. 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 apparatuur 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 logging 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.

Zoals de RvdR in zijn advies ook heeft opgemerkt hebben de datum en het tijdstip van betrekking op gegevensregistratie door het Nederlandse technische hulpmiddel. Als de gegevens afkomstig zijn van een locatie uit een andere tijdszone, dan zal het technische hulpmiddel de Nederlandse datum en tijd registeren. Na overlegging van de onderzoeksresultaten door het technische team aan het tactische team kan het tactische team het tijdsverloop reconstrueren.

De RvdR geeft in overweging om te bepalen dat indien de gegevens afkomstig zijn van een locatie uit een andere tijdzone, daarbij zoveel mogelijk het verschil tussen de geregistreerde tijd en de lokale tijd te vermelden. Dit zal worden meegenomen in het keuringsprotocol.

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 voor het verrichten van onderzoekshandelingen

Artikel 14 Voorafgaande goedkeuring en herkeuring

Uitgangspunt is dat bij het verrichten van onderzoekshandelingen gebruik wordt gemaakt van een vooraf goedgekeurd technisch hulpmiddel (eerste lid). Een technisch hulpmiddel wordt uitsluitend goedgekeurd als het voldoet aan de artikelen 8 tot en met 13 gestelde eisen (tweede lid). Dit wordt beoordeeld tijdens de keuring door een keuringsdienst. Keuring van een technisch hulpmiddel kan enkele maanden in beslag nemen, zeker als de software nog aanpassing behoeft voordat deze kan worden goedgekeurd. Voor zover de aan te schaffen technische hulpmiddelen voor het verrichten van onderzoekshandelingen onderdeel uitmaken van een softwarepakket waarmee ook een geautomatiseerd werk kan worden binnengedrongen, zal de politie in de voorbereiding van de inwerkingtreding van de wet onderzoeken welke betrouwbare bedrijven dergelijke software kunnen leveren en de mogelijkheden bezien deze software voorafgaand aan de aanschaf voor een specifiek onderzoek alvast te keuren.

Herkeuring van een technisch hulpmiddel 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 13 gestelde eisen (derde lid). 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 de reactie van BoF op het ontwerp-besluit is gevraagd om een verduidelijking van het herkeuringsbeleid. Wanneer er een update van de software plaatsvindt, zal bij de keuringsinstantie een inschatting worden gemaakt of redelijkerwijs kan worden aangenomen dat het technisch hulpmiddel nog aan de technische eisen voldoet. Dit gebeurt mede op basis van de notificatie die de update begeleidt waarin de impact van de update wordt vermeld. Dit kan variëren van een toevoeging van een bepaalde taal waarin de software verkrijgbaar is tot een aanpassing van de functionaliteiten. Zo nodig wordt het technische hulpmiddel opnieuw gekeurd.

T-mobile heeft in de reactie op het ontwerp-besluit te kennen gegeven graag een garantie opgenomen te zien in het besluit dat er geen schade wordt toegebracht aan de systemen, netwerken en bedrijfsprocessen van internetproviders. Internetproviders zouden tevens inspraak moeten hebben in de manier waarop een keuring plaatsvindt en op basis van welke eisen, aldus T-mobile. Deze suggesties zijn niet overgenomen. Het doel van de keuring is om te kunnen borgen dat de werking van een technisch hulpmiddel dusdanig betrouwbaar is dat de met een technisch hulpmiddel verkregen gegevens, die kunnen dienen als bewijs in een strafzaak, betrouwbaar, integer en herleidbaar zijn. De inschatting, beheersing en beperking van de risico's voor het geautomatiseerde werk zijn afwegingen die niet zozeer betrekking hebben op de werking van een technisch hulpmiddel als wel op de daadwerkelijke inzet hiervan. Daarbij is de deskundigheid van de betrokken opsporingsambtenaren van essentieel belang. Gelet hierop zijn de handelingen die met een technisch hulpmiddel worden verricht voorbehouden aan hiervoor speciaal opgeleide opsporingsambtenaren van een technisch team

BoF heeft in de reactie op het ontwerpbesluit verzocht het herkeurings-beleid te verduidelijken en expliciet beleid op te stellen. In reactie hierop wordt opgemerkt dat het herkeuringsbeleid onderdeel zal zijn van het keuringsprotocol dat wordt opgesteld door de keuringsdienst.

Voorts heeft BoF gevraagd of er afspraken zijn met de leveranciers van de technische hulpmiddelen om voor de keuring inzage te krijgen in, bijvoorbeeld, de broncode van het technisch hulpmiddel, of het algoritme dat wordt ingezet om bijvoorbeeld zoekopdrachten uit te voeren. Dergelijke afspraken worden niet voorzien, omdat de leveranciers de broncode niet zullen prijsgeven.

De NOvA heeft opgemerkt dat het besluit niet voorziet in effectieve toetsing van de betrouwbaarheid van het technische hulpmiddel omdat er geen sprake is van periodieke keuring van het hulpmiddel. Zolang het niet wordt gewijzigd wordt het veilig en betrouwbaar gehouden. In reactie hierop wordt gewezen op artikel 18, derde lid, onder g, waarin is bepaald dat een keuringsrapport de periode waarvoor de keuring geldt vermeldt, op de voorwaarde dat de werking van het technische hulpmiddel niet tussentijds gewijzigd wordt. Een keuringsrapport zal voor bepaalde tijd worden afgegeven. Na afloop van de termijn kan de keuringsdienst het hulpmiddel opnieuw keuren of, indien de werking niet gewijzigd is, de goedkeuring verlengen. In het keuringsprotocol worden de voorwaarden nader worden uitgewerkt.

Artikel 15 Uitzonderingen op voorafgaande keuring en herkeuring

Van het uitgangspunt van voorafgaande keuring en herkeuring van een technisch hulpmiddel kan worden afgeweken indien de officier van justitie dit heeft bepaald omdat een dringend onderzoeksbelang daartoe noodzaakt. Deze uitzondering is geregeld in artikel 15 van dit besluit. Als een technisch hulpmiddel wordt gebruikt dat niet vooraf is goedgekeurd, wordt het hulpmiddel na afloop alsnog gekeurd (artikel 15, eerste lid en artikel 21, 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 keuring achterwege blijft (artikelen 15, tweede lid, en 21, vierde lid). Voor een nadere toelichting op de situaties waarin een uitzondering wordt gemaakt op het gebruik van vooraf gekeurde technische hulpmiddelen en de hierbij te volgen procedure wordt verwezen naar de artikelsgewijze toelichting bij artikel 21.

Het advies van KPN om technische hulpmiddelen voor het verrichten van onderzoekshandelingen altijd vooraf te keuren om schade van derden te voorkomen wordt niet gevolgd, omdat dit de opsporingspraktijk teveel zou belemmeren. Opgemerkt wordt verder dat in de praktijk niet lichtzinnig van het gebruik van een goedgekeurd hulpmiddel zal worden afgezien. Bij deze afweging zal de officier van justitie in overleg met de keuringsinstantie nagaan of het beoogde technische hulpmiddel naar verwachting zal voldoen aan de in het besluit gestelde technische eisen. Het verrichten van onderzoekshandelingen met het hulpmiddel is voorbehouden aan deskundige leden van een technisch team.

De AP heeft in het advies over het besluit aangegeven dat zij graag had gezien dat technische hulpmiddelen voor het verrichten van onderzoekshandelingen altijd vooraf gekeurd zouden worden, maar is van mening dat de nadere onderbouwing met betrekking tot het achterwege laten van de keuring voldoende duidelijkheid geeft ten aanzien van het gebruik van niet gekeurde technische hulpmiddelen.

Artikelen 16 tot en met 19 Keuringsdienst, keuringsprotocol, keuringsrapport

In de artikelen 16 tot en met 19 van dit besluit is de keuringsprocedure neergelegd. 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 keuringsdienst 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 Justitie en Veiligheid. 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 worden volstaan met verwijzing naar dit keuringsnummer. 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. Het is mogelijk om te voldoen aan een of meer in het besluit gestelde technische eisen via vervangende procedurele waarborgen (derde lid, onderdeel e). 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 op de voorwaarde dat de werking van het technische hulpmiddel 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. De Inspectie JenV houdt toezicht op de naleving van de keuringsprocedure.

De RvdR en de NVvR hebben geadviseerd om de keuze voor het beleggen van de keuringstaak bij de politie zelf te heroverwegen dan wel nader toe te lichten. In reactie hierop wordt opgemerkt dat de keuring van de «traditionele» technische hulpmiddelen voor de opsporing eveneens is opgedragen aan een onderdeel van de politieorganisatie. De ervaringen met deze keuring bevestigen dat de politie in staat is om de keuring op onafhankelijke wijze te borgen binnen de eigen organisatie. Ter voorbereiding van inwerkingtreding van de wet wordt binnen de politieorganisatie geïnvesteerd in de ontwikkeling van hoogwaardige expertise voor het keuren van technische hulpmiddelen voor het verrichten van onderzoekshandelingen in een geautomatiseerd werk.

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 die, onder de voorwaarden genoemd in artikel 20, niet alleen geldt voor technische hulpmiddelen en keuringsrapporten uit lidstaten van de Europese Unie, maar ook voor andere technische hulpmiddelen en keuringsrapporten uit landen waarmee de EU een douaneunie of een vrijhandelszone vormt.[6]

Hoofdstuk 7 Het verrichten van onderzoekshandelingen in een geautomatiseerd werk

In hoofdstuk 7 worden eisen gesteld aan de onderzoeksfase waarin al dan niet met een technisch hulpmiddel onderzoekshandelingen worden verricht en gegevens worden vastgelegd op een technische infrastructuur die kunnen dienen als bewijs in een strafzaak. De Inspectie VenJ houdt toezicht op de naleving van de eisen die gesteld worden in hoofdstuk 7 van dit besluit.

Artikel 21 Uitvoering van een bevel

In artikel 21 wordt de relatie tussen het bevel van de officier van justitie en het verrichten van onderzoekshandelingen al dan niet met een technisch hulpmiddel uitgewerkt. Hoofdregel in artikel 21, eerste lid, is dat bij de uitvoering van een bevel gebruik wordt gemaakt van een vooraf goedgekeurd technisch hulpmiddel (conform artikel 14). Bij de voorbereiding van het bevel wordt hiermee rekening gehouden. Het technische team stelt een rapport haalbaarheidsonderzoek op voor de officier van justitie, dat het plan van aanpak voor de uitvoering van een onderzoek bevat. In het rapport wordt onder meer opgenomen welk technisch hulpmiddel voor het verrichten van onderzoekshandelingen 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. Bij de aanvraag om machtiging wordt informatie verstrekt aan de rechter-commissaris over de beoogde functionaliteiten van het technisch hulpmiddel.

Indien het onderzoeksbelang dit dringend vordert, kan de officier van justitie bepalen dat een niet vooraf gekeurd technisch hulpmiddel wordt gebruikt (tweede lid). Hierbij kan worden gedacht aan de situatie dat (her)keuring voorafgaand aan de inzet teveel tijd zou vergen. Het moet dan gaan om situaties waarin het belang van het onderzoek de inzet van het desbetreffende technische hulpmiddel dringend vordert. Bij deze afweging zal de officier van justitie in overleg met de keuringsinstantie 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 vermeld dat een niet vooraf gekeurd technisch hulpmiddel wordt ingezet (artikel 21, tweede lid). Als bij de uitvoering van een bevel gebruik wordt gemaakt van een niet vooraf gekeurd hulpmiddel vindt alsnog keuring achteraf plaats (artikel 15, eerste

[6] Niet lidstaten waarmee de EU een vrijhandelszone vormt zijn: Liechtenstein, Noorwegen, IJsland en Zwitserland.

lid). De officier vermeldt de uitkomst van de keuring in de processtukken (artikel 21, derde lid).

In uitzonderingsgevallen kan de keuring van een technisch hulpmiddel geheel achterwege blijven, namelijk indien de aard van het technische hulpmiddel zich naar het oordeel van de officier van justitie daartegen verzet (artikel 21, vierde lid). Van deze uitzondering zal in de praktijk niet lichtzinnig gebruik worden gemaakt. Hierbij kan worden gedacht aan de situatie van een speciaal op maat gemaakt technisch hulpmiddel. Wanneer het technische hulpmiddel specifiek is aangepast aan de omgeving waarin de inzet heeft plaatsgevonden, kan het problematisch zijn om bij een keuring dezelfde situatie na te bootsen. Met name bij op maat gemaakte software die tijdens het verrichten van onderzoekshandelingen nog moet worden aangepast aan de omstandigheden, kan het onuitvoerbaar zijn om de omstandigheden waarbinnen de inzet plaats heeft gevonden te reproduceren en het ingezette technische hulpmiddel daarop te keuren. Indien de officier van justitie beveelt dat onderzoekshandelingen worden verricht zonder technisch hulpmiddel dan worden ter uitvoering van het bevel de onderzoekshandelingen verricht die omschreven zijn in het bevel (artikel 21, vijfde lid).

Als keuring van een hulpmiddel geheel achterwege blijft of als onderzoekshandelingen worden verricht zonder gebruik van een technisch hulpmiddel dan vermeldt de officier in de processtukken welke aanvullende waarborgen zijn getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de vastgelegde gegevens te garanderen (artikel 21, vierde en vijfde lid). Hierbij kan worden gedacht aan een uitgebreide omschrijving van de functionele specificaties van op maat gemaakt technische hulpmiddel, het voegen van een digitale kopie van de software en de broncode bij het proces-verbaal, het vooraf en achteraf maken van een forensische kopie of het audiovisueel vastleggen van de uitvoering van de onderzoekshandelingen. De aanvullende procedurele eisen van de officier van justitie kunnen de rechtmatigheid van de inzet waarborgen en voorkomen dat er twijfel ontstaat over de betrouwbaarheid, integriteit en herleidbaarheid van de vastgelegde gegevens.

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

T-Mobile heeft in reactie op het ontwerp-besluit vragen gesteld over het de uitwerking in de praktijk van het treffen van de noodzakelijke procedurele maatregelen bij het werken met een ad-hoc script. Verwezen wordt naar de hierboven genoemde (niet limitatieve) voorbeelden van maatregelen die kunnen worden getroffen.

Artikelen 22 en 23 Toegang en plaatsing van een technisch hulpmiddel

Artikel 22 bepaalt dat de toegang tot technische hulpmiddelen centraal wordt geregistreerd. De korpschef wijst één of meer ambtenaren aan die met de registratie zijn belast (eerste lid). 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 (tweede lid). De toegang tot een technisch hulpmiddel wordt verleend voor de periode die nodig is voor de uitvoering van het bevel (derde lid). De met registratie belaste ambtenaar registreert de aanduiding van het technische hulpmiddel, het tijdstip van de toegangverlening, de in het bevel vermelde aanduidingen van de aard en functionaliteit van het technische hulpmiddel, de in het bevel vermelde periode waarbinnen aan het bevel uitvoering moet worden gegeven en, in navolging van het advies van de RvdR, de aanduiding van de opsporings-

ambtenaar die om toegang tot het technische hulpmiddel verzoekt. De Inspectie VenJ en houdt toezicht op de naleving van de toegangsprocedure.

Artikel 23 Plaatsing van een technisch hulpmiddel

De plaatsing van een technisch hulpmiddel vindt plaats door een opsporingsambtenaar van een technisch team (artikel 23). 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 technische 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 waarmee onderzoekshandelingen worden verricht geplaatst. Het tweede lid vereist dat bij de plaatsing van een technisch hulpmiddel uitsluitend de in het bevel van de officier aangeduide functionaliteiten worden ingeschakeld. Hierover wordt verantwoording afgelegd in een proces-verbaal. 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. Indien bij de plaatsing een onregelmatigheid plaatsvindt dan maakt een opsporingsambtenaar van een technisch team hiervan proces-verbaal op, dat aan de officier van justitie wordt gezonden (derde lid). Via de logging kan controle worden uitgeoefend op het plaatsen van een technisch hulpmiddel.

In navolging van een daartoe strekkend advies van de RvdR is zowel in artikel 23 (plaatsing) als in artikel 24 (onderzoekshandelingen verrichten) een artikellid toegevoegd over melding van eventuele (technische) onregelmatigheden in het proces-verbaal (vierde lid).

Artikelen 24 Onderzoekshandelingen verrichten.

In artikel 24 wordt geregeld dat het verrichten van onderzoekshandelingen al dan niet met een technisch hulpmiddel plaatsvindt door een opsporingsambtenaar van een technisch team (eerste lid). Van het verrichten van onderzoekshandelingen wordt proces-verbaal opgemaakt, dat aan de officier van justitie wordt gezonden (tweede lid). Indien bij de uitvoering van de onderzoekshandelingen een onregelmatigheid plaatsvindt maakt een opsporingsambtenaar van een technisch team hiervan melding in het proces-verbaal (derde lid). Via de logging kan controle worden uitgeoefend op de verrichte onderzoekshandelingen.

Artikelen 25 en 26 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 JenV houdt toezicht op de naleving op de juiste uitvoering van de verwijderingsprocedure.

De NP heeft opgemerkt dat uit het besluit niet duidelijk op te maken valt op welke gronden tot verwijderen van een technisch hulpmiddel na afloop van een bevel tot binnendringen van een geautomatiseerd werk wordt overgegaan en beveelt aan om aansluiting te zoeken bij artikel 2.8.2.1.1 vijfde lid uit het in consultatie gegeven wetsvoorstel van boek 2 van het Wetboek van Strafvordering. Hiervoor is in het onderhavige geval geen aanleiding nu de verwijdering van een technisch hulpmiddel, gelet op de formulering van artikel 28, moet plaatsvinden uiterlijk zodra de periode waarbinnen aan het bevel uitvoering moet worden gegeven is verlopen.

T-mobile heeft gevraagd hoe gegarandeerd kan worden dat bij niet of niet volledige verwijdering: de nog steeds aanwezige technische hulpmiddelen geen schade toebrengen aan de TMNL infrastructuur, bedrijfsprocessen etc. Dit is vooral van belang omdat er geen sprake meer is van communicatie tussen hulpmiddel en technische infrastructuur en dus wellicht ook geen actieve monitoring over het goed functioneren van een technisch hulpmiddel. T-Mobile is van mening dat de opsporing een plicht heeft om het technische hulpmiddel te verwijderen. Volgens het principe van «ethical hacking» dienen alle technische hulpmiddelen weer verwijderd te worden.

Het uitgangspunt bij de opsporing is dat een geplaatst technisch hulpmiddel ook weer wordt verwijderd. Er kunnen zich echter situaties voordoen waarin de verwijdering niet mogelijk is, of niet mogelijk zonder zeer grote kans op onderkenning van het onderzoek. In dat geval wordt het transport van de gegevens beëindigd.

Artikelen 27 en 28 Vastlegging van gegevens op technische infrastructuur, betrouwbaarheid en integriteit technische infrastructuur

De vastlegging van de in de onderzoeksfase 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 tijdens het verrichten van onderzoekshandelingen geregistreerde gegevens (artikel 27). De technische infrastructuur moet in staat zijn om het unieke gegeven dat door het technische hulpmiddel aan de geregistreerde gegevens is toegevoegd te herkennen. 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. 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.

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 (artikel 28). De gegevens mogen niet inhoudelijk worden bewerkt en dienen te worden beveiligd tegen wijziging en kennisneming hiervan door onbevoegden. De vastgelegde gegevens zijn uitsluitend toegankelijk voor de door de korpschef aangewezen ambtenaren. Tactische opsporingsambtenaren hebben geen toegang.

De veiligheidsstandaarden voor de digitale infrastructuur van de politie in het algemeen moeten voldoen aan hoge standaarden aangezien deze structuur voortdurend onder druk staat van buitenaf om de beveiliging te compromitteren. De veiligheid van het technische hulpmiddel en de technische infrastructuur is voor de opsporingsinstanties van groot belang, omdat het compromitteren hiervan van invloed kan zijn op de integriteit van het bewijs. Daarom worden aanvullend de bovengenoemde eisen gesteld.

Via de logging kan controle worden uitgeoefend op het functioneren van de technische infrastructuur. Zowel tijdens de uitvoering van een bevel als achteraf moet kunnen worden vastgesteld of wijziging dan wel onbevoegde kennisneming van de op de technische infrastructuur vastgelegde gegevens heeft plaatsgevonden. Indien een onregelmatigheid wordt vastgesteld die van invloed is op de kwaliteit van de 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 JenV houdt toezicht op de naleving van de regels en procedures omtrent de vastlegging van gegevens op een beveiligde technische infrastructuur.

Hoofdstuk 8 Verstrekking van ter uitvoering van een bevel vastgelegde gegevens

Artikel 29 Verstrekking en bewerking van vastgelegde gegevens

Artikel 29 stelt regels over de verstrekking en bewerking van op de technische infrastructuur vastgelegde gegevens. Deze gegevens, die kunnen dienen als bewijs in een strafzaak, worden verstrekt aan een opsporingsambtenaar van een tactisch team. Indien het ter uitvoering van een bevel of ten behoeve van het opsporingsonderzoek nodig is om een selectie te maken uit op een technische infrastructuur vastgelegde gegevens, kan een opsporingsambtenaar van een technisch team vooraf de gegevens bewerken (tweede lid). Selectie kan bijvoorbeeld aan de orde zijn bij het opnemen van vertrouwelijke communicatie of het aftappen en opnemen van telecommunicatie of de vastlegging van gegevens die in het geautomatiseerde werk zijn of worden opgeslagen, zoals email-verkeer. Hierbij kan niet worden uitgesloten dat gegevens worden verkregen over andere personen die bij de communicatie zijn betrokken. Deze gegevens zijn niet van belang voor het opsporingsonderzoek. Daarom wordt uitsluitend het email-verkeer waarvan de email-adressen zijn opgenomen op een vooraf opgestelde lijst ter beschikking gesteld van het tactische onderzoeksteam. In het bevel wordt melding 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 aan het tactische team.

Als de opsporingsambtenaar van een technisch team een bewerking uitvoert dan gebruikt hij een forensische kopie van de conform artikel 27 op de technische infrastructuur vastgelegde gegevens (tweede lid). Bij de selectie van gegevens legt de opsporingsambtenaar vast welke bewerkingen hebben plaatsgevonden met betrekking tot de gegevens (derde lid).

Hoofdstuk 9 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 10 Inwerkingtreding

Artikelen 30 en 31 Inwerkingtreding en citeertitel

Dit besluit heeft als citeertitel «Besluit onderzoek in een geautomatiseerd werk» en treedt tegelijk in werking met de wet.

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus